Network Layer

The **Network Layer (Layer 3) of the OSI Model** is responsible for **routing packets** from the source to the destination across different networks. It determines the best path for data to travel using IP (Internet Protocol). The two main functions of this layer are:

1. **Logical addressing** (assigning IP addresses to devices).
2. **Routing** (deciding the best path for data transmission).

IPv4 (Internet Protocol Version 4)

IPv4 is the most widely used version of the Internet Protocol (IP). It is a **connectionless** and **best-effort** protocol, meaning it does not guarantee delivery but makes its best attempt. IPv4 uses **32-bit addresses**, which are usually represented in **dotted decimal notation** (e.g., `192.168.1.1`).

- IPv4 provides **packet switching**, meaning data is sent in small units called **datagrams**.

IPv4 Datagram and Encapsulation

An **IPv4 datagram** is the basic unit of data transfer in an IP network. It consists of:

1. **Header** – Contains essential control information such as source and destination IP addresses, time-to-live (TTL), and protocol.
2. **Payload** – Contains the actual data being transmitted.

IPv4 Header Fields

Some important fields in the IPv4 header:

- **Version**: Specifies the IP version (4 for IPv4).
- **Header Length**: Indicates the length of the header.
- **Total Length**: Specifies the size of the entire datagram.
- **Identification, Flags, Fragment Offset**: Helps in fragmenting and reassembling large packets.
- **Time to Live (TTL)**: Limits the packet's lifespan to prevent infinite loops.
- **Protocol**: Indicates whether the data belongs to TCP, UDP, or another protocol.
- **Source & Destination IP Addresses**: Identifies the sender and receiver.
- **Checksum**: Used for error checking.

Encapsulation

Encapsulation is the process of **wrapping data** with necessary protocol information at each layer of the OSI model. In IPv4:

1. The data from the **Transport Layer** (e.g., TCP or UDP segment) is encapsulated into an **IPv4 datagram**.
2. The IPv4 datagram is further encapsulated into a **Data Link Layer** frame (e.g., Ethernet frame).
3. The frame is sent over the **Physical Layer** as electrical signals.

IPv4 Address Classes

IPv4 addresses are categorized into **five classes** based on the first few bits:

Class	Range	Default Subnet Mask	Usage
A	`1.0.0.0 – 126.255.255.255`	255.0.0.0	Large networks (e.g., ISPs, large corporations)
B	`128.0.0.0 – 191.255.255.255`	255.255.0.0	Medium-sized businesses and organizations
C	`192.0.0.0 – 223.255.255.255`	255.255.255.0	Small networks (e.g., home and small businesses)
D	`224.0.0.0 – 239.255.255.255`	N/A	Used for multicast
E	`240.0.0.0 – 255.255.255.255`	N/A	Reserved for future use

- **Class A**: Supports **16 million** hosts per network.
- **Class B**: Supports **65,000** hosts per network.
- **Class C**: Supports **254** hosts per network.

Address Resolution Protocol (ARP)

The **Address Resolution Protocol (ARP)** is used to map an **IP address** (Layer 3) to a **MAC address** (Layer 2). Since devices communicate using MAC addresses on a local network, ARP helps find the MAC address associated with an IP.

How ARP Works

1. A device sends an **ARP Request**: "Who has IP `192.168.1.2`? Tell `192.168.1.1`."
2. The device with that IP responds with an **ARP Reply**, providing its MAC address.
3. The sender stores the response in an **ARP table** to avoid repeated requests.

Types of ARP Messages

- **ARP Request**: A broadcast message asking for a MAC address.
- **ARP Reply**: A unicast message providing the requested MAC address.

ARP Cache

- To reduce traffic, devices store ARP results in an **ARP cache** for a short time.