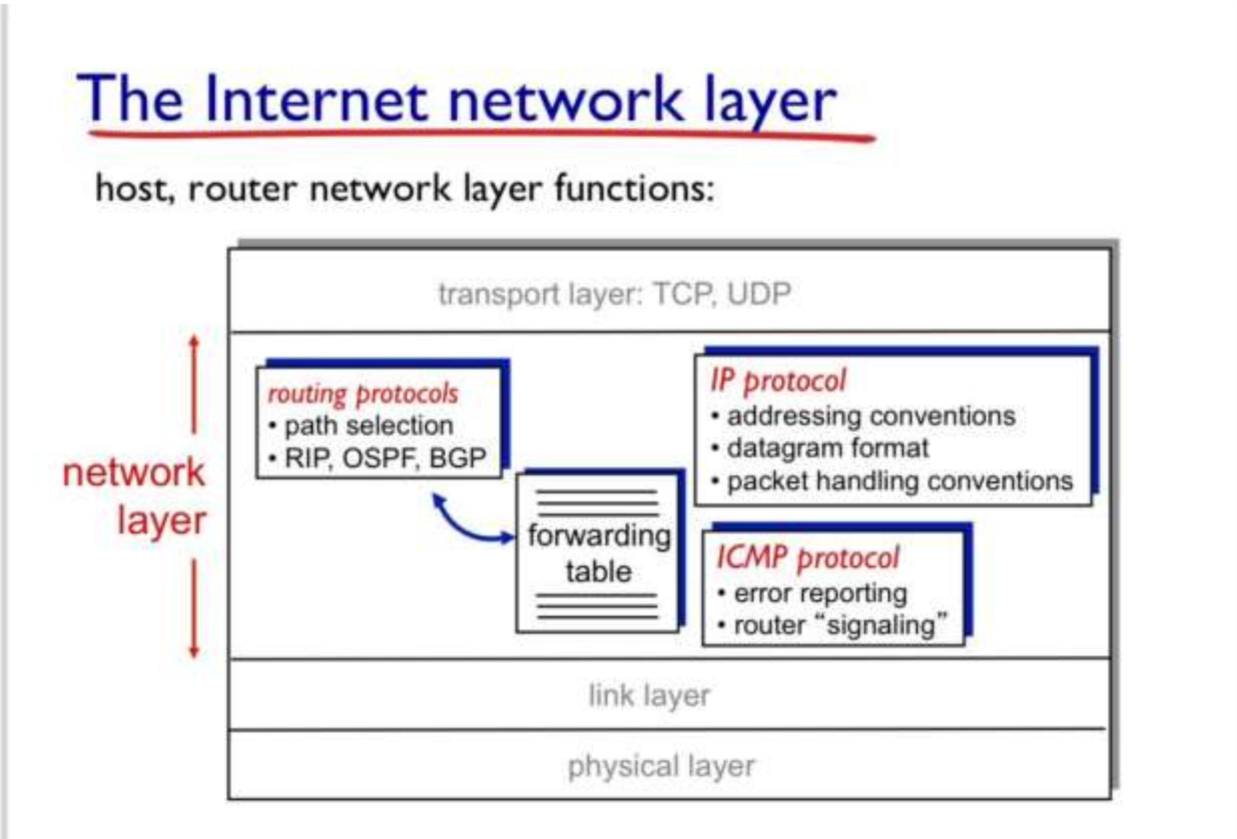
UNIT III NETWORK LAYER

Packet switching - Routing – Distance Vector and Link State Algorithms – RIP, OSPF and BGP - IPV4 Packet Format and Addressing – Effective IP address management techniques – Subnetting – CIDR – VLSM – DHCP – NAT – ICMP – Need for IPv6 – Addressing methods and types in IPv6 – IPv6 header – Advantages of IPv6 – Transition from IPv4 to IPv6.



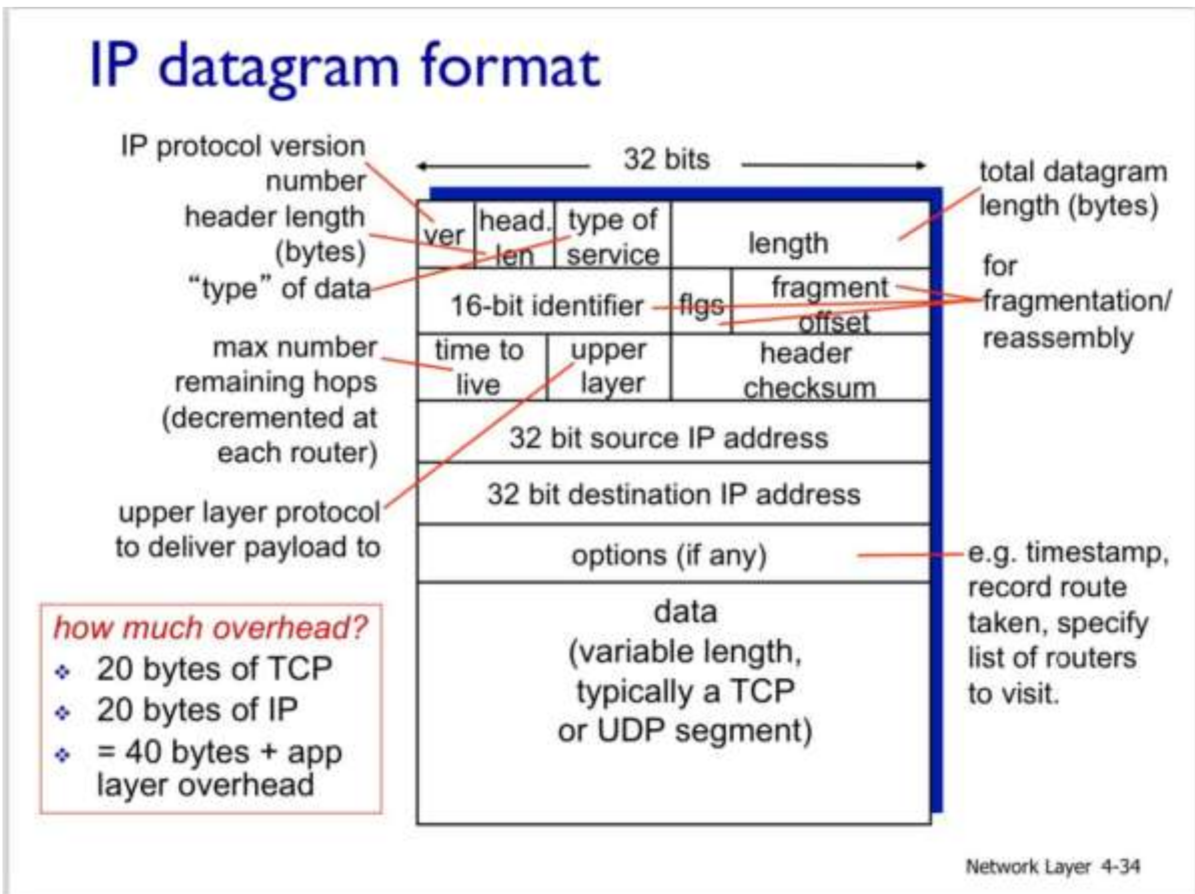
IPv4 Datagram Header

Characteristics of IPv4

- IPv4 could be a 32-Bit IP Address.
- IPv4 could be a numeric address, and its bits are separated by a dot.
- The number of header fields is twelve and the length of the header field is twenty.
- It has Unicast, broadcast, and multicast style of addresses.
- IPv4 supports VLSM (Virtual Length Subnet Mask).

- IPv4 uses the Post Address Resolution Protocol to map to the MAC address.
- RIP may be a routing protocol supported by the routed daemon.
- Networks ought to be designed either manually or with DHCP.
- Packet fragmentation permits from routers and causing host.

IPv4 Datagram Header



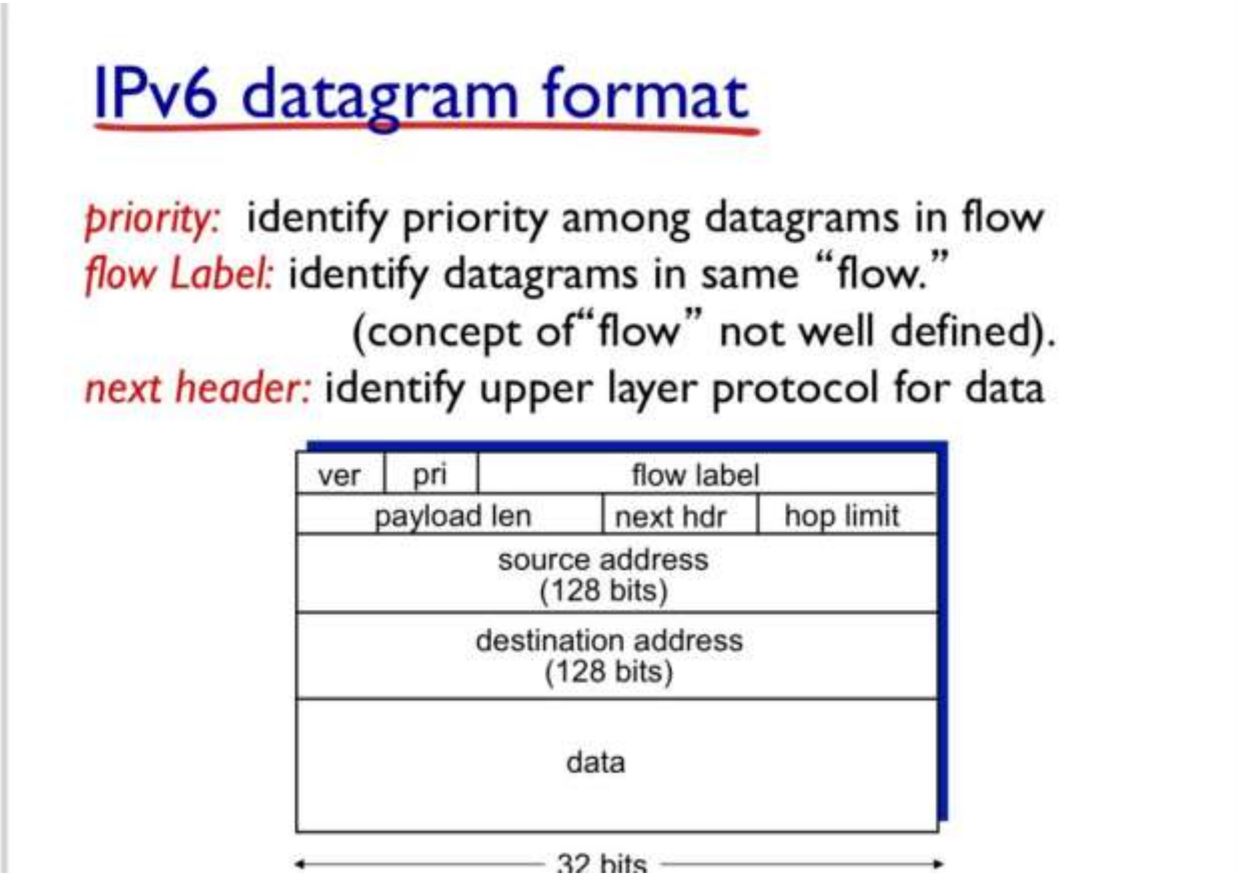
- **VERSION:** Version of the IP protocol (4 bits), which is 4 for IPv4
- **HLEN:** IP header length (4 bits), which is the number of 32 bit words in the header. The minimum value for this field is 5 and the maximum is 15.
- **Type of service:** Low Delay, High Throughput, Reliability (8 bits)

- **Total Length:** Length of header + Data (16 bits), which has a minimum value 20 bytes and the maximum is 65,535 bytes.
- **Identification:** Unique Packet Id for identifying the group of fragments of a single IP datagram (16 bits)
- **Flags:** 3 flags of 1 bit each : reserved bit (must be zero), do not fragment flag, more fragments flag (same order)
- **Fragment Offset:** Represents the number of Data Bytes ahead of the particular fragment in the particular Datagram. Specified in terms of number of 8 bytes, which has the maximum value of 65,528 bytes.
- **Time to live:** Datagram's lifetime (8 bits), It prevents the datagram to loop through the network by restricting the number of Hops taken by a Packet before delivering to the Destination.
- **Protocol:** Name of the protocol to which the data is to be passed (8 bits)
- **Header Checksum:** 16 bits header checksum for checking errors in the datagram header
- **Source IP address:** 32 bits IP address of the sender
- **Destination IP address:** 32 bits IP address of the receiver
- **Option:** Optional information such as source route, record route. Used by the Network administrator to check whether a path is working or not.

The IPv4 packet has a fixed header with a variable-length data section. Key fields in the header:

Field	Size (bits)	Description
Version	4	IPv4 (value = 4)
Header Length	4	Length of the header in 32-bit words (min = 5, max = 15)
Type of Service (TOS)	8	Priority and quality of service options
Total Length	16	Total length of the packet (header + data)
Identification	16	Unique identifier for fragmented packets
Flags	3	Control fragmentation
Fragment Offset	13	Indicates the fragment’s position in the original packet
Time to Live (TTL)	8	Limits the lifetime of the packet (hop count)
Protocol	8	Indicates the higher-layer protocol (e.g., TCP, UDP)
Header Checksum	16	Validates the header’s integrity
Source Address	32	IP address of the sender
Destination Address	32	IP address of the receiver
Options	Variable	Additional settings (rarely used)
Data	Variable	Payload containing upper-layer protocol information

IPv6 Header



Field	Size (bits)	Description
Version	4	IPv6 (value = 6)
Traffic Class	8	Similar to IPv4's TOS; QoS priority.
Flow Label	20	Identifies packets requiring special handling.
Payload Length	16	Length of the payload (data).
Next Header	8	Indicates the next protocol (e.g., TCP, UDP).
Hop Limit	8	Similar to IPv4's TTL; limits the number of hops.
Source Address	128	IPv6 address of the sender.
Destination Address	128	IPv6 address of the receiver.

Need for IPv6

IPv4 has limitations that necessitated the development of IPv6:

- **Address Exhaustion:** IPv4 provides ~4.3 billion addresses, which is insufficient for the growing number of devices.
- **Network Growth:** IPv6 supports a virtually unlimited number of devices.
- **Improved Security:** IPv6 integrates IPsec for secure communication.
- **Better QoS:** IPv6 offers improved Quality of Service (QoS) for real-time applications.
- **Simplified Configuration:** IPv6 includes autoconfiguration capabilities, reducing administrative overhead.

Addressing Methods and Types in IPv6:

Addressing Method	Description
Unicast	Identifies a single interface; packets are delivered to one specific recipient.
Multicast	Identifies multiple interfaces; packets are delivered to all members of a group.
Anycast	Identifies multiple interfaces; packets are delivered to the nearest one in terms of routing distance.

Address Type	Prefix	Description
Global Unicast	2000::/3	Unique addresses routable over the internet.
Link-Local	FE80::/10	Automatically configured addresses for communication within a link; not routable beyond the link.
Unique Local Address	FC00::/7	For local communications; not routable over the internet but unique within an organization.

Multicast	FF00::/8	Used for multicast groups; packets are delivered to multiple destinations.
Unspecified Address	::	Represents no address (used as a placeholder).
Loopback Address	::1	Used by a device to send packets to itself (loopback testing).
Reserved Addresses	Various	Reserved for special purposes, including future use and testing (e.g., FF02::1 for all nodes).

Advantages of IPv6

- **Larger Address Space:** IPv6 provides 21282^{128}2128 addresses, far more than IPv4's 2322^{32}232.
- **Simplified Header:** Improves processing efficiency by routers.
- **Improved Security:** Built-in IPsec support for authentication and encryption.
- **Autoconfiguration:** Supports stateful (DHCPv6) and stateless (SLAAC) configuration.
- **Better Support for Mobile Devices:** Allows seamless mobility with minimal disruption.
- **Eliminates NAT:** Direct addressing removes the need for Network Address Translation.

Transition from IPv4 to IPv6

Challenges in Transition

- IPv4 and IPv6 are not directly compatible.
- Requires dual-stack operation and gradual migration.

Techniques for Transition

1. **Dual-Stack:** Devices run both IPv4 and IPv6 simultaneously.
2. **Tunneling:** IPv6 packets are encapsulated within IPv4 packets for transport over an IPv4 network.

- Examples: 6to4, Teredo, and ISATAP.

3. **Translation:** Converts IPv4 packets to IPv6 and vice versa using NAT64/DNS64.

Effective IP Address Management Techniques:

1. **Subnetting**
   a. **Definition**: Dividing a large IP network into smaller, manageable sub-networks (subnets).
   b. **Purpose**: Optimizes IP address usage, improves network performance, and enhances security.
   c. **Example**: Splitting `192.168.1.0/24` into two subnets: `192.168.1.0/25` and `192.168.1.128/25`.

2. **CIDR (Classless Inter-Domain Routing)**
   a. **Definition**: A method to allocate IP addresses efficiently by allowing flexible prefix lengths, replacing the rigid class-based addressing.
   b. **Purpose**: Reduces wasted IP addresses and simplifies routing.
   c. **Example**: Instead of a classful network `192.168.1.0/24`, CIDR can allocate smaller networks like `192.168.1.0/28` for 16 addresses.

3. **VLSM (Variable Length Subnet Masking)**
   a. **Definition**: Extends subnetting by allowing different subnets to have varying sizes within the same network.
   b. **Purpose**: Maximizes efficient IP address allocation based on the number of required hosts.
   c. **Example**: A `192.168.1.0/24` network can be divided as `192.168.1.0/26` for 64 hosts and `192.168.1.64/27` for 32 hosts.

4. **DHCP (Dynamic Host Configuration Protocol)**
   a. **Definition**: Automatically assigns IP addresses and other network configurations to devices.
   b. **Purpose**: Simplifies IP management in dynamic or large networks.

   c. **Example**: Assigns IP addresses from a pool (`192.168.1.100` to `192.168.1.200`) to devices when they connect.

5. **NAT (Network Address Translation)**
   a. **Definition**: Allows multiple devices on a private network to access the Internet using a single public IP address.
   b. **Purpose**: Conserves public IPs, enhances security, and provides IP address mapping.
   c. **Example**: A private network (`192.168.1.0/24`) is translated to a single public IP (`203.0.113.1`) for external communication.

6. **ICMP (Internet Control Message Protocol)**
   a. **Definition**: Used for diagnostic and error-reporting purposes in network communication.
   b. **Purpose**: Helps identify issues like unreachable hosts or network errors.
   c. **Example**: **Ping** uses ICMP to check the availability and response time of a host.

Subnetting

Definition:

Subnetting is the process of dividing a larger IP network into smaller, more manageable sub-networks (subnets). Each subnet operates as an independent network while still being part of the original larger network.

Purpose:

- **Efficient IP Address Utilization**: Allocates IP addresses based on specific needs (e.g., number of devices per subnet).
- **Improved Network Performance**: Reduces broadcast traffic within each subnet.
- **Enhanced Security**: Isolates sensitive parts of a network.
- **Simplified Management**: Organizes networks logically.

Key Concepts

1. **Subnet Mask**:

   a. Defines the division between the network and host portions of an IP address.
   b. Example: `255.255.255.0` (or /24) indicates the first 24 bits represent the network.
2. **CIDR Notation**:
   a. Specifies the subnet mask using a / followed by the number of network bits.
   b. Example: `192.168.1.0/25`.
3. **Subnet ID and Broadcast Address**:
   a. Each subnet has a unique ID and broadcast address.
   b. Example: For `192.168.1.0/25`, the subnet ID is `192.168.1.0`, and the broadcast address is `192.168.1.127`.

Subnetting Example

- **Given**: Network `192.168.1.0/24`.
- **Task**: Create four subnets.
- **Solution**: Increase subnet mask from /24 to /26 (adds 2 bits to the network portion).
    - Subnet Mask: `255.255.255.192` or /26.
    - Each subnet has `2^6 = 64` addresses (62 usable for hosts).

Subnets:

Subnet ID	First Host	Last Host	Broadcast Address
192.168.1.0/26	192.168.1.1	192.168.1.62	192.168.1.63
192.168.1.64/26	192.168.1.65	192.168.1.126	192.168.1.127
192.168.1.128/26	192.168.1.129	192.168.1.190	192.168.1.191
192.168.1.192/26	192.168.1.193	192.168.1.254	192.168.1.255

Benefits of Subnetting:

1. **Conserves IP Addresses**: Reduces wastage in larger networks.
2. **Limits Broadcast Domains**: Ensures less traffic and better performance.
3. **Logical Organization**: Facilitates departmental or geographical segregation.

Supernetting

Definition:

Supernetting is the process of combining multiple smaller, contiguous networks (subnets) into a single larger network (supernet). It is the inverse of subnetting and is typically used in routing to reduce the size of routing tables.

Purpose:

- Simplifies routing by aggregating multiple routes into a single entry.
- Optimizes the allocation of IP addresses.
- Reduces the load on routers and improves efficiency in large networks

Key Features:

1. **Combines Networks**: Merges multiple networks with contiguous IP address ranges.
2. **Flexible Masking**: Uses a shorter subnet mask to include more addresses in a single block.
3. **Classless**: Like CIDR, supernetting ignores traditional class boundaries (Class A, B, C).

Example:

Suppose you have four Class C networks:

- `192.168.1.0/24`
- `192.168.2.0/24`
- `192.168.3.0/24`
- `192.168.4.0/24`

To supernet these, a shorter prefix `/22` can represent them as a single block:

- **Supernet**: `192.168.0.0/22`
- **Address Range**: `192.168.0.0` to `192.168.3.255`.

Benefits:

1. Reduces routing table size by advertising one route instead of four.
2. Simplifies network management.
3. Minimizes overhead in routers.

Applications:

- Used by ISPs for route aggregation to advertise fewer routes.
- Optimizes large-scale enterprise networks with contiguous IP address blocks.

1. CIDR (Classless Inter-Domain Routing)

- **Definition**: A method for allocating IP addresses and routing by allowing flexible subnet masks instead of fixed class-based masks (Class A, B, C).
- **Purpose**: Optimizes IP address allocation and reduces routing table size.
- **Key Features**:
  - Uses **prefix length** to define networks (e.g., `192.168.1.0/24` for 256 addresses).
  - Aggregates routes to minimize entries (e.g., `192.168.0.0/16` combines multiple /24 subnets).
- **Example**:

Instead of allocating a full Class B network (`172.16.0.0/16`), CIDR allows creating a smaller network, such as `172.16.0.0/20` for 4,096 addresses.

STEPS TO CONVERT SUBNET TO CIDR

1. **Write the subnet mask in decimal notation.** Example: 255.255.255.0.
2. **Convert the decimal subnet mask into binary.**
   - 255.255.255.0 becomes 11111111.11111111.11111111.00000000.
3. **Count the number of 1 bits in the binary subnet mask.**
   - Here, there are 24 ones.
4. **The CIDR notation is the number of 1s.**
   - For the example 255.255.255.0, the CIDR is /24.

Examples

1. **Subnet Mask: 255.255.255.128**
   - Binary: 11111111.11111111.11111111.10000000
   - Number of 1s: 25
   - CIDR: /25

2. **Subnet Mask: 255.255.252.0**
   - Binary: 11111111.11111111.11111100.00000000
   - Number of 1s: 22
   - CIDR: /22

Steps to Convert CIDR to Subnet Mask

1. **Identify the CIDR Prefix**
   The number after the / in CIDR represents the number of 1s in the subnet mask. For example, /20 means the subnet mask has 20 1s.
2. **Write the Binary Subnet Mask**
   Write 1s for the prefix length and fill the rest with 0s to make a total of 32 bits.
   Example for /20: 11111111.11111111.11110000.00000000.
3. **Convert Each Octet from Binary to Decimal**
   Break the 32-bit binary string into four 8-bit segments (octets) and convert each to decimal.
   Example: 11111111.11111111.11110000.00000000 → 255.255.240.0.

Example Conversions

CIDR	Binary Subnet Mask	Decimal Subnet Mask
/16	11111111.11111111.00000000.00000000	255.255.0.0
/24	11111111.11111111.11111111.00000000	255.255.255.0
/27	11111111.11111111.11111111.11100000	255.255.255.224
/30	11111111.11111111.11111111.11111100	255.255.255.252

2. VLSM (Variable Length Subnet Masking)

- **Definition**: Extends subnetting by allowing subnets of different sizes within the same network.
- **Purpose**: Efficiently uses IP addresses by matching the subnet size to the number of required hosts.
- **Key Features**:
    - Avoids IP wastage by creating subnets based on host requirements.
    - Compatible with CIDR.
- **Example**:

From `192.168.1.0/24`:

- `/26` for 64 hosts (e.g., `192.168.1.0/26`).
- `/27` for 32 hosts (e.g., `192.168.1.64/27`).
- `/30` for point-to-point links (e.g., `192.168.1.96/30`).

3. DHCP (Dynamic Host Configuration Protocol)

- **Definition**: A protocol that dynamically assigns IP addresses and other network settings to devices.
- **Purpose**: Simplifies IP management in networks with frequently changing devices.
- **Key Features**:
    - Centralized IP allocation.
    - Prevents conflicts by ensuring unique IPs.
    - Can also configure DNS, default gateway, and subnet masks.
- **Example Workflow**:
    - A device sends a **DHCP Discover** message.
    - The DHCP server replies with a **DHCP Offer**.
    - The device accepts using a **DHCP Request**.
    - The server confirms with a **DHCP Acknowledgement**.

4. NAT (Network Address Translation)

- **Definition**: A technique where private IP addresses are translated to a public IP address for external communication.

- **Purpose**: Conserves public IP addresses and enhances security.
- **Key Features**:
  - **Static NAT**: Maps a private IP to a specific public IP.
  - **Dynamic NAT**: Maps private IPs to a pool of public IPs.
  - **PAT (Port Address Translation)**: Multiple private IPs share a single public IP using unique ports.
- **Example**:
  - Internal Network: `192.168.0.0/24`.
  - External IP: `203.0.113.1`.
  - Devices with private IPs access the internet using `203.0.113.1`.

5. ICMP (Internet Control Message Protocol)

- **Definition**: A protocol used for diagnostic and error-reporting in IP networks.
- **Purpose**: Helps identify network issues such as unreachable hosts or congestion.
- **Key Features**:
  - Works alongside IP but does not transfer data.
  - Generates error messages (e.g., "Destination Unreachable").
  - Used by tools like **ping** and **traceroute**.
- **Example Uses**:
  - **Ping**: Sends ICMP Echo Request to check if a host is reachable.
  - **Traceroute**: Uses ICMP to map the path packets take to a destinatio