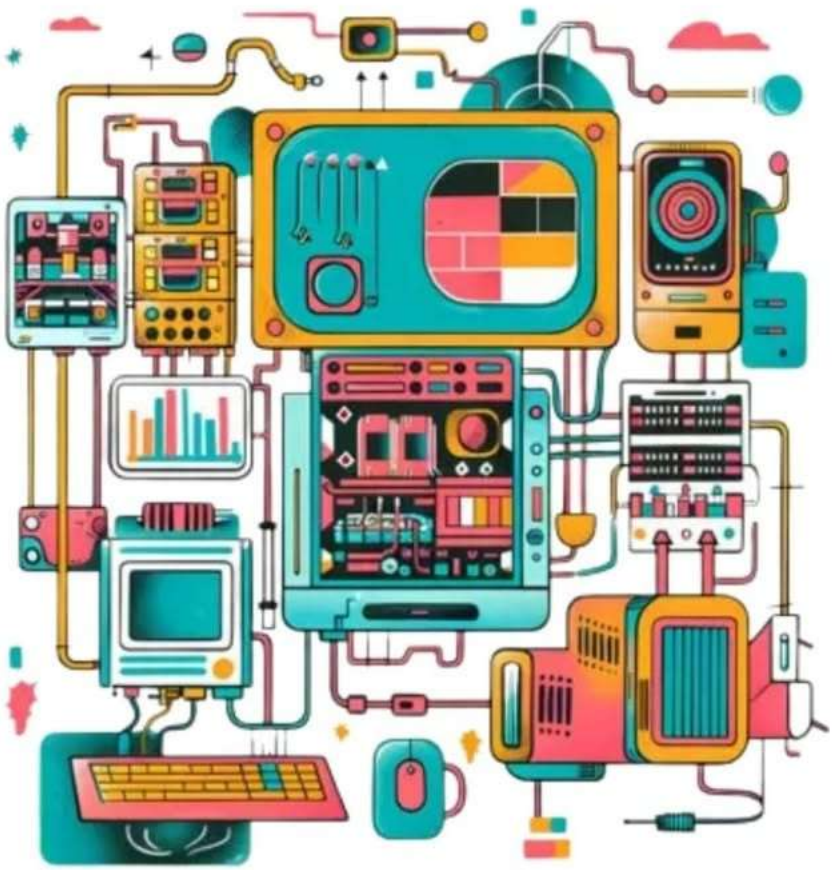
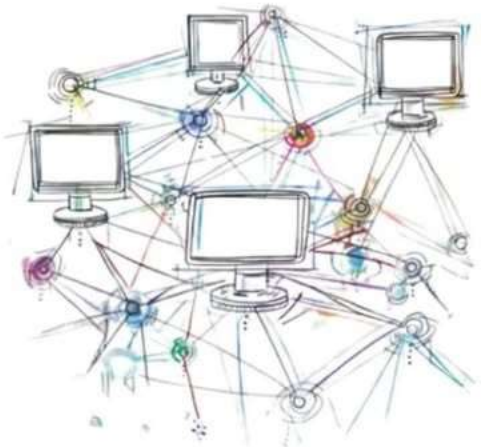
ALMOST ALL ABOUT NETWORKING !



Swipe...

WHAT IS NETWORKING?



Networking is the practice of connecting computers and other devices together so they can communicate and share resources. Imagine it like a group of friends chatting and sharing their things with each other.

Networking allows multiple devices, like computers, smartphones, and printers, to connect with each other and exchange information. This could be sending emails, sharing files, or accessing the internet.

The main **goal of networking** is to facilitate communication and resource sharing. For example:

- Sharing files: You can share documents with your coworkers easily.
- Accessing the internet: All devices in a home can connect to the internet through a single router.
- Playing online games: You can connect with friends around the world.

TYPES OF NETWORKS

1. Local Area Network (LAN)

A LAN is a network that connects devices within a small geographic area, like a home, office, or school.

For example, your home Wi-Fi network connects your smartphone, laptop, and smart TV.
Features:

- High speed: Typically very fast, as devices are close together.
- Limited range: Covers a small area, usually within a few hundred meters.
- Common use: File sharing, gaming, and printer access.

2. Wide Area Network (WAN)

A WAN connects multiple LANs over a large geographic area, often using leased telecommunication lines.

For example, the internet itself is the largest WAN, connecting millions of networks globally.
Features:

- Long distance: Covers large areas, even continents.
- Lower speed: Generally slower than LANs due to the distance and the technology used.
- Common use: Connecting branch offices of a company or providing internet access.

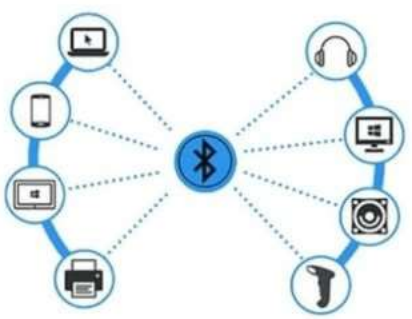
TYPES OF NETWORKS

3. Metropolitan Area Network (MAN)

A MAN covers a larger geographic area than a LAN but is smaller than a WAN, typically serving a city or a large campus.
For example the network used by a city to connect government buildings and public services.
Features:

- Medium range: Typically spans 5 to 50 kilometers.
- Higher speed than WAN: Faster than WANs but slower than LANs.
- Common use: Connecting local government offices, universities, and business districts.

4. Personal Area Network (PAN)



A PAN is a very small network, typically used for connecting personal devices like smartphones, tablets, and laptops.
For example connecting your smartphone to a Bluetooth headset or smart watch.
Features:

- Very short range: Usually within a few meters.
- Low power consumption: Often uses Bluetooth or infrared connections.
- Common use: Sharing data between personal devices, like files, music, or internet access.

NETWORKING DEVICES

Switch

A switch is a networking device that connects devices within a local area network (LAN) and uses MAC addresses to forward data to the correct device. Imagine you're in a room with a few people and you want to give a letter to just one specific person. A switch is like someone in the middle, helping deliver the letter (data) directly to the right person based on their MAC address. Switches work within local networks to forward data to the correct device.

Router

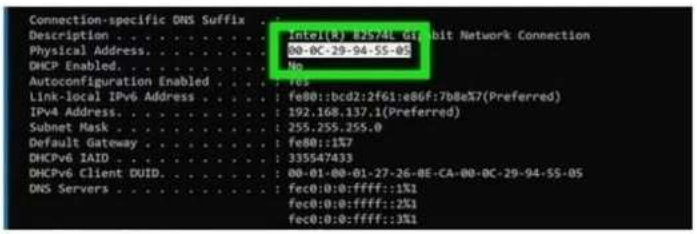
A router is a networking device that connects different networks together. It directs data packets between different networks, like a GPS for your data, deciding which route the data needs to take to reach a device that's not in your immediate network (like over the internet).

Hub

A hub is a basic networking device that connects multiple devices in a network but is less efficient than switches. It sends data to all devices on a network, regardless of which device it's meant for. It's like shouting in a room and hoping the right person hears it. These are being replaced by switches due to their inefficiency.

SOME TYPES OF ADDRESSES IN NETWORKING

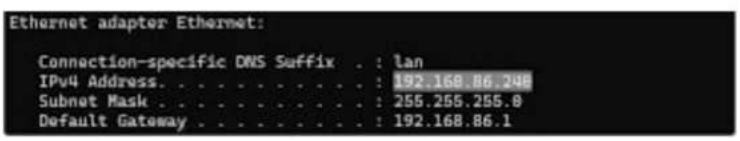
MAC Address



A MAC address (Media Access Control address) is like a unique serial number assigned to the network hardware (like a Wi-Fi card) in your device. It's hardwired into the device and doesn't change, similar to how every car has a unique VIN (Vehicle Identification Number).
A MAC address helps identify your device on a local network, such as when your computer connects to your home Wi-Fi. It tells the router which device is requesting data.
When devices on the same local network want to communicate, they use MAC addresses to ensure the data goes to the right device.

Format: A MAC address usually looks like six pairs of letters and numbers separated by colons (e.g., 00:1A:2B:3C:4D:5E).

IP Address



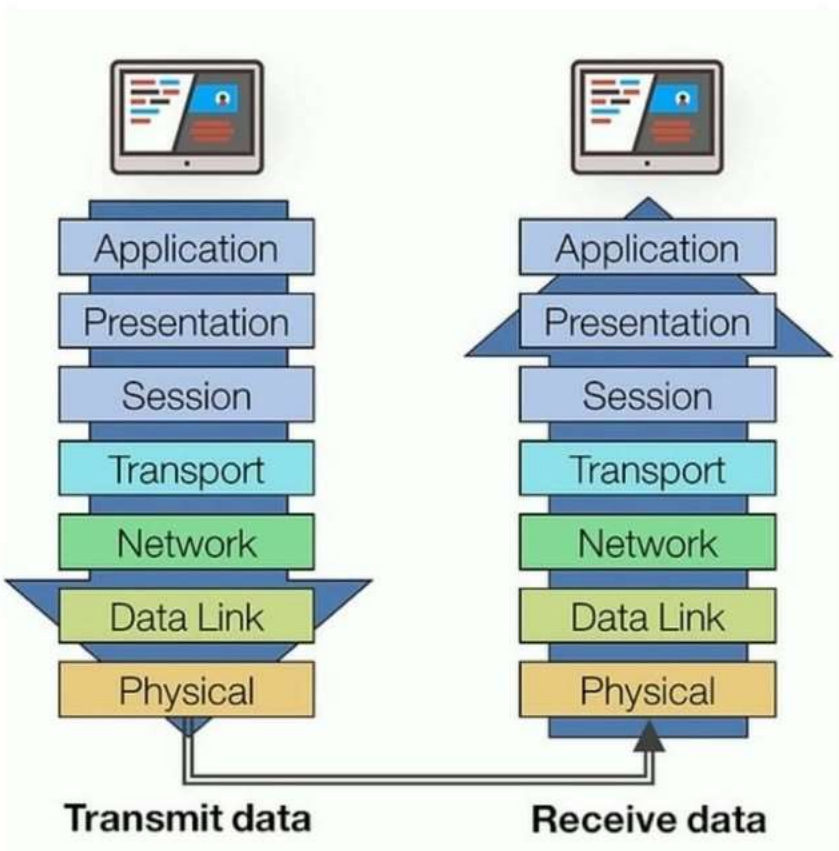
An IP address (Internet Protocol address) is like a home address for your computer or any device connected to the internet or a network. It helps other devices know where to send data. Just like your home address helps the mailman deliver your letters, an IP address helps data find its way to your device.When you send or receive data over the internet, IP addresses help route that data from one place to another, ensuring it reaches the correct destination. Types:

- IPv4: This is the most common type of IP address, made up of four numbers separated by periods (e.g., 192.168.1.1). Each number can be from 0 to 255.
- IPv6: As we ran out of IPv4 addresses, IPv6 was introduced. It's longer and uses a mix of numbers and letters (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

NETWORK MODELS OR PROTOCOL MODELS

A network model or protocol model refers to a conceptual framework that describes how data is transmitted and communicated across networks. These models define the rules and procedures for how devices interact, ensuring effective communication over various types of networks

OSI MODEL (Open Systems Interconnection)



The OSI model is a framework developed by the International Organization for Standardization (ISO) to standardize network communication that helps us understand how different networking technologies interact with each other. It divides the complex process of communication over a network into seven manageable layers, each with its own specific functions. Think of it like a set of layers in a cake, where each layer has a distinct role in making the whole cake (or network communication) work smoothly.

The Seven Layers of the OSI Model

1.Physical Layer (Layer 1)

- What it Does: This layer deals with the physical connection between devices. It defines the hardware components like cables, switches, and the electrical signals used to transmit data. Example: When you
- plug an Ethernet cable into your computer, you are dealing with the physical layer.

2.Data Link Layer (Layer 2)

- What it Does: This layer is responsible for node-to-node data transfer and error detection/correction. It ensures that data is packaged correctly for transmission and helps devices on the same network communicate.
- Example: When your computer sends data over Wi-Fi, the data link layer handles the communication with the router.

3.**Network Layer (Layer 3)**

- What it Does: This layer manages data routing and forwarding between different networks. It determines the best path for data to travel across the network.
- Example: When you access a website, the network layer helps route your request from your computer to the server hosting the site.

4.Transport Layer (Layer 4)

- What it Does: This layer ensures reliable data transfer between devices. It manages data segmentation, flow control, and error recovery. It makes sure that data arrives intact and in the correct order.
- Example: When you download a file, the transport layer checks that all parts of the file arrive correctly.

5.Session Layer (Layer 5)

- What it Does: This layer manages sessions or connections between applications. It establishes, maintains, and terminates connections as needed.
- Example: When you log in to an online service, the session layer keeps your session active until you log out.

6.Presentation Layer (Layer 6)

- What it Does: This layer formats and translates data between the application layer and the network. It ensures that data is in a readable format for the receiving application. Example: If you're viewing a
- website, the presentation layer helps convert the data from the server into a format your browser can display.

7.Application Layer (Layer 7)

- What it Does: This is the topmost layer, where end-user applications operate. It provides services for user applications and facilitates communication between software applications. Example: When you
- use a web browser or send an email, you're interacting with the application layer.

6.Presentation Layer (Layer 6)

- What it Does: This layer formats and translates data between the application layer and the network. It ensures that data is in a readable format for the receiving application. Example: If you're viewing a
- website, the presentation layer helps convert the data from the server into a format your browser can display.

7.Application Layer (Layer 7)

- What it Does: This is the topmost layer, where end-user applications operate. It provides services for user applications and facilitates communication between software applications. Example: When you
- use a web browser or send an email, you're interacting with the application layer.

The FourLayers of the TCP/IP Model

1.Link Layer (Network Interface Layer) , Network Acces

- What it Does: This layer handles the physical connection between devices on the same network. It deals with the hardware and protocols that allow devices to communicate over a local network, including Ethernet and Wi-Fi. Example: When your computer sends data over Wi-
- Fi, this layer manages that communication.

2.Internet Layer

- What it Does: This layer is responsible for routing data across different networks. It uses the Internet Protocol (IP) to send packets of data from the source device to the destination device, determining the best path for that data. Example: When you visit a website, the Internet
- layer helps direct your request to the correct server on the internet.

3.Transport Layer

- What it Does: This layer ensures reliable data transfer between devices. It uses protocols like Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) to manage data segmentation, flow control, and error checking. Example: When you download a file, TCP
- ensures that all pieces of the file arrive correctly and in order.

4.Application Layer

- What it Does: This is the top layer where user applications operate. It provides the interface for applications to communicate over the network. Protocols like HTTP (for web browsing) and FTP (for file transfer) function at this layer. Example: When you use a web browser
- to access a website, you're interacting with the Application layer.

IP Address Classes (IPv4)

IPv4 addresses are grouped into classes (A, B, C, D, E), which help to allocate addresses based on network sizes. The division of IP addresses into classes is based on the value of the first octet (the first number in the address).

Class A:

- Range: 0.0.0.0 to 127.255.255.255
- Used For: Large networks (e.g., internet service providers or large corporations).
- Number of Networks: Supports up to 128 networks.
- Number of Hosts: Each network can support over 16 million hosts (devices).
- First Octet Range: 0 to 12

Class B:

- Range: 128.0.0.0 to 191.255.255.255
- Used For: Medium-sized networks (e.g., universities, large businesses).
- Number of Networks: Supports up to 16,384 networks.
- Number of Hosts: Each network can support up to 65,534 hosts.
- First Octet Range: 128 to 191

Class C:

- Range: 192.0.0.0 to 223.255.255.255
- Used For: Small networks (e.g., home networks, small businesses).
- Number of Networks: Supports up to 2 million networks.
- Number of Hosts: Each network can support 254 hosts.
- First Octet Range: 192 to 223

Class D (Multicast):

- Range: 224.0.0.0 to 239.255.255.255
- Used For: Multicast groups (sending data to multiple devices simultaneously).
- Not Used for Hosts: This class is reserved for special use.

Class E (Experimental):

- Range: 240.0.0.0 to 255.255.255.255
- Used For: Reserved for research and experimental purposes.
- Not Used for Hosts: This class is not for public use.

IP Address Classes (IPv4)

Address Class	RANGE	Default Subnet Mask
A	1.0.0.0 to 126.255.255.255	255.0.0.0
B	128.0.0.0 to 191.255.255.255	255.255.0.0
C	192.0.0.0 to 223.255.255.255	255.255.255.0
D	224.0.0.0 to 239.255.255.255	Reserved for Multicasting
E	240.0.0.0 to 254.255.255.255	Experimental

Note: Class A addresses 127.0.0.0 to 127.255.255.255 cannot be used and is reserved for loopback testing.

https://notes.davidvarghese.dev

Why Is There a Limit of 255.255.255.255? In IPv4, each address is divided into four parts, called octets, with each part representing 8 bits. An octet can represent any number from 0 to 255, which is 8 bits in binary form.

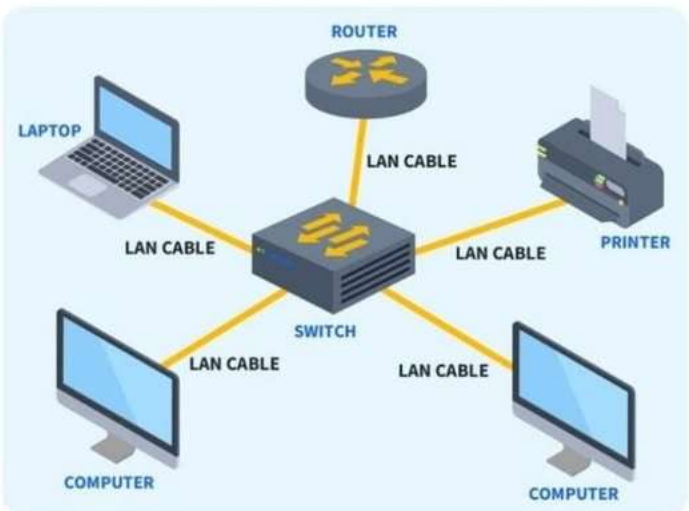
why the limit is 255:

- Each octet consists of 8 binary digits (bits). Since each bit can either be a 0 or a 1, an 8-bit number can represent 2^8 = 256 possible values (0 to 255). Therefore, each octet of the IP address can have a value ranging
- from 0 to 255. This makes the maximum possible IPv4 address 255.255.255.255.

How Devices Communicate in a Network

When devices like computers, smartphones, or printers want to exchange information over a network, they use a system of packets. A packet is a small chunk of data that gets sent across the network from one device to another. Think of it like a digital postcard containing information like your request to load a webpage or send a file.

Communication Within a Local Network (Using a Switch)

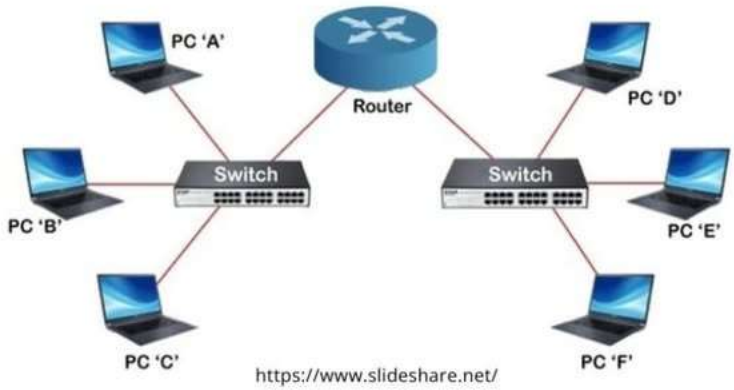


https://www.cbtnuggets.com/

When two devices are on the same network (e.g., in the same office or home), they use a device called a switch to communicate. The switch forwards the data packet to the correct device based on the MAC address.

- MAC Address: This is like a device's unique fingerprint on the network. Every device, whether it's a computer, smartphone, or printer, has a MAC address. It is permanently assigned to the device and helps the switch know where to deliver the data. Switch's Job: When a switch receives a packet, it checks the destination MAC address and sends the
- packet directly to that device, avoiding any confusion with other devices on the network.

Communication Between Different Networks (Using a Router)



If the devices are on different networks (for example, one device is in your home, and another is on the internet), then a router is used to handle the communication.

- IP Address: Each device on a network also has an IP address (like a mailing address for devices). While the MAC address is used for communication within the local network, the IP address is needed when data needs to leave the local network and travel across the internet. Router's Job: The router checks the destination IP address on the packet and decides how to
- forward the data across multiple networks until it reaches its final destination.

How Devices Find Each Other Using ARP (Address Resolution Protocol)

Sometimes, a device may know the IP address of the device it wants to send data to, but it doesn't know the MAC address (which is needed for local delivery). This is where ARP comes in.

- ARP's Job: ARP helps find the MAC address of the device by essentially asking, "Who has this IP address?" When the correct device responds with its MAC address, the sending device can now send the data directly using the switch.

Networking Protocols

Networking protocols are sets of rules and standards that allow devices (computers, servers, routers, etc.) to communicate with each other across networks like the internet or local networks. These protocols define how data is transmitted, routed, and received between devices.

1. TCP (Transmission Control Protocol)

- Purpose: Provides reliable, ordered, and error-checked data transmission between devices.
- How It Works: TCP breaks data into packets and ensures all packets arrive at the destination in the correct order. If packets are lost, TCP handles re-transmission.
- Example: Used in web browsing (HTTP/HTTPS), file transfer (FTP), and email (SMTP, IMAP).

2. IP (Internet Protocol)

- Purpose: Responsible for addressing and routing packets of data so that they can travel across networks and reach the correct destination.
- How It Works: Every device has an IP address, and IP protocols help guide data from one IP address to another.
- Example: IP is part of the foundational TCP/IP model used on the internet.

3. UDP (User Datagram Protocol)

- Purpose: Provides faster data transmission without the error-checking and re-transmission features of TCP.
- How It Works: Unlike TCP, UDP sends packets without ensuring they are received in order, making it faster but less reliable.
- Example: Used in real-time applications like video streaming, online gaming, and VoIP (Voice over IP).

4. HTTP (Hypertext Transfer Protocol)

- Purpose: The protocol used for transferring web pages over the internet.
- How It Works: When you visit a website, HTTP sends requests from your browser to the web server and receives the web pages back.
- Example: Used in almost all web communications. HTTPS (secure HTTP) encrypts the data for secure transmission.

5. FTP (File Transfer Protocol)

- Purpose: Used for transferring files between devices over a network.
- How It Works: FTP allows users to upload and download files to/from a remote server.
- Example: Commonly used in website management to upload files to web servers.

Protocols

6. SMTP (Simple Mail Transfer Protocol)

- Purpose: Used for sending emails from a client to a mail server and between mail servers.
- How It Works: SMTP handles the outbound emails, while protocols like IMAP and POP3 are used for retrieving emails.
- Example: Every time you send an email, it's transmitted via SMTP.

7. DNS (Domain Name System)

- Purpose: Translates human-readable domain names (like google.com) into IP addresses that computers can understand. How It Works: DNS servers
- store directories of domain names and their corresponding IP addresses, allowing devices to locate websites and services. Example: When you type a website's name, DNS translates it into the IP address of the server
- hosting the website.

8. DHCP (Dynamic Host Configuration Protocol)

- Purpose: Assigns IP addresses to devices automatically on a network.
- How It Works: When a device connects to a network, DHCP assigns it a unique IP address for communication.
- Example: Every time you connect your laptop or phone to a Wi-Fi network, DHCP is working behind the scenes to give it an IP address.

9. SNMP (Simple Network Management Protocol)

- Purpose: Used to manage and monitor network devices like routers, switches, and servers. How It Works: SNMP collects and organizes data
- about devices on a network, helping network administrators track performance or identify issues. Example: Used by IT administrators to check the status and health of network devices.
-

10. ARP (Address Resolution Protocol)

- Purpose: Maps IP addresses to MAC addresses on a local network. How It
- Works: When a device knows another device's IP address but not its MAC address, ARP helps discover the MAC address for local communication. Example: Used in local area networks (LANs) to ensure data is delivered to
- the right device.

Networking Protocols

11. ICMP (Internet Control Message Protocol)

- Purpose: Used by network devices to send error messages and operational information. How It Works: ICMP is most commonly known for the ping
- command, which tests connectivity between devices by sending a request and waiting for a response. Example: When troubleshooting network issues, the ping command checks if a server is reachable.
-

12. TLS/SSL (Transport Layer Security/Secure Sockets Layer)

- Purpose: Encrypts data to provide secure communication over a network.
- How It Works: SSL (now replaced by TLS) secures connections, like those between a browser and a website, by encrypting the data exchanged.
- Example: Used in HTTPS to secure web traffic and protect sensitive information like credit card details during online transactions.

Packet and Frame Packet

A packet is a unit of data used at the network layer (Layer 3) of the OSI model. It contains both the data being sent and important information, such as the source and destination IP addresses.

Packets are created and used primarily by routers for transferring data between different networks. When a packet is sent across the internet, routers use the information in the packet to determine where it should go.

Structure: A packet contains:

- Header (including source and destination IP addresses)
- Data (the actual payload)
- Trailer (optional, depending on the protocol)

Example: If you send a message over the internet, it will be broken into packets, which will be routed to the destination through different networks.

Frame

A frame is a unit of data used at the data link layer (Layer 2) of the OSI model. It is the packet's next form when it's transmitted across the local network (like through Ethernet or Wi-Fi). It contains the source and destination MAC addresses.

Frames are used by switches and Network Interface Cards (NICs) to move data within a local network. While packets carry data between different networks, frames are responsible for getting data from one device to another within the same network.

Structure: A frame contains:

- Header (with source and destination MAC addresses)
- Data (the payload, which may contain a packet)
- Trailer (includes error-checking information like a CRC or checksum)

Example: When a packet arrives at your local network, your router or switch will encapsulate it into a frame for delivery to your specific device.