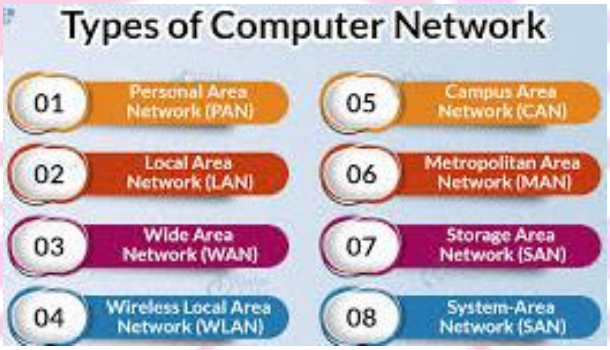
History of Computer Networks

- 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

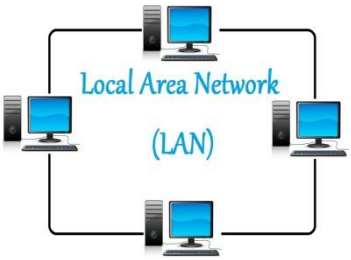
- A computer network is a collection of interconnected devices (such as computers, servers, and peripherals) that communicate and share resources (e.g., data, applications, and hardware) using wired or wireless communication channels.
- Networks range from small (LAN) to global (Internet), supporting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

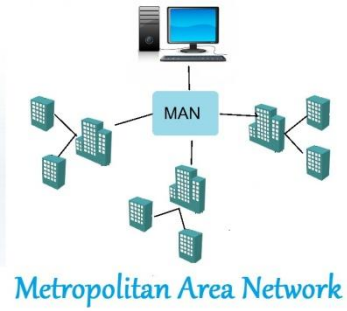


Advantages:
High speed and low latency.
Cost-effective as it uses inexpensive equipment like switches and routers.
Easy to maintain and troubleshoot.

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:

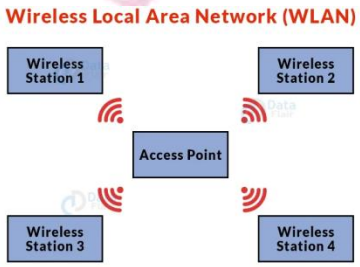
- Convenient and easy to set up.
- Low cost due to limited range and simple devices.
- Promotes mobility and portability.

Disadvantages:

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

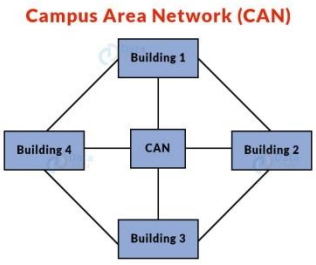
5. Wireless Local Area Network (WLAN)

- 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.



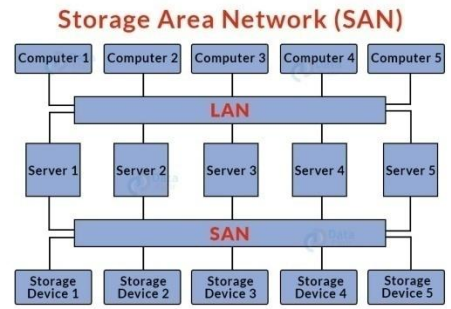
6. Campus Area Network (CAN)

- 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.



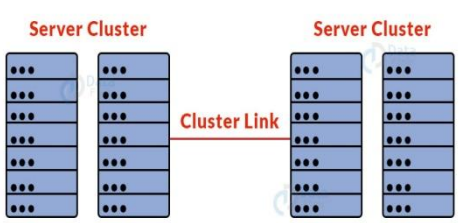
7. Storage Area Network (SAN)

- 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.

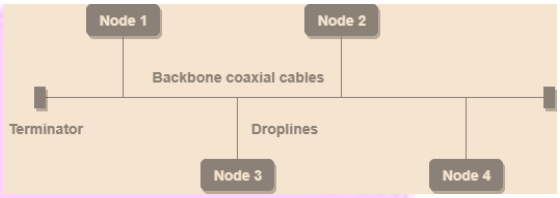
2. Extranet

- 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:

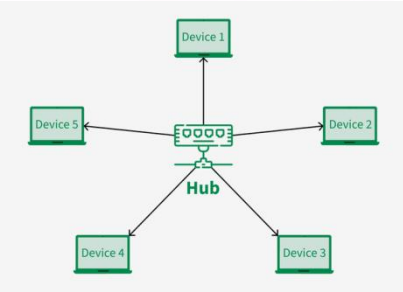
- Simple and inexpensive to implement.
- Requires less cable compared to other topologies.

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:

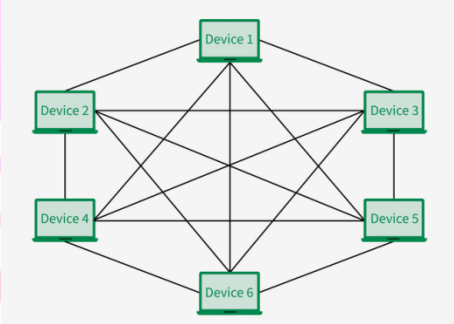
- Equal access to the network for all devices.
- Efficient for small networks with predictable traffic.

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:

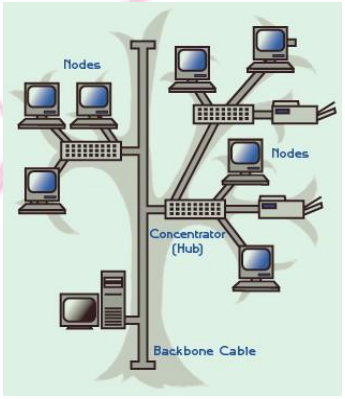
- Network remains functional even if one device fails.
- No traffic issues due to dedicated point-to-point links.
- Offers high privacy, security, and reliable data transmission.
- Adding devices does not disrupt the network.

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:

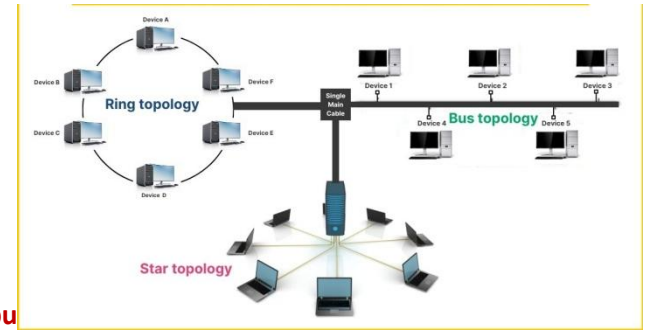
- Scalable and suitable for hierarchical organizations as the leaf nodes can add one or more nodes.
- Fault isolation is easier.

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.



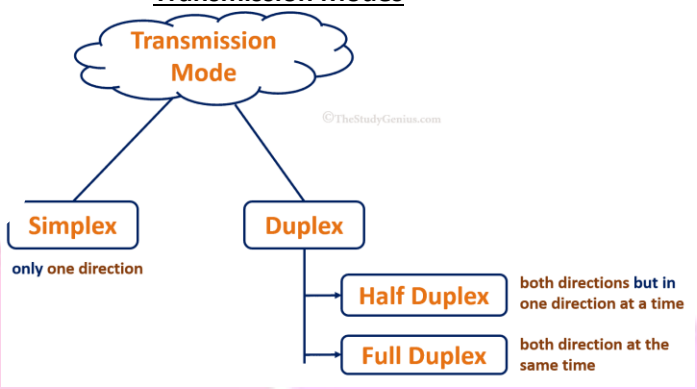
Advantages:

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

Disadvantages:

- Complex to design and maintain.
- Expensive

Transmission Modes

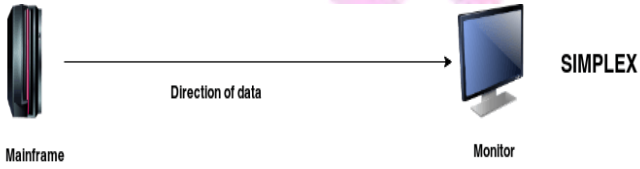


1. Simplex Mode

- 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:

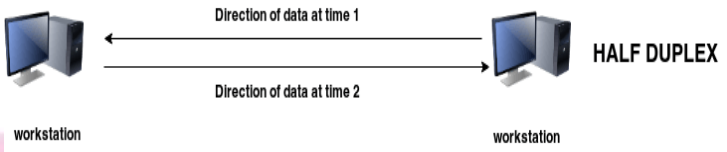
- Simple and cost-effective.
- Efficient for applications where only one-way communication is needed.

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:

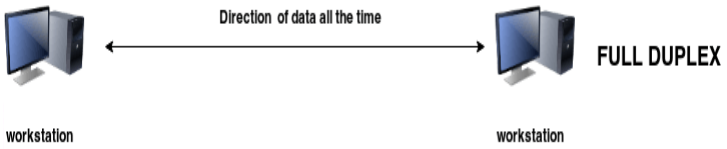
- Allows two-way communication.
- More cost-effective than full-duplex systems.

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:

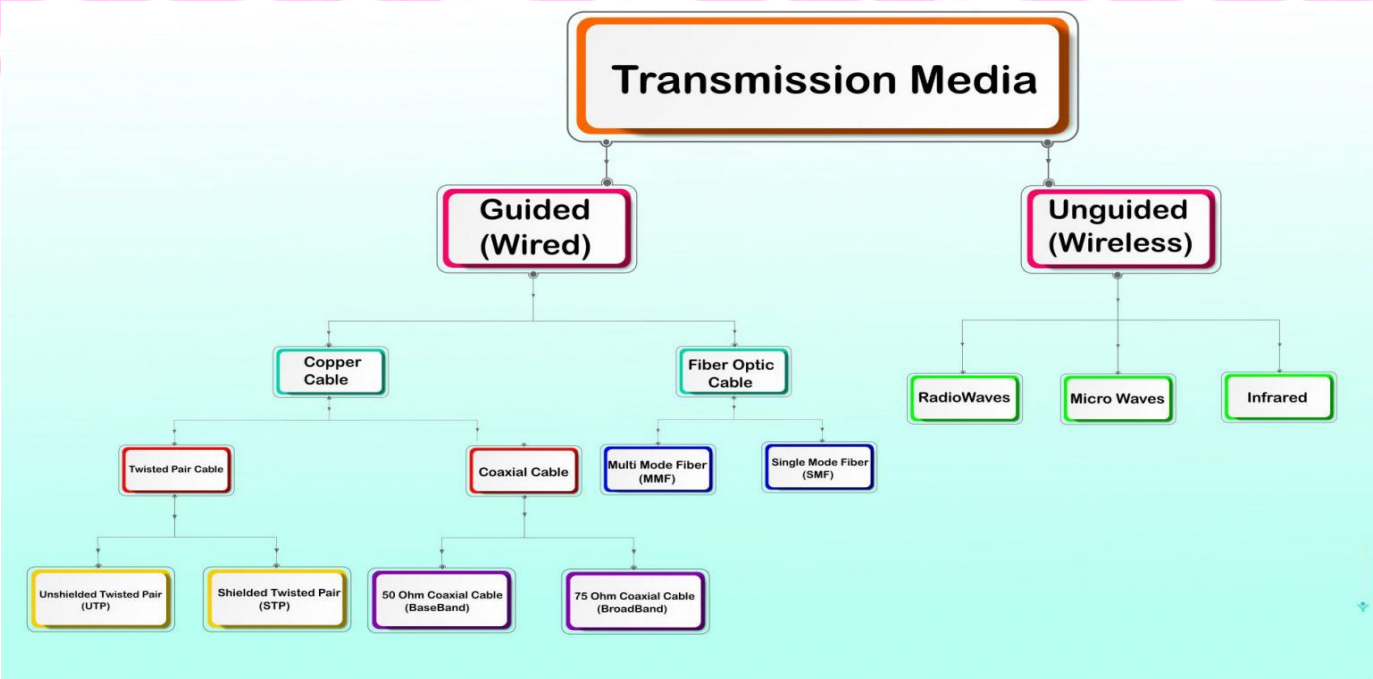
- Fast and efficient communication.
- Ideal for real-time applications like voice and video calls.

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.

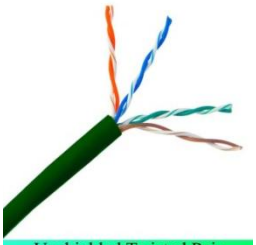


Types of Transmission media

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

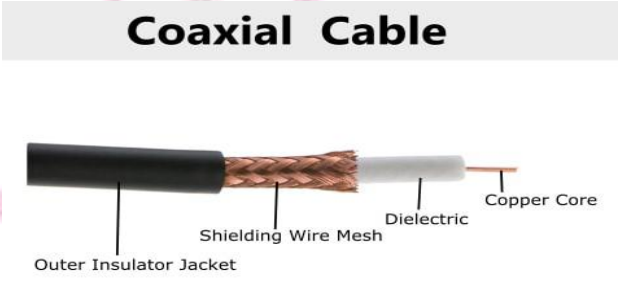
- Cost-Effective: Cheaper than other guided media like coaxial and fiber optic cables.
- Flexible and Easy to Install: Lightweight and simple to handle.
- Widely Available: Easily found and used in most network setups.

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

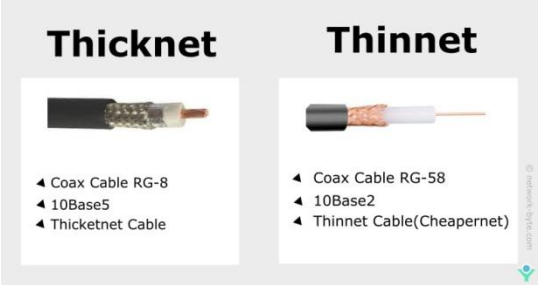
- A coaxial cable (coax cable) is a high-frequency transmission cable with low signal loss.
- It has a single solid copper core surrounded by insulation, a metallic shield, and an outer cover.
- This design prevents electromagnetic interference and helps transmit radio frequency (RF) signals as transverse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



The coaxial cable transmits information in two modes:

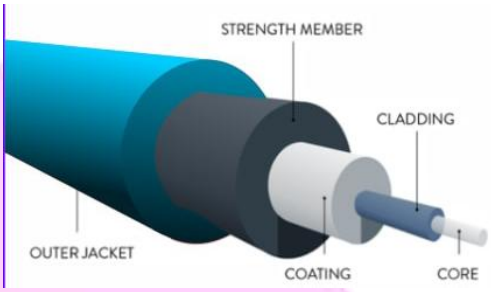
a) **Baseband mode**
b) **Broadband mode**.

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.

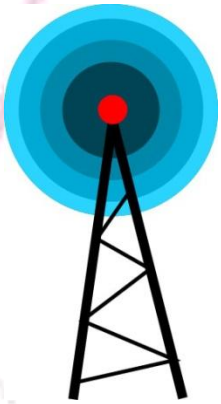
Disadvantages:
Expensive, complex installation, and maintenance.

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

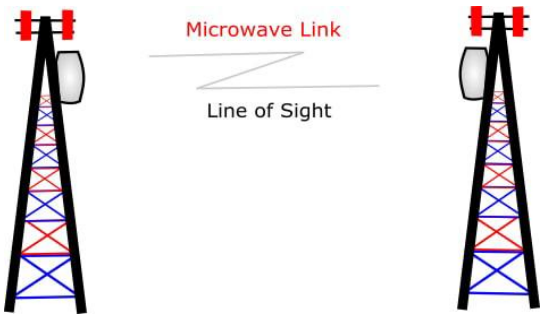
- Radio waves are electromagnetic waves with wavelengths ranging from 1 mm to 100 km (frequencies between 3 kHz to 300 GHz).
- They are omnidirectional, meaning they travel in all directions from the source.
- Generated by radio transmitters and received by radio receivers, both use antennas to transmit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

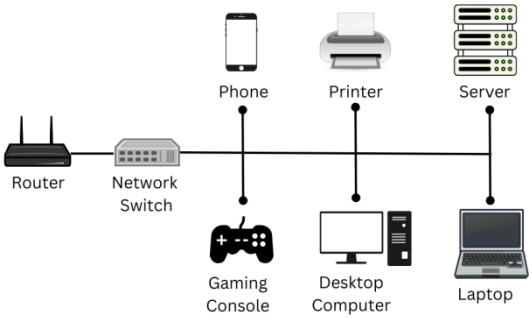
Applications: Small networks with minimal traffic.

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.

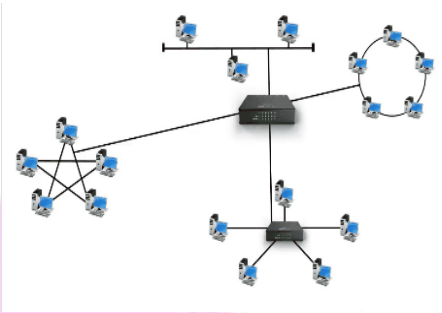
2. Switch

- 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.



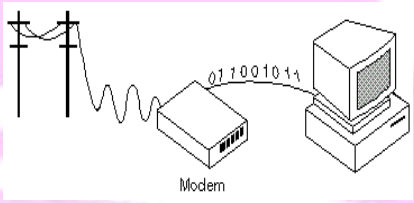
3. Router

- 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.



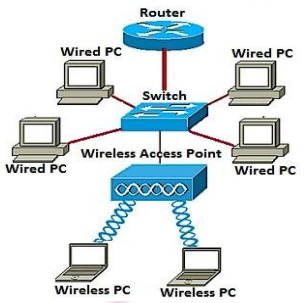
4. Modem

- 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.



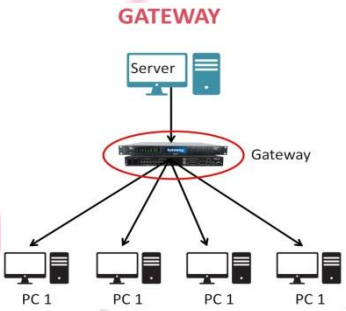
5. Access Point (AP)

- 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.



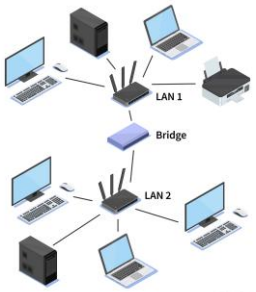
6. Gateway

- 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.



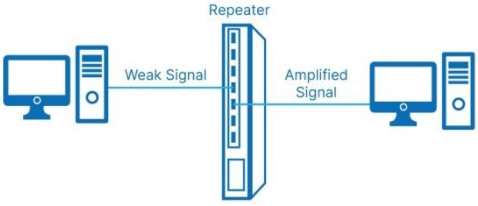
7. Bridge

- 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.



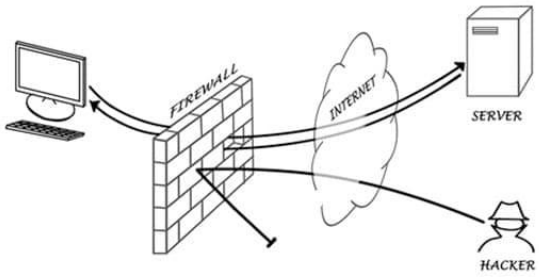
8. Repeater

- 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

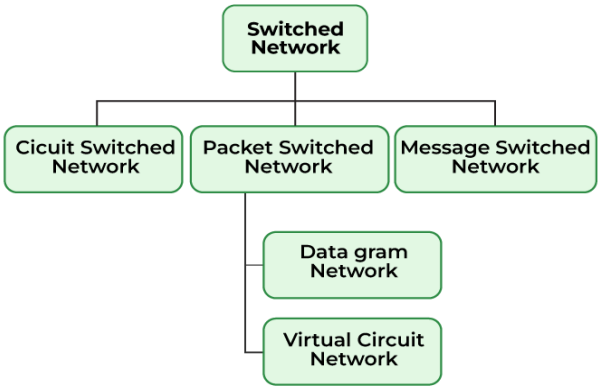
1. Traffic Filtering:
2. Access Control:
3. Packet Inspection:
4. Monitoring and Logging:
5. Protecting Against Attacks:

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

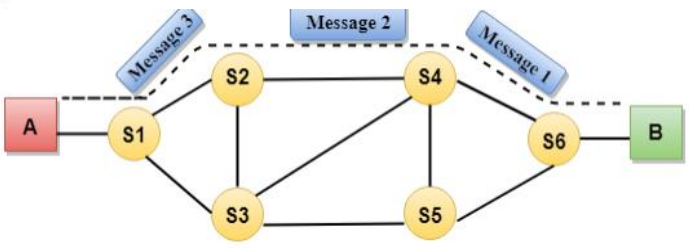
Switching techniques are the methods used to establish a path for data transmission between two points in a network. These techniques play a crucial role in ensuring efficient communication, especially in large and complex networks.



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.



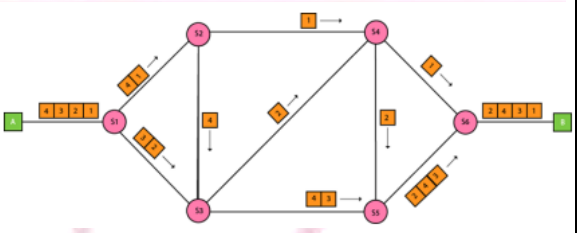
- Communication through circuit switching has 3 phases:
  1. **Circuit establishment**
  2. **Data transfer**
  3. **Circuit Disconnect Circuit**
- Example: Traditional Telephone Network: When you make a phone call, a circuit is established between your phone and the recipient's phone, and the entire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

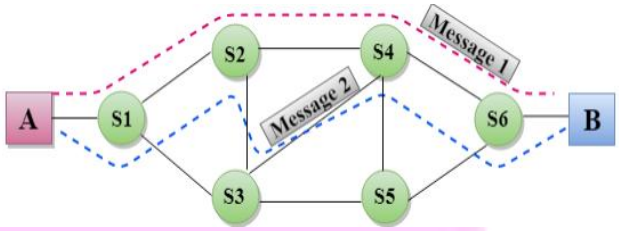
Virtual Circuit Switching: establishes a logical connection between the sender and receiver before transmitting data. Once the virtual circuit is set up, all packets follow the same predefined path.
Example: Telephone Networks (VoIP)

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:

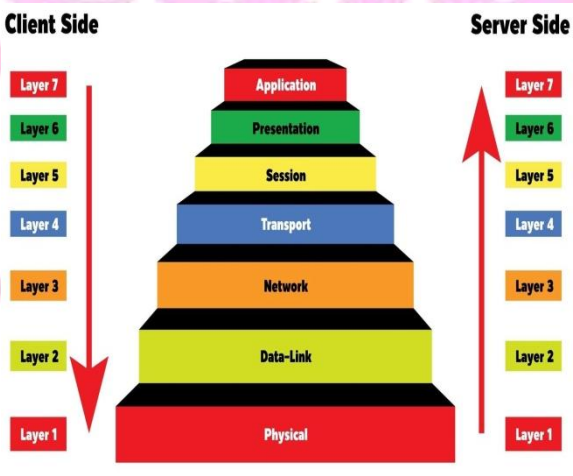
- No Dedicated Path: No need for a dedicated path to be reserved for communication, leading to better resource utilization.
- Efficient for Large Messages: Can handle large messages more efficiently than packet switching in some cases.

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

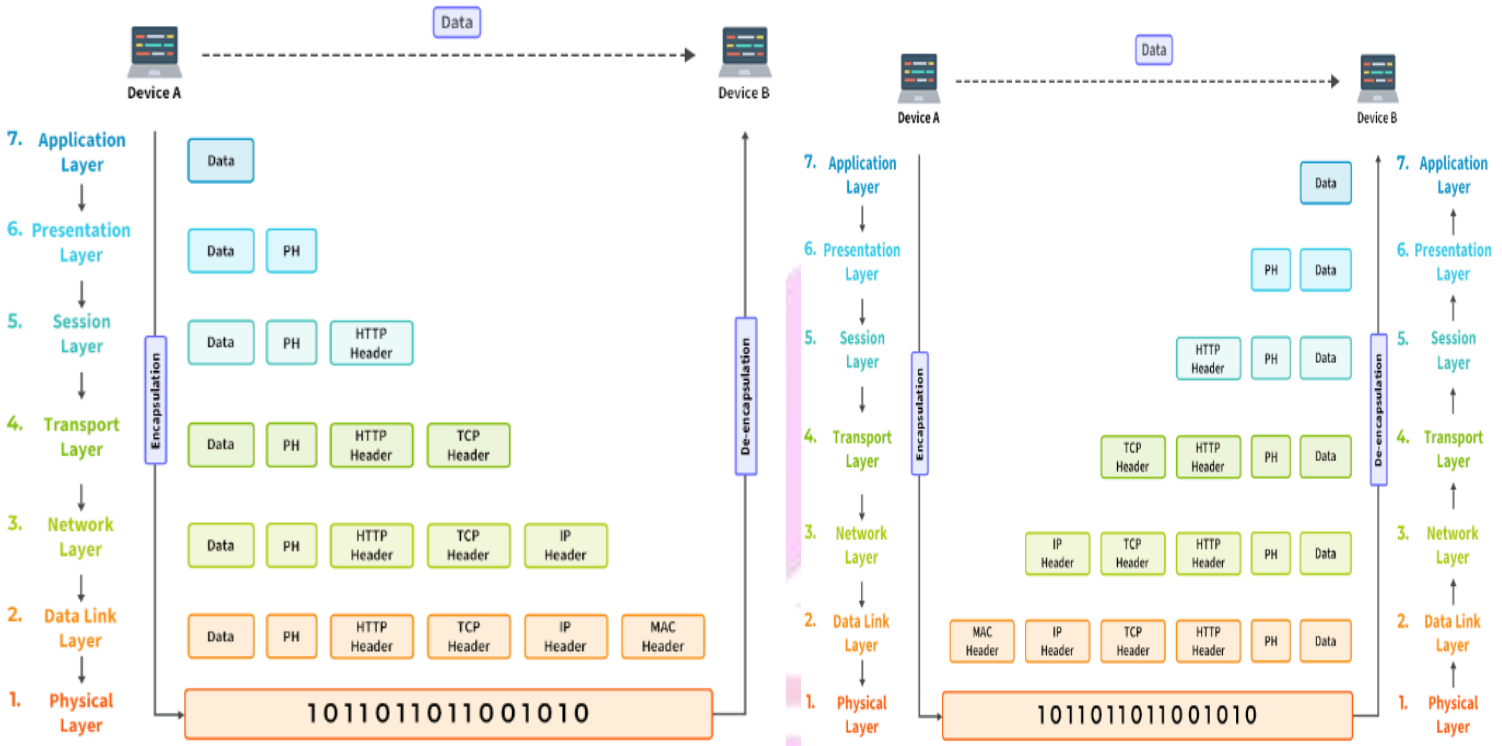
- The OSI (Open Systems Interconnection) Model is a conceptual or reference model that explains how different computer systems communicate over a network.
- OSI Model was developed by the International Organization for Standardization (ISO) in 1984.
- The OSI model creates a standard set of rules for 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

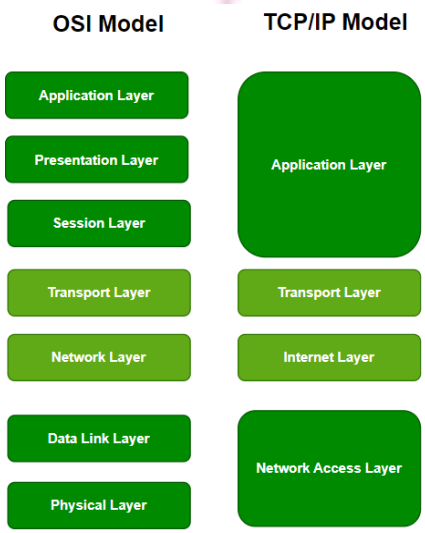


TCP/IP Model (Transmission Control Protocol/Internet Protocol Model)

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.

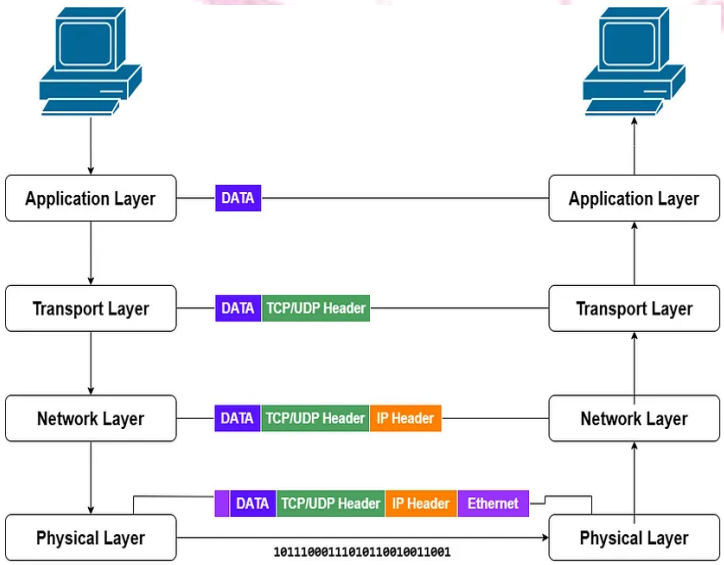
On the basis of OSI model TCP/IP model is implemented to communicate with different devices over the internet.

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



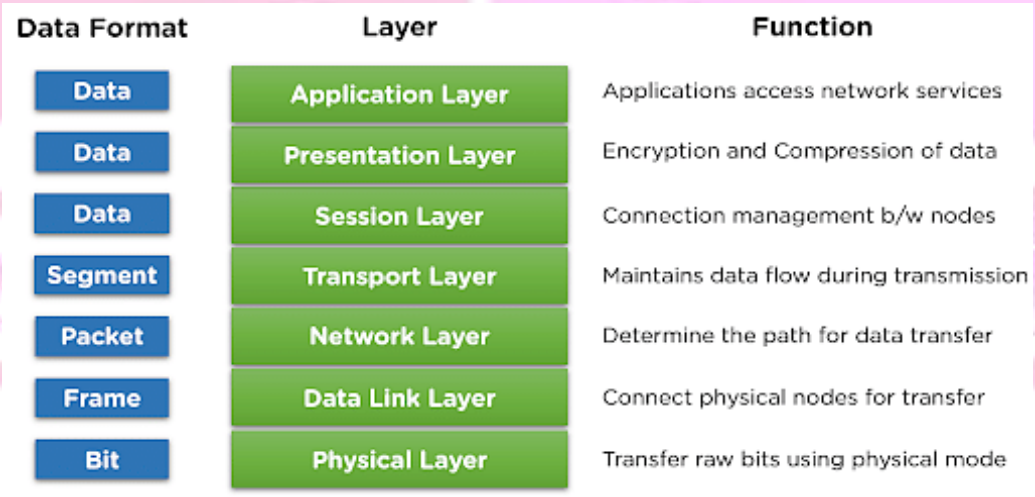
TCP/IP Model has 4 layers:

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.

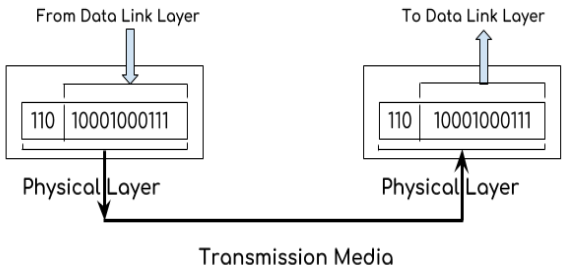
Responsibilities of the Physical Layer

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).

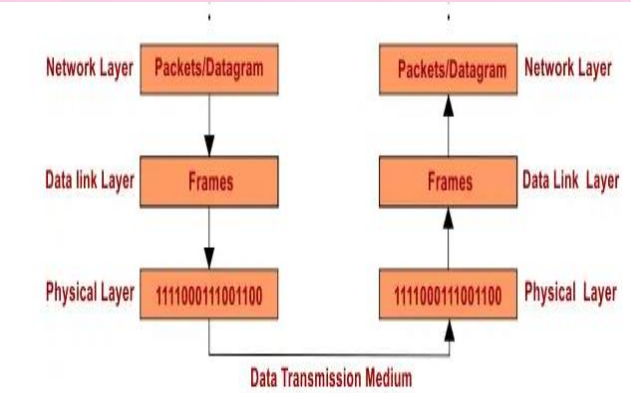
Challenges Addressed by the Physical Layer

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.



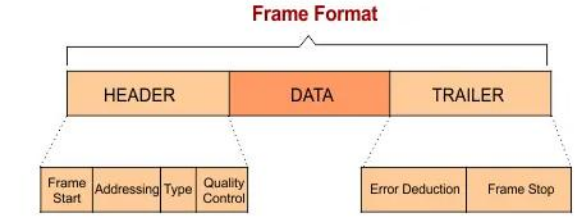
At Sender Side: Data link layer receives packets/datagram from network layer and convert these packets/datagrams to frames and transmit these frames to physical layer.

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.

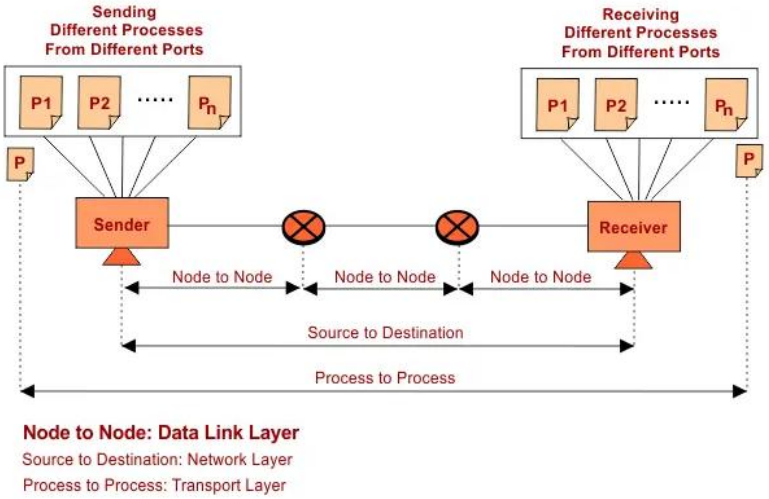


2. **Node to Node Connection:**

- 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.

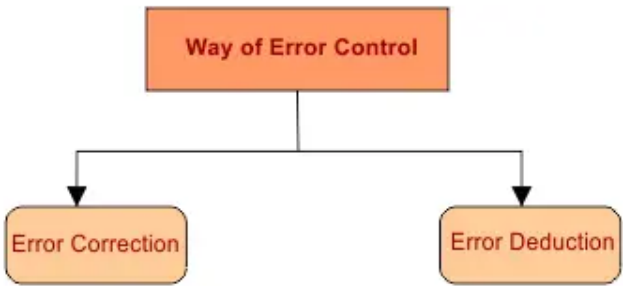
4. **Flow Control:**
   - Sometimes, one node has higher speed and capacity than other nodes. Then sending speed may be higher than receiver node. So, flow control comes into the picture.
   - Thus, data link layer control the flow of data node to node.
   - But the Transport layer deals with source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

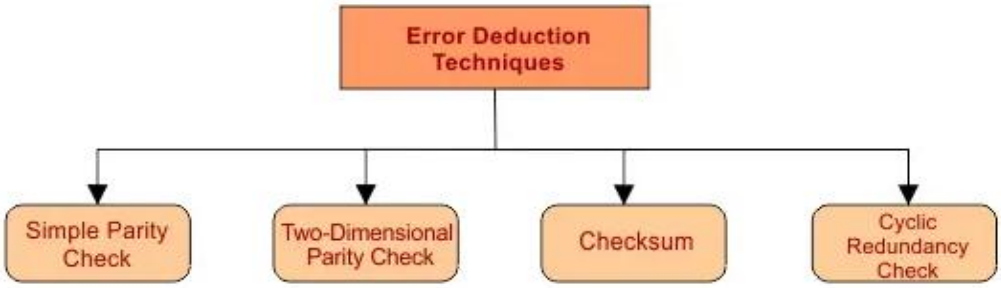
Types of Errors

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.

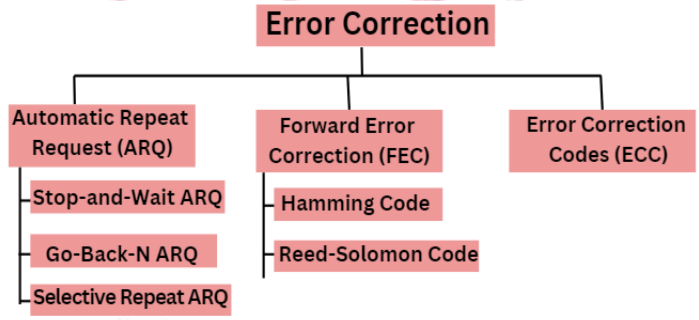
2. **Checksum:** Treats data as a sequence of integers. Calculates the sum of all integers and transmits it with the data. At the receiver, the sum is recalculated and compared with the received checksum.
This method uses a Checksum Generator on the sender side and a Checksum Checker on the receiver 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):

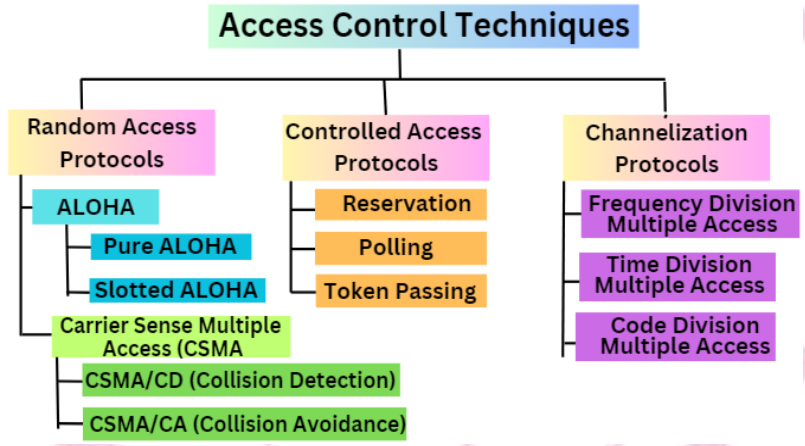
Codes like BCH (Bose–Chaudhuri–Hocquenghem) and LDPC (Low-Density Parity Check) are used in advanced communication systems like satellite and 5G networks.

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.

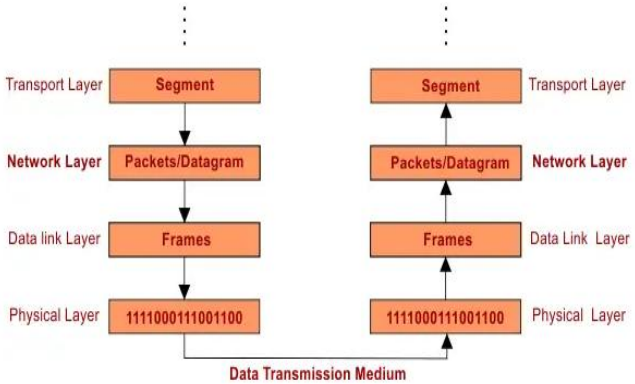
2. **Media Access Control (MAC):**
   - The second sublayer, Media Access Control, deals with the physical addressing of frames.
   - It encapsulates frames to prepare them for transmission, resolves situations that require more than one data frame transmission, and fixes collisions if they should occur.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

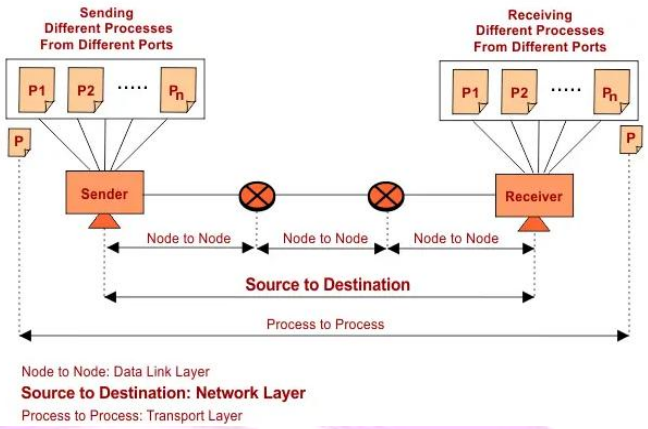
- The Network Layer is the third layer in the OSI model, positioned above the Data Link Layer and below the Transport Layer.
- Its primary role is to manage the delivery of data packets from the source to the destination, even across multiple networks.
- It is responsible for routing, addressing, and 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.

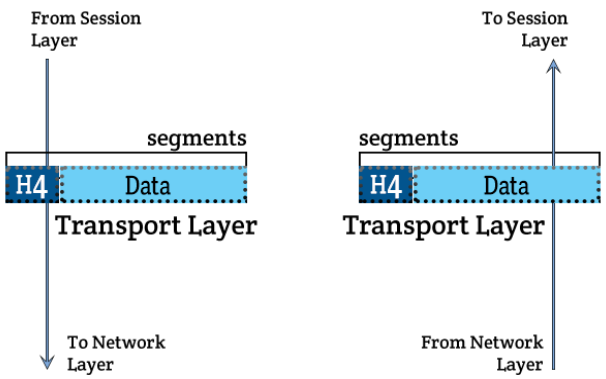
9. **IGMP (Internet Group Management Protocol)**
   - It manages multicast groups for one-to-many communication.
   - Used in video streaming or online gaming.
   - Example: Streaming live sports to multiple viewers.

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

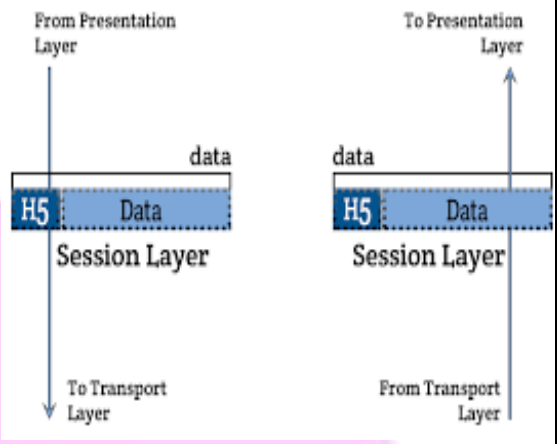
1. **Transmission Control Protocol (TCP):**
- Reliable, connection-oriented protocol.
- Ensures error checking, flow control, and retransmission of lost packets.
- Example: Web browsing (HTTP), email (SMTP), and file transfer (FTP) use TCP for reliable communication.

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.

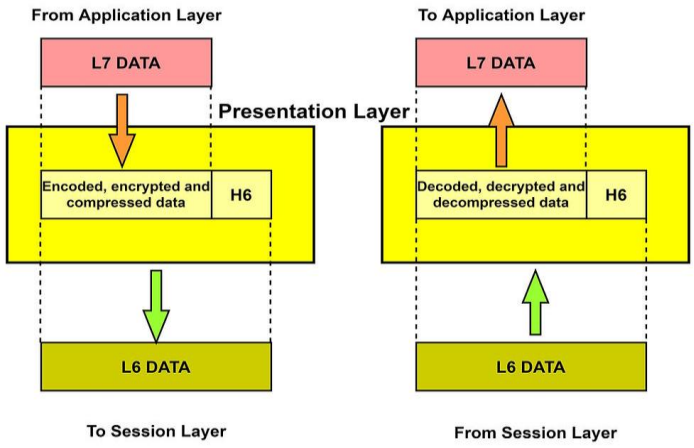
6. Presentation Layer

- 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.

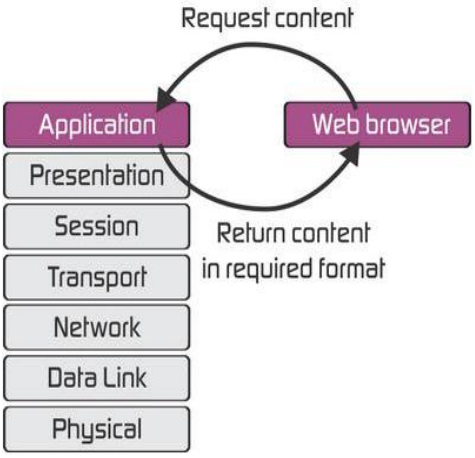
5. **Character Encoding:**
   - Handles character set conversions to ensure text data is displayed correctly across different systems.
   - Example: Converting Unicode to UTF-8.

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)

Used for transferring web pages from a web server to a browser.
HTTP: Sends data in plain text.
HTTPS: Secures data transmission using encryption (SSL/TLS).
Example: When you type www.google.com in your browser, HTTP/HTTPS fetches the web page from Google's server.
HTTPS ensures secure online shopping or banking by encrypting sensitive data like credit card details.

2. FTP (File Transfer Protocol)

Transfers large files between a client and a server.
Uses separate channels for data transfer (port 20) and control commands (port 21).
Example: Web developers use FTP to upload files to a website's server.
For instance, uploading a website's HTML files from a local machine to a hosting server.

3. SMTP (Simple Mail Transfer Protocol)

Sends emails from a client (e.g., Outlook) to a mail server.
Works with TCP to ensure reliable email delivery.
Example: When you send an email using Gmail, SMTP forwards the email to the recipient's mail server.

4. DNS (Domain Name System)

Translates human-readable domain names (e.g., www.google.com) into IP addresses (e.g., 142.250.190.14).
Example: When you enter www.youtube.com, DNS finds the corresponding IP address so your browser can load the website.

5. SNMP (Simple Network Management Protocol)

Monitors and manages devices on a network (e.g., routers, switches).
Example: A network administrator uses SNMP to check the health of devices in a company's network, such as monitoring the bandwidth usage of a router.

6. POP3 (Post Office Protocol v3)

Downloads emails from a mail server to a client and deletes them from the server.
Example: Using POP3, you can download all emails to your Outlook client, but those emails won't remain accessible from another device.

7. IMAP (Internet Message Access Protocol)

Allows accessing emails on a server while keeping them synchronized across multiple devices.
Example: With IMAP, you can read an email on your smartphone, and the same email remains available on your laptop or tablet.

8. Telnet and SSH

- **Telnet**:
  Provides remote access to a device over an unencrypted connection.
  Example: Using Telnet to access a server for configuration tasks (rarely used today due to lack of security).
- **SSH (Secure Shell)**:
  Provides secure, encrypted remote access to a device.
  Example: System administrators use SSH to manage cloud servers securely.

9. DHCP (Dynamic Host Configuration Protocol)

Automatically assigns IP addresses to devices on a network.
Example: When you connect your laptop to Wi-Fi, DHCP assigns an IP address without requiring manual configuration.

10. TFTP (Trivial File Transfer Protocol)

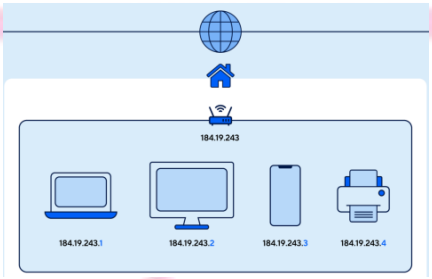
Transfers files without requiring authentication (simpler than FTP).
Example: Used in network devices like routers to transfer firmware updates or configuration files.

11. MIME (Multipurpose Internet Mail Extensions)

Extends email functionality to support multimedia content (e.g., images, videos, PDFs).
Example: When you attach a PDF file or an image to an email, MIME ensures the recipient's email client can interpret and display the attachment correctly.

IP address

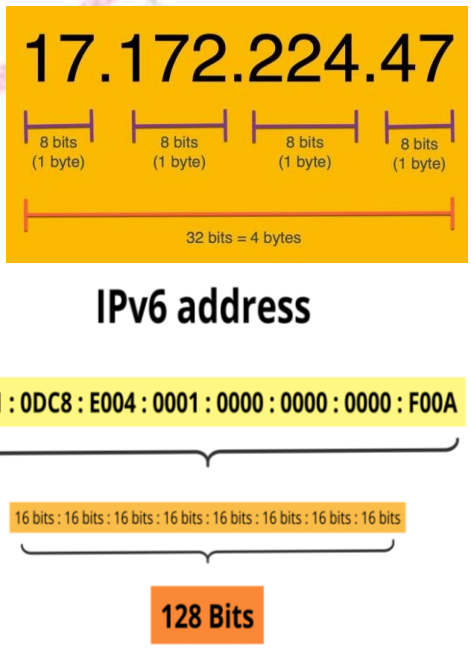
- An IP address (Internet Protocol address) is a unique identifier assigned to each device connected to a network, such as the internet.
- It allows devices to communicate with each other by specifying the source and destination of data packets.
- It is also called logical address.



Types of IP Addresses

1. **IPv4 (Internet Protocol Version 4):**
   Format: A 32-bit address, typically written as four decimal numbers (8 bit each) separated by dots (e.g., 192.168.1.1).
   Address Space: Approximately 4.3 billion unique addresses.

2. **IPv6 (Internet Protocol Version 6):**
   Format: A 128-bit address(divided in 8 part(16 bit each)), written in hexadecimal format, separated by colons
   (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
   Address Space: Virtually unlimited, designed to overcome IPv4 address exhaustion.



IPv4

- IPv4 stands for Internet Protocol Version 4, the fourth version of the Internet Protocol.
- It is a connectionless protocol used for identifying devices on a network through an addressing system.
- IPv4 is the most widely used protocol for communication over the internet.
- An IPv4 address is divided into 4 octets (8 bits each).
- Example: 192.168.1.1 (in binary: 11000000.10101000.00000001.00000001).

How IP Addresses Work

- Devices use IP addresses to send and receive data across the network.
- When you access a website, your device sends a request to the server's IP address. The server then sends the requested data back to your device's IP address.
- Routers and other network devices use IP addresses to forward packets to the correct destination.

Parts of IPv4

IPv4 addresses have three parts:

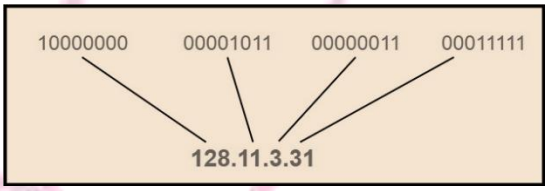
1. **Network Part:** Identifies the network and is the same for all devices in that network.'
2. **Host Part:** Uniquely identifies each device within the network.
3. **Subnet Number (Optional):** Used to divide large networks into smaller sections (subnets).

IPV4 addresses classified in 2 categories

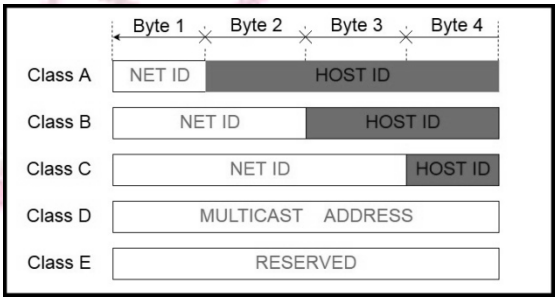
1. Classful addressing
2. Classless addressing

Classful addressing

- Classful addressing divides the IPv4 address space into five classes (A, B, C, D, and E), each designed for specific purposes.
- The classes are distinguished by the first few bits of the IP address and determine the size of the network and host portions.
- The class of IP address is used to determine the bits used for network ID and host ID and the number of total networks and hosts possible in that particular class.



- Each of these classes has a valid range of IP addresses. Classes D and E are reserved for multicast and experimental purposes respectively. The order of bits in the first octet determines the classes of the IP address.
- IP addresses are managed globally by the Internet Assigned Numbers Authority (IANA) and Regional Internet Registries (RIRs).
- When calculating the total number of host IP addresses in a network, 2 addresses are excluded:
  - The first address in a network is reserved as the network identifier.
  - The last address is reserved as the broadcast address.



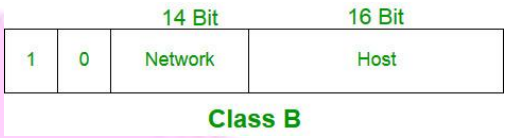
Class A

- Range: First octet 0 to 127.
- Binary Representation: First bit is always 0.
- Address Range: 0.0.0.0 to 127.255.255.255.
  Note: 127.x.x.x is reserved for loopback testing, so usable range is 1.0.0.0 to 126.255.255.255.
- Default Subnet Mask: 255.0.0.0.
- Network/Host: 8 bits for the network, 24 bits for the host.
- Number of Networks: $2^7-2=126$ (excluding reserved).
- Number of Hosts per Network: $2^{24}-2=16,777,214$ (excluding network and broadcast addresses).

- Use Case: Large organizations like ISPs.
- Example: 10.0.0.1.

Class B

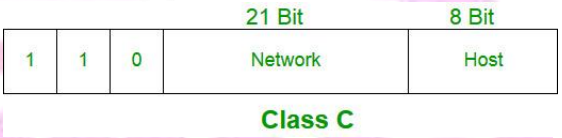
- Range: First octet 128 to 191.
- Binary Representation: First two bits are always 10.
- Address Range: 128.0.0.0 to 191.255.255.255.
- Subnet Mask: 255.255.0.0.
- Network/Host: 16 bits for the network, 16 bits for the host.
- Number of Networks: 2^{14}=16,384.
- Number of Hosts per Network: 2^{16}−2=65,534(excluding network and broadcast addresses)
- Use Case: Medium-sized networks like universities or large businesses.
- Example: 172.16.0.1.



Class B

Class C

- Range: First octet 192 to 223.
- Binary Representation: First three bits are always 110.
- Address Range: 192.0.0.0 to 223.255.255.255.
- Subnet Mask: 255.255.255.0.
- Network/Host: 24 bits for the network, 8 bits for the host.
- Number of Networks: 2^{21}=2,097,152.
- Number of Hosts per Network: 2^{8}−2=254 (excluding network and broadcast addresses)
- Use Case: Small networks like small businesses or home networks.
- Example: 192.168.1.1.



Class C

Class D

- Range: First octet 224 to 239.
- Binary Representation: First four bits are always 1110.
- Address Range: 224.0.0.0 to 239.255.255.255.
- Subnet Mask: Not applicable.
- Purpose: Reserved for multicast traffic (sending data to multiple devices).
- Use Case: Applications like video streaming and conferencing.
- Example: 224.0.0.1.

Class D

Class E

- Range: First octet 240 to 255.
- Binary Representation: First four bits are always 1111.
- Address Range: 240.0.0.0 to 255.255.255.255.
- Subnet Mask: Not applicable.
- Purpose: Reserved for research and experimental use.
- Use Case: Not used in general networking.
- Example: 250.1.2.3.

Class E

Special Addresses in IPv4 Classes

1. **Static IP Address:**
   - Manually assigned and remains constant over time.
   - Often used for servers or devices that need a permanent address.

2. **Dynamic IP Address:**
   - Assigned automatically by a Dynamic Host Configuration Protocol (DHCP) server.
   - Changes periodically (e.g., when a device reconnects to the network).

3. **Loopback Address:**
   - Used by a device to refer to itself for testing and troubleshooting purposes.
   - Used for testing and debugging within the same host.
   - Range: 127.0.0.0 to 127.255.255.255 (commonly 127.0.0.1)

4. **IP address 0.0.0.0:** Represents "any network" or an unknown network.
5. **Broadcast Address: 255.255.255.255**
   Used to send data to all devices in a network and also used in network discovery and announcements.
6. **Link-Local Address (APIPA - Automatic Private IP Addressing):**
   Automatically assigned when a device cannot obtain an IP address from a DHCP server.
   Enables communication between devices on the same local network when no DHCP is available.
   Range: 169.254.0.0 to 169.254.255.255.

7. **Reserved Private IP Ranges:**
   - Used within private networks (e.g., homes, offices) for internal communication.
   - Not routable on the internet.
   - Enables communication within a local network.
   - Devices in private networks use Network Address Translation (NAT) to access the internet.
   - Class A: 10.0.0.0 to 10.255.255.255
   - Class B: 172.16.0.0 to 172.31.255.255
   - Class C: 192.168.0.0 to 192.168.255.255

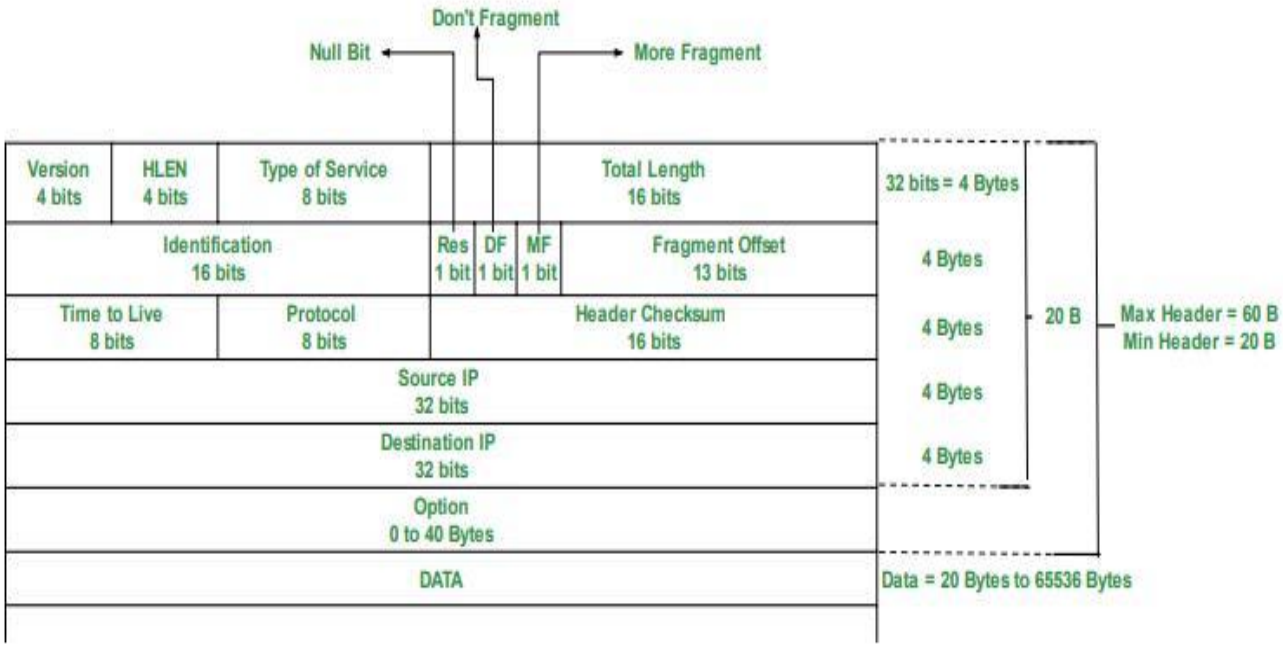
8. **Multicast Address**
   - Used to send data to multiple devices simultaneously within a group.
   - Range: 224.0.0.0 to 239.255.255.255 (Class D).
   - Streaming media, video conferencing, and routing protocols (e.g., OSPF, RIP).

CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

IPV4 Datagram header format

The IPv4 header is typically 20 bytes long but can grow up to 60 bytes if options are included.
It consists of multiple fields, each serving a specific function.

1. **Version (4 bits):** Indicates the version of the Internet Protocol. For IPv4, this field always contains 4 bits.
2. **Header Length (4 bits):** Specifies the length of the IPv4 header in 32-bit words. Since the minimum header size is 5 (20 bytes), this field indicates the number of 32-bit words in the header.
3. **Type of Service (8 bits):** Specifies the quality of service (QoS) and priority of the packet.
   - It is used for prioritizing traffic (e.g., low-latency or high-throughput).
   - 3 bits for precedence and 5 bits for TOS.
   - Precedence (3 bits): Priority of the packet.
   - TOS (5 bits): Specifies the desired service (e.g., delay, throughput, Cost, reliability).
4. **Total Length (16 bits):** Specifies the total length of the IP packet, including both the header and the data (payload). The maximum value is 65,535 bytes.
5. **Identification (16 bits):** A unique identifier for each packet sent from the source. It is used to reassemble fragmented packets. All fragments of a packet share the same identification number.
6. **Flags (3 bits):** These bits are used for controlling and identifying packet fragmentation.
   It contains three bits:
   Bit 0: Reserved (must be set to 0).
   Bit 1: "Don't Fragment" (DF) flag: If set, the packet cannot be fragmented.
   Bit 2: "More Fragments" (MF) flag: If set, more fragments follow.
7. **Fragment Offset (13 bits):** Specifies the position of the fragment in the original packet. It helps in reassembling fragmented packets. The offset is measured in 8-byte units.
8. **Time to Live (TTL) (8 bits):** Prevents packets from circulating indefinitely in the network. It specifies the maximum number of hops (routers) the packet can pass through. Each router decreases the TTL by 1.
9. **Protocol (8 bits):** This field indicates the type of protocol used in the data portion of the packet, such as 6- TCP, 17-UDP, 1- ICMP, or others.
10. **Header Checksum (16 bits):** A checksum used for error-checking the header. It ensures the integrity of the header data. If the checksum is incorrect, the packet is discarded.
11. **Source IP Address (32 bits):** The 32-bit IP address of the sender (source) of the packet.
12. **Destination IP Address (32 bits):** This field holds the IP address of the recipient or destination of the packet.
13. **Options (Variable):-** Optional field that can be used for various purposes like security, timestamp, routing, etc. This field is rarely used.
14. **Padding (Variable):-** This field ensures that the IPv4 header length is a multiple of 32 bits. It is used to align the header if the options field is used.



Problems in IPv4 Classful Addressing

Classful addressing was the initial method for allocating IP addresses, but it has several limitations:

1. **Wastage of IP Addresses:**
- Classful addressing allocates a fixed number of IP addresses based on the class. For example, a Class A network provides over 16 million addresses, even if an organization only needs 10,000. The remaining addresses go unused, leading to inefficient utilization.
- **Example:** A company needing 10,000 addresses must use Class A (16 million addresses) or Class B (65,536 addresses), wasting a large portion of the allocated space.

2. **Limited Number of Networks:**
- Class A and B networks have a limited number of network IDs. Class A has only 128 network IDs, and Class B has 16,384. These are insufficient for large organizations or ISPs, forcing smaller organizations to use Class C, which can only support up to 254 hosts.
- **Example:** If a large ISP needs more than 16,384 networks, Class B addresses may run out, leading to a shortage for other users.

3. **Inflexible Addressing:**
- Fixed boundaries of Class A, B, and C make it hard to meet diverse network size requirements. Small networks might need more than 254 addresses (Class C) but fewer than 65,536 (Class B). This lack of flexibility forces organizations to either waste addresses or manage multiple smaller networks.
- Example: A university needing 1,000 IPs cannot use Class C and must upgrade to Class B, wasting over 64,000 addresses.

4. **Routing Inefficiency:**
- Classful addressing does not support route aggregation, leading to large routing tables in routers. This increases memory usage and slows down data forwarding.
- Example: A router managing multiple Class C networks (e.g., 192.168.0.0, 192.168.1.0, 192.168.2.0) must maintain separate routes for each network, instead of aggregating them.

5. **Address Exhaustion:**
- The rigid allocation of IPv4 addresses, combined with their limited 32-bit space, led to rapid depletion. As more devices connect to the internet, the remaining addresses are insufficient.
- Example: By the late 2000s, IPv4 addresses were nearly exhausted due to the rapid growth of internet-connected devices like smartphones and IoT devices.

Solution

- CIDR (Classless Inter-Domain Routing) allows flexible allocation of IP addresses by removing fixed class boundaries.
- IPv6 was introduced to provide a larger address space and address these limitations.

Classless Addressing

- Classless Inter-Domain Routing (CIDR) was introduced in 1993 to replace classful addressing.
- CIDR is a method for efficiently assigning IP addresses and routing data. Unlike classful addressing, which uses fixed classes (A, B, C), CIDR allows for flexible subnetting with variable-length subnet masks (VLSM).
- This means networks can be divided into smaller, more suitable subnets based on actual needs, rather than being limited by rigid class boundaries.

CIDR Notation

- CIDR notation combines the IP address with a subnet mask, written as IP_address/Prefix_Length. The prefix length specifies the number of bits used for the network portion of the address.
- **Example:** 192.168.10.0/24 means the first 24 bits are used for the network portion, leaving 8 bits for the host portion. This represents a network with 256 IP addresses (192.168.10.0 to 192.168.10.255).

Efficient Use of Address Space:

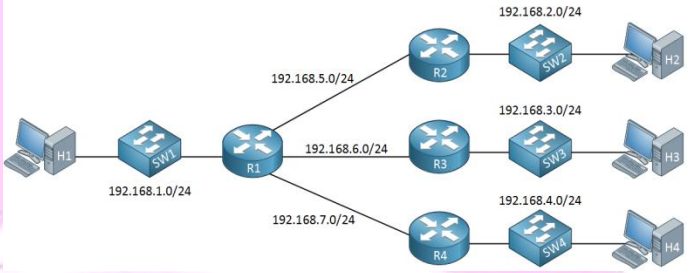
- CIDR allows IP address blocks to be assigned in more precise sizes, reducing wastage of IP addresses. It enables more efficient use of the available address space.
- Example: A network that needs only 500 addresses can be assigned a block like 192.168.10.0/23, which provides 512 addresses (from 192.168.10.0 to 192.168.11.255), instead of wasting a larger block like 192.168.0.0/22 (which provides 1,024 addresses).

Route Aggregation (Supernetting):

- CIDR allows route aggregation, where multiple IP address ranges (previously treated as separate networks in classful addressing) can be grouped into a single route. This reduces the size of routing tables, improving routing efficiency.
- Example: Instead of having separate routes for 192.168.0.0/24, 192.168.1.0/24, and 192.168.2.0/24, CIDR allows them to be aggregated into one route, such as 192.168.0.0/22, covering all three networks.

Subnetting

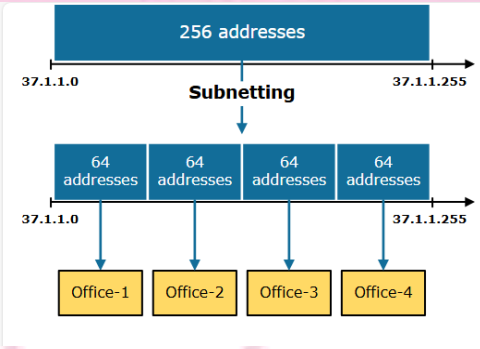
- Subnetting is the process of dividing a larger network into smaller, more manageable sub-networks, called subnets.
- This is done to improve network performance, security, and organization. Subnetting allows an organization to use its IP address space more efficiently, create smaller broadcast domains, and manage traffic better.



Key Concepts in Subnetting:

1. **IP Address Structure:**
   An IP address is made up of two parts:
   - ✓ **Network Part:** Identifies the network.
   - ✓ **Host Part:** Identifies the specific device (host) on the network.

   Subnetting divides the host part of an IP address into additional subnets, creating smaller networks within the larger one.

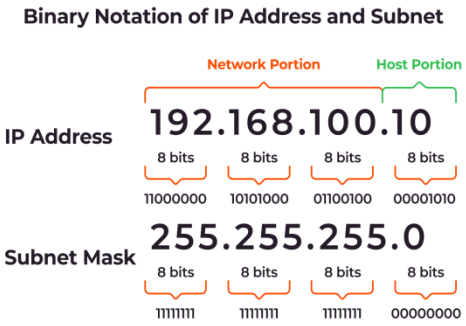


2. **Subnet Mask:**
   A subnet mask is used to define the size of the network and the host portion of an IP address. It is a 32-bit number that "masks" the network portion of the address and allows the router to differentiate between the network and host portions.
   Example: A common subnet mask for a small network is 255.255.255.0 (or /24 in CIDR notation), where the first 24 bits represent the network, and the remaining 8 bits are for hosts.

Steps in Subnetting:

1. Determine the Network Requirements:
   - How many subnets are needed?
   - How many hosts are needed in each subnet?

   Based on these requirements, you can calculate the subnet mask and the number of subnets.



1. **Calculate the Subnet Mask:**
   The subnet mask is determined by borrowing bits from the host portion of the IP address. The more bits borrowed, the more subnets you can create, but fewer hosts will be available in each subnet.

   Formula:
   Number of Subnets = 2^n,
   where n is the number of bits borrowed from the host portion.

2. **Find the Number of Hosts per Subnet:**
   After borrowing bits for the subnets, the remaining bits are used for hosts.
   The formula for the number of hosts is:

   Number of Hosts = 2^h - 2,

   where h is the number of bits left for hosts.
   The subtraction of 2 accounts for the network address and the broadcast address, which cannot be assigned to hosts.

Example of Subnetting:

Suppose we have the network 196.16.12.0 and we want to create 2 subnets.

Solution:

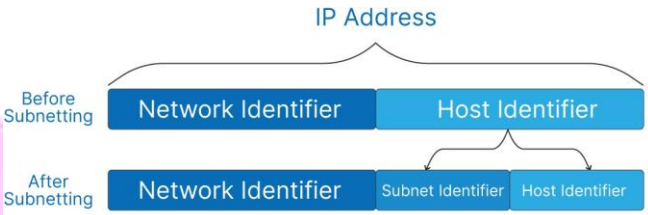
This is class C network so Subnet mask: 255.255.255.0**.**

This network has 256 possible host addresses, from 196.16.12.0 to 196.16.12.255.

Network Id of network: 196.16.12.0

Broadcast Id of network: 196.16.12.255

Divide this network into two smaller subnets, each with 128 host addresses.

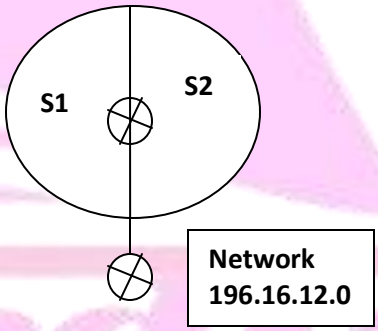


For example: you could use the subnet mask 255.255.255.0, which would give you two subnets with 128 host addresses each:

- **Subnet 1: 196.16.12.0 – 192.168.1.127**
  Network Id of subnet1: 196.16.12.0
  Broadcast Id of subnet1: 196.16.12.127

- **Subnet 2: 192.168.1.128 – 192.168.1.255**
  Network Id of subnet1: 196.16.12.128
  Broadcast Id of subnet1: 196.16.12.255

- **Subnet mask for internal network: 255.255.255.128**



You can also create additional subnets by using a different subnet mask. For example, you could use a subnet mask of 255.255.255.128

Some Values Calculated in Subnetting:

1. Number of subnets : 2(Given bits for mask – No. of bits in default mask)
2. Subnet address : AND result of subnet mask and the given IP address
3. Broadcast address : By putting the host bits as 1 and retaining the network bits as in the IP address
4. Number of hosts per subnet : 2(32 – Given bits for mask) – 2
5. First Host ID : Subnet address + 1 (adding one to the binary representation of the subnet address)
6. Last Host ID : Subnet address + Number of Hosts

Variable Length Subnet Mask

VLSM (Variable Length Subnet Mask) is a technique used in IP networking to divide an IP address space into subnets of different sizes. In traditional subnetting, all subnets within a network have the same size, meaning some subnets may have more addresses than they need, while others may not have enough.

VLSM solves this problem by allowing different subnets to have different sizes, ensuring that IP addresses are used more efficiently.

Working of VLSM

1. **Start with a Network Address:**
   You begin with a network address and a subnet mask (e.g., 192.168.1.0/24). The /24 means that the first 24 bits are for the network portion, and the remaining 8 bits are for hosts.

2. **Divide the Network into Subnets:**
   With VLSM, you can create subnets of varying sizes. For example, if you need a subnet for 30 hosts and another for 100 hosts, you can allocate a subnet mask that fits the specific requirements of each.

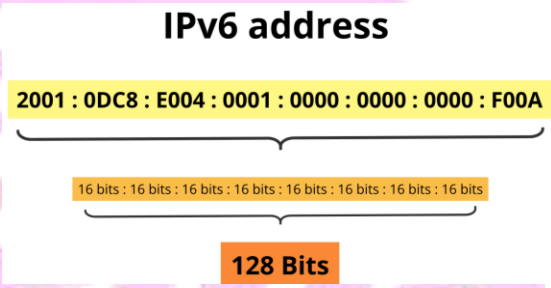
3. **Use Different Subnet Masks:**
   For the subnet with 100 hosts, you might need a /25 subnet mask (which provides 126 usable host addresses), and for the subnet with 30 hosts, you might use a /27 subnet mask (which provides 30 usable host addresses).

Characteristics of IPv4:

- IPv4 is a 32-bit IP address.
- It is a numeric address with bits separated by dots.
- The header contains 12 fields, and its length is 20 bytes.
- IPv4 supports unicast, broadcast, and multicast addressing.
- It allows Virtual Length Subnet Mask (VLSM).
- IPv4 uses the Address Resolution Protocol (ARP) to map IP addresses to MAC addresses.
- The RIP routing protocol is supported by the routed daemon.
- Networks can be configured manually or using DHCP.
- Packet fragmentation is handled by routers and may require reassembly by the host.

IPV6

- In July 1999, the Internet Assigned Numbers Authority (IANA) assigned IPv6 address blocks to the Regional Internet Registries (RIRs).
- Ratification: IPv6 was ratified as an internet standard in July 2017.
- IPv6 uses 128-bit addresses, which theoretically allows for 3.4 x 10^{38} unique IP addresses.



IPv6 Address Format:

An IPv6 address is written as 8 groups of 4 hexadecimal digits, separated by colons.

For example:

2001:0db8:85a3:0000:0000:8a2e:0370:7334

Hexadecimal Notation:

Each group of 4 digits represents 16 bits (or 2 bytes). Since there are 8 groups, the total length of the IPv6 address is 128 bits.

Leading Zero Compression (abbreviation):

Leading zeros in each group can be omitted for simplicity. For example, 0000 can be written as 0, so the address could be simplified to:

2001:db8:85a3::8a2e:370:7334

Double Colon (::): A double colon is used to represent consecutive groups of zeros. This can only be used once in an address to avoid ambiguity.

Example1: AF02::2

AF02:0:0:0:0:0:0:2 – The address after removing the abbreviated double-colon

AF02:0000:0000:0000:0000:0000:0000:0002 – The address after adding leading zeros

So the full address of the abbreviated address AF02::2 is

AF02:0000:0000:0000:0000:0000:0000:0002.

Example2: A0EC:0342:0000:0000:0000:C2E0:0000:FDE0

Omitting leading zero :

A0EC:342:0:0:0:C2E0:0:FDE0

Use double colon for consecutive zeros:

A0EC:342::C2E0:0:FDE0

Features of IPv6

1. **Larger Address Space:**
   IPv6 uses 128-bit addresses, which allows for a vastly larger address space compared to IPv4's 32-bit addresses.

2. **Simplified Header Format:**
   The IPv6 header is design00ed to be simpler and more efficient than IPv4. Some fields in the IPv4 header, like the checksum, are removed to streamline processing. This leads to better routing and faster packet processing.

3. **Improved Security:**
   IPv6 was designed with security in mind. It includes mandatory support for IPsec (Internet Protocol Security), which ensures encrypted communication between devices, helping prevent eavesdropping and data tampering.

4. **Autoconfiguration:**
   IPv6 devices can automatically configure their own IP address using stateless address autoconfiguration (SLAAC). This allows devices to join a network and communicate without needing a DHCP server.

5. **Better Multicast Support:**
   IPv6 has improved multicast capabilities, which allows efficient one-to-many communication (e.g., video streaming or conferencing) without broadcasting to all devices in a network.

6. **No Need for NAT (Network Address Translation):**
   With IPv6, each device can have its own unique global IP address, eliminating the need for NAT, which is commonly used in IPv4 to conserve address space.

7. **Dual Stack:**
   Dual Stack allows devices and networks to run both IPv4 and IPv6 simultaneously. A device configured with dual stack can use IPv4 or IPv6 depending on the communication requirements. Devices prefer IPv6 when available but fall back to IPv4 if needed.

8. **Tunneling:**
   Tunneling allows IPv6 packets to be sent over an existing IPv4 network by encapsulating IPv6 packets inside IPv4 packets. The IPv6 packet is wrapped with an IPv4 header. At the destination, the IPv4 header is removed, and the IPv6 packet is processed.

Types of IPV6

IPv6 addresses are categorized into three main types based on their functionality and usage.

1. **Unicast Address**
2. **Multicast Address**
3. **Anycast Address**

1. **Unicast Address**

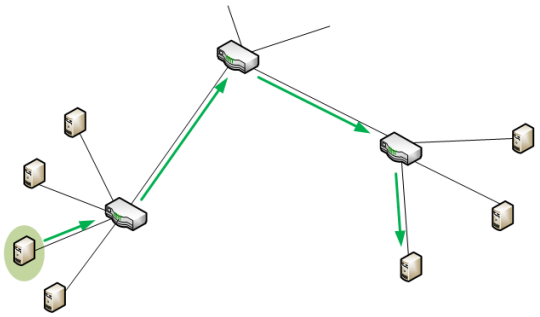
Used for one-to-one communication, where data is sent to a single, specific device.

Types of Unicast Addresses:

Global Unicast: Public addresses routable on the global internet (similar to IPv4 public addresses).Its high level 3 bits are fixed as 001

Prefix: 2000::/3

Example: 2001:db8::1



Link-Local: Used for communication within the local network (not routable beyond the link).
Prefix: fe80::/10
Example: fe80::1

Unique Local (ULA): Private addresses used within an organization (not routable on the internet).
Prefix: fc00::/7
Example: fd00::1

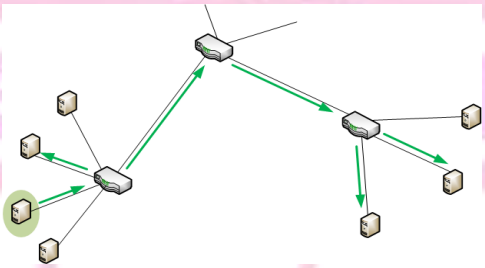
Loopback: Used for internal testing within a single device.
Address: ::1
Unspecified Address: Indicates the absence of an address 0:0:0:0:0:0:0:0 .
Address: ::

Example:
A server with a Global Unicast address (2001:db8::10) can communicate over the internet.
Devices in the same network use Link-Local addresses (fe80::1).

2. Multicast Address

Used for one-to-many communication, where data is sent to multiple devices in a group.
Prefix: ff00::/8
Multicast addresses have different scopes that define their reach:

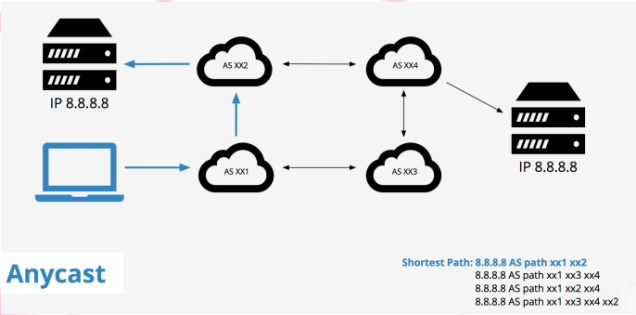
- Link-Local: ff02::1 (all nodes on the local link)
- Site-Local: ff05::1 (nodes within a site)
- Global: ff0e:: (globally routable multicast group)



Example:
ff02::1 is used to send data to all devices on the local link.

3. Anycast Address

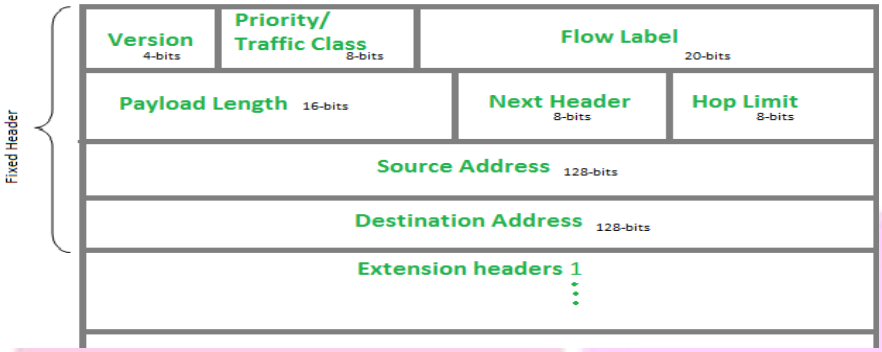
- Used for one-to-nearest communication, where data is sent to the nearest device (in terms of routing distance) among multiple devices with the same address.
- Commonly used for load balancing and services like DNS.
- Example: A DNS query sent to an Anycast address will reach the nearest DNS server.



Address Type	Purpose	Prefix/Example
Unicast	One-to-one communication	2001:db8::1, fe80::1
Multicast	One-to-many communication	ff02::1, ff05::1
Anycast	One-to-nearest communication	Shared among multiple devices

IPV6 Header Format

The IPv6 header is 40 bytes in size, unlike IPv4 where the header size can vary.



IPv6 Header Fields

1. **Version (4 bits):** Specifies the IP version. For IPv6, the value is always 6.
2. **Traffic Class (8 bits):** Used to identify and prioritize different types of traffic (similar to the Type of Service field in IPv4). Helps in implementing Quality of Service (QoS).
3. **Flow Label (20 bits):** Used to identify and manage specific traffic flows. Useful for applications that require real-time data, such as video streaming or VoIP.Routers use this field to handle packets belonging to the same flow efficiently.
4. **Payload Length (16 bits):** Indicates the size of the data (payload) in bytes that follows the header. Maximum value is 65,535 bytes.
5. **Next Header (8 bits):** Specifies the type of header that follows the IPv6 header. It can be a transport-layer protocol (e.g., TCP, UDP) or an extension header (like fragmentation or routing headers).
   Examples: 6 for TCP, 17 for UDP, 58 for ICMPv6
6. **Hop Limit (8 bits):** Similar to the TTL (Time to Live) field in IPv4. Specifies the maximum number of hops (routers) the packet can travel before being discarded. Each router decreases the hop limit by 1. When it reaches 0, the packet is dropped.
7. **Source Address (128 bits):** Specifies the IPv6 address of the sender. Example: 2001:db8::1.
8. **Destination Address (128 bits):** Specifies the IPv6 address of the intended recipient.
   Example: 2001:db8::2.

comparison between IPv4 and IPv6

Feature	IPv4	IPv6
Address Size	32-bit address	128-bit address
Address Format	Numeric, written in decimal, separated by dots (e.g., 192.168.1.1)	Alphanumeric, written in hexadecimal, separated by colons (e.g., 2001:0db8::1)
Address Space	4.3 billion (2^{32} addresses)	Vast, approximately 340 undecillion (2^{128} addresses)
Header Size	Variable (20-60 bytes)	Fixed (40 bytes)
Header Fields	12 fields	8 fields (simplified for efficiency)
Fragmentation	Performed by sender and routers	Performed only by the sender
Checksum	Present in the header	Removed to simplify processing
Routing Efficiency	Less efficient due to complex headers	More efficient with simplified headers
Security	Optional (IPSec is not mandatory)	Built-in security with mandatory IPSec
Address Configuration	Manual (Static) or DHCP	Automatic using Stateless Address Autoconfiguration (SLAAC) or DHCPv6
Broadcast	Supports broadcast communication	No broadcast; uses multicast instead
Multicast Support	Supported	Supported and improved
Quality of Service (QoS)	Limited support via Type of Service (ToS)	Improved with Traffic Class and Flow Label fields
NAT (Network Address Translation)	Widely used due to address exhaustion	Not required (sufficient addresses)
Mobility	Limited	Improved mobility and routing

Packet Size	576 bytes (minimum)	1280 bytes (minimum)
Compatibility	Works with IPv4-only devices	Backward compatible using transition mechanisms (e.g., Dual Stack, Tunneling)
Example Address	192.168.1.1	2001:0db8:85a3::8a2e:0370:7334
Usage	Still widely used	Gradually being adopted globally

Routing Concepts

- Routing is the process of selecting the best path for data packets to travel from the source to the destination across a network.
- It involves routing algorithms and routing protocols that determine the most efficient path.

1. Static Routing vs Dynamic Routing

Feature	Static Routing	Dynamic Routing
Definition	Routes are manually configured by the network administrator.	Routes are learned and updated automatically using routing protocols.
Configuration	Manual (fixed routes).	Automatic (adaptive to network changes).
Scalability	Suitable for small networks.	Suitable for large, complex networks.
Maintenance	Requires manual changes when topology changes.	Automatically adjusts to topology changes.
Bandwidth Usage	No bandwidth is used for routing updates.	Consumes bandwidth for routing updates.
Example	Used in small office networks.	Used in enterprise-level networks.

2. Routing Algorithms

Routing algorithms are used to determine the best path for data to travel. The two main types of routing algorithms are:

1. **Distance Vector Routing Algorithm:**
   Distance Vector Routing calculates the best path based on the distance (hop count) to the destination. Each router shares its routing table with its directly connected neighbors.
2. **Link State Routing Algorithm:**
   Link State Routing calculates the best path based on the state (cost, bandwidth, delay) of the links in the network. Routers have a complete view of the network topology.

3. Routing Protocols

Routing protocols are rules that routers use to communicate and share routing information. The three main routing protocols are:

1. **RIP (Routing Information Protocol):**
   - It is a Distance Vector Routing Protocol.
   - In a small network, RIP calculates the shortest path based on hop count. If a path has fewer hops, it is preferred.
2. **OSPF (Open Shortest Path First)**
   - It is a Link State Routing Protocol.
   - If there are two paths to a destination:
   - Path 1: 100 Mbps (cost = 1) & Path 2: 10 Mbps (cost = 10)
     OSPF selects Path 1 as it has a lower cost.
3. **BGP (Border Gateway Protocol)**
   - Path Vector Routing Protocol (used for inter-domain routing).
   - Used to connect different autonomous systems (AS) on the Internet.
   - When traffic needs to move between two ISPs, BGP determines the best path based on attributes like shortest AS path or preferred policy.

Some Important Terms in Networking

1. Port

- A port is a 16 bit logical endpoint used to identify specific processes or services running on a device.
- Ports are associated with IP addresses to allow communication between applications over a network.
- Ports are identified using port numbers (ranging from 0 to 65535).

Types of Ports:

1. **Well-Known Ports (0–1023):** Reserved for standard protocols (e.g., HTTP - Port 80, FTP - Port 21).
2. **Registered Ports (1024–49151):** Assigned for user-defined applications.
3. **Dynamic/Private Ports (49152–65535):** Used temporarily by client applications.

Example:

- Port 80 is used for HTTP communication.
- Port 443 is used for HTTPS communication.

Commonly Used Port Numbers

Port Number	Protocol/Service	Description
20	FTP (Data)	File Transfer Protocol - Data Transfer
21	FTP (Control)	File Transfer Protocol - Control Commands
22	SSH	Secure Shell for secure remote administration
23	Telnet	Remote login service (insecure)
25	SMTP	Simple Mail Transfer Protocol (Email sending)
53	DNS	Domain Name System - Translates domain names
67/68	DHCP	Dynamic Host Configuration Protocol
69	TFTP	Trivial File Transfer Protocol (simplified FTP)
80	HTTP	Hypertext Transfer Protocol (Web traffic)
110	POP3	Post Office Protocol v3 (Email retrieval)
143	IMAP	Internet Message Access Protocol (Email)
161/162	SNMP	Simple Network Management Protocol
443	HTTPS	Secure HTTP (Web traffic over SSL/TLS)
8080	HTTP Proxy	Alternate port for HTTP

2. Socket

- A socket is a combination of an IP address and a port number.
- It is a software structure that acts as an interface for sending and receiving data.
- Sockets enable communication between applications running on the same or different devices.

Example: Suppose a client application with IP 192.168.1.2 communicates with a server on IP 192.168.1.10 using port 80.
Client Socket: 192.168.1.2:45678 (random port assigned)
Server Socket: 192.168.1.10:80
The combination of IP and port ensures data reaches the correct application.

3. Bandwidth:

- Bandwidth is the maximum amount of data that can be transmitted over a communication channel in a given amount of time.
- It is measured in Hertz (Hz) for analog signals and bits per second (bps) for digital signals.
- **Example:** A network with a bandwidth of 10 Mbps can transmit a maximum of 10 megabits of data per second.

4. Data Rate:

- Data rate refers to the speed at which data is transmitted over a network. It is measured in bits per second (bps).
- Data rate depends on the bandwidth and the quality of the communication channel.
- Example: If a file size is 1 MB (8 megabits), and the data rate is 8 Mbps, it will take 1 second to transfer the file.

5. Noise:

- Noise is any unwanted signal that interferes with the transmission of data over a communication channel.
- Noise reduces the quality of the signal and can cause errors in data transmission.

Types of Noise:

1. Thermal Noise: Caused by the random motion of electrons in a conductor.
2. Intermodulation Noise: Occurs when multiple signals mix and interfere with each other.
3. Crosstalk: Interference between adjacent wires or cables.
4. Impulse Noise: Caused by sudden disturbances like lightning or switching.

6. Attenuation:

- Attenuation is the gradual loss of signal strength as it travels over a distance.
- It occurs due to the resistance of the medium.
- Solution: Use amplifiers or repeaters to boost the signal strength.
- Example: A signal sent over a 100-meter cable may lose power and become weak by the time it reaches the other end.

7. Distortion:

- Distortion occurs when the signal changes its shape or form as it travels through the medium.
- It happens because different frequencies of a signal travel at different speeds.
- Use equalizers to correct the signal.
- Example: In a digital signal, if the original square wave gets rounded or delayed, it causes distortion.

8. Bit Rate

- Bit rate is the number of bits transmitted per second in a communication channel.
- It is measured in bits per second (bps).
- Bit rate depends on the data rate and the encoding technique used.
- Example: A data rate of 1000 bits per second (bps) means 1000 bits are transmitted in one second.

9. Baud Rate

- Baud rate is the number of signal changes (symbols) per second in a communication channel.
- Each signal change (symbol) can represent one or more bits, depending on the encoding scheme.
- Relationship Between Bit Rate and Baud Rate:
- Bit Rate = Baud Rate × Number of Bits per Symbol
- Example: If a system transmits 1000 symbols per second and each symbol represents 2 bits, then:

  Bit Rate = 1000 × 2 = 2000 bps

  Here, the baud rate is 1000 baud and the bit rate is 2000 bps.

10. Network Troubleshooting Tools

a. Ping:

- Ping is used to check the connectivity between two devices on a network.
- Example: ping 192.168.1.1

  This checks if the device with IP 192.168.1.1 is reachable.

b. Traceroute

- Traceroute is used to determine the path packets take from the source to the destination device.
- Example: traceroute google.com

  This shows the route taken to reach google.com.

c. Netstat

- Netstat (Network Statistics) displays active network connections, listening ports, and network statistics.
- Example: netstat -an

  Displays all active connections and listening ports.

Network Security Concept

Types of Threats in Network Security

1. **Malware (Malicious Software):** Malware is a collective term for malicious software designed to harm, exploit, or disable devices, networks, or data. Below are the key types of malware:

a. **Virus:**
A self-replicating program that attaches itself to legitimate files or software and spreads when the file is opened.
Infects the host system and can corrupt files, steal data, or crash the system.
Example: ILOVEYOU Virus (2000), Code Red(2001), Creeper, Bomber, Byte Bandit

b. **Worm:**
A standalone malware that spreads across networks without user intervention.
Exploits vulnerabilities in software or systems to replicate itself.
Example: Morris Worm (1988), Stuxnet, Nimda, Sasser.

c. **Trojan Horse**
Disguised as legitimate software but contains malicious code.
Users unknowingly install it, allowing attackers to gain control of the system.
Example: A fake antivirus program that claims to clean your system but actually steals your data.

d. **Ransomware**
Encrypts files on a device and demands payment (usually in cryptocurrency) for decryption.
Blocks access to data until the ransom is paid.
Example: WannaCry (2017): Targeted organizations worldwide, encrypting files and demanding Bitcoin payments.

e. **Spyware**
Secretly monitors user activity and collects sensitive information without consent.
Tracks keystrokes, browser history, and other personal data.
Example: Spyware in free software that collects user data for advertisers.

f. **Adware**
Displays unwanted advertisements and may redirect users to malicious websites.
Often bundled with free software and tracks user behavior for targeted ads.
Example: Pop-up ads that appear while browsing, redirecting to suspicious sites.

g. **Rootkit**
A set of tools that allow attackers to gain administrator-level control of a system.
Hides its presence and enables attackers to control the system remotely.
Example: Rootkits used to disable antivirus software and open backdoors for further attacks.

h. **Keylogger**
Records keystrokes to capture sensitive information like passwords or credit card numbers.
Runs silently in the background, logging every key pressed.
Example: Keyloggers installed on public computers to steal login credentials.

i. **Botnets**
A network of infected devices controlled by an attacker to perform coordinated attacks.
Used for spamming, DDoS attacks, or mining cryptocurrency.
Example: The Mirai Botnet (2016): Infected IoT devices to launch a massive DDoS attack.

j. Phishing

Phishing is a type of social engineering attack where attackers trick users into revealing sensitive information.
Types of Phishing Attacks:

1. **Email Phishing**
   Fake emails designed to look like they come from trusted sources (e.g., banks, government).
   Users click on malicious links or attachments, leading to data theft.
   Example: An email claiming to be from your bank asking you to verify your account by entering credentials on a fake website.

2. **Spear Phishing**
   A targeted phishing attack aimed at specific individuals or organizations.
   Uses personal information (e.g., names, job titles) to appear more convincing.
   Example: An email pretending to be from your manager asking for sensitive company data.

3. **Whaling**
   A phishing attack targeting high-profile individuals like CEOs or government officials.
   Focuses on obtaining sensitive business or financial information.
   Example: A fake email from a "legal department" asking a CEO to approve a wire transfer.

4. **Smishing (SMS Phishing)**
   Phishing through text messages.
   Users are tricked into clicking on malicious links sent via SMS.
   Example: A text claiming you've won a lottery and asking for your bank details to claim the prize.

5. **Vishing (Voice Phishing)**
   Phishing through phone calls.
   Attackers pose as legitimate entities (e.g., tech support) to extract sensitive information.
   Example: A scammer pretending to be from "Microsoft Support" asking for remote access to your computer.

3. DoS (Denial of Service) Attacks

DoS attacks aim to disrupt the availability of a service or network by overwhelming it with traffic.

Types of DoS Attacks

a. Volume-Based Attacks
Flood the network with a high volume of traffic, consuming all bandwidth.
Example: Sending millions of requests to a website, causing it to crash.

b. Protocol Attacks
Exploit vulnerabilities in network protocols to disrupt services.
Example: SYN Flood Attack: Exploits the TCP handshake process to overwhelm a server.

c. Application Layer Attacks
Target specific applications (e.g., web servers) by sending malicious requests.
Example: HTTP Flood Attack: Sends a large number of HTTP requests to a web server, exhausting its resources.

d. Distributed Denial of Service (DDoS)
A coordinated attack from multiple systems (botnets) to flood a target with traffic.
Example: The Dyn DDoS Attack (2016) disrupted services like Twitter, Netflix, and Reddit.

Security Measures in Network Security

1. **Firewalls**

   A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on predefined security rules.

Types of Firewalls

1. **Packet-Filtering Firewall**
   Inspects each packet (data unit) and allows or blocks it based on IP addresses, port numbers, and protocols.
   Example: Blocks packets from a suspicious IP address attempting to access your network.
2. **Stateful Inspection Firewall**
   Tracks the state of active connections and makes decisions based on the state and context of the traffic.
   Example: Allows only packets that are part of an established connection.
3. **Proxy Firewall**
   Acts as an intermediary between users and the internet, inspecting traffic before forwarding it.
   Example: A proxy server filters harmful web requests and hides user IP addresses.
4. **Next-Generation Firewall (NGFW)**
   Combines traditional firewall features with advanced capabilities like deep packet inspection and intrusion prevention.
   Example: Detects and blocks modern threats like malware and application-layer attacks.

2. **Virtual Private Networks (VPNs)**

   A VPN creates a secure, encrypted connection over a public or untrusted network, such as the internet. It ensures data privacy and security by masking the user's IP address and encrypting data traffic.

How VPNs Work

1. **Encryption:** Data transmitted between the user and the VPN server is encrypted.
2. **Tunneling:** Data is sent through a secure "tunnel," protecting it from interception.
3. **IP Masking:** The user's real IP address is hidden, and a virtual IP address is assigned.

Types of VPNs

1. **Remote Access VPN:** Allows employees to securely access their company's internal network from remote locations.
   Example: A remote worker accesses company files while traveling.
2. **Site-to-Site VPN:** Connects entire networks (e.g., between branch offices).
   Example: A company connects its headquarters and branch offices securely.
3. **Client-Based VPN:** Requires users to install software on their devices.
   Example: Using the NordVPN app on a laptop to browse securely.
4. **Cloud VPN:** Provides secure access to cloud-based resources.
   Example: Accessing Google Cloud resources securely through a VPN.

Advantages of VPNs

- **Data Security:** Prevents hackers from intercepting sensitive data.
- **Privacy:** Protects user identity and browsing activity.
- **Bypassing Geo-Restrictions:** Access blocked content in certain regions.

Introduction to Cryptography

Cryptography is the practice of securing communication and data by transforming information into a format that is unreadable to unauthorized users. It ensures confidentiality, integrity, and authenticity of data.
Cryptography is widely used in securing sensitive information such as passwords, financial transactions, and communication over the internet.

Encryption

Encryption is the process of converting plain text into unreadable ciphertext to protect data from unauthorized access. It requires a decryption key to convert ciphertext back into plain text.

Types of Cryptography

Cryptography is broadly classified into Symmetric Cryptography and Asymmetric Cryptography, based on the type of keys used.

1. **Symmetric Cryptography (Private Key Cryptography)**

   In symmetric cryptography, the same key is used for both encryption (converting plain text to ciphertext) and decryption (converting ciphertext back to plain text).

   How It Works

   1. A sender encrypts the message using a shared secret key.
   2. The receiver decrypts the message using the same key.
   3. Both parties must have the same key securely shared between them.

   Key Features

   - **Fast:** Symmetric encryption is computationally efficient and faster than asymmetric encryption.
   - **Key Sharing Issue:** Requires secure methods to share the secret key between parties.
   - **Best For:** Securing large amounts of data quickly.

   Examples of Symmetric Algorithms

   1. **AES (Advanced Encryption Standard):** Used for securing sensitive data in industries like banking.
   2. **DES (Data Encryption Standard):** An older encryption method, replaced by AES due to vulnerabilities.
   3. **Blowfish:** Known for its speed and effectiveness in applications like password protection.

2. **Asymmetric Cryptography (Public Key Cryptography)**

   In asymmetric cryptography, two keys are used:

   1. **Public Key:** Used for encryption and shared with anyone.
   2. **Private Key:** Used for decryption and kept secret by the recipient.

   How It Works

   1. The sender encrypts the message using the recipient's public key.
   2. Only the recipient can decrypt the message using their private key.
   3. This eliminates the need for securely sharing a single key.

   Key Features

   - **Secure Key Distribution:** No need to share private keys; only public keys are exchanged.
   - **Slower:** Computationally more intensive than symmetric encryption.
   - **Best For:** Securing small amounts of data, authentication, and digital signatures.

   Examples of Asymmetric Algorithms

   1. **RSA (Rivest-Shamir-Adleman):** Widely used in securing online transactions and email encryption.
   2. **ECC (Elliptic Curve Cryptography):** Provides strong security with smaller key sizes, used in mobile devices and IoT.
   3. **Diffie-Hellma**n: Securely exchanging cryptographic keys over an insecure channel.