Network Layer

Aayush Adhikari
Roshan Tiwari
Shishir Sharma Rijal
Sudip Acharya

July 11, 2024

Contents

1 Introduction to Networking **1**

1.1 MAC Addresses in LAN 1

1.2 Introduction to IP Addresses 1

1.3 IP Datagram Structure 2

1.3.1 Header Fields 2

1.4 IP Address Classes 3

1.5 Address Resolution Protocol (ARP) 4

1.6 Detailed Content: IPv4 vs IPv6 5

1.6.1 Address Space 5

1.6.2 Notation 5

1.6.3 Header 5

1.6.4 Security 5

1.6.5 Quality of Service (QoS) 6

1.6.6 Fragmentation 6

1.6.7 Address Configuration 6

1.7 Subnetting 6

1.7.1 Basics of Subnetting 6

1.7.2 Subnetting Process 6

1.7.3 Subnetting Example 7

1.7.4 VLSM (Variable Length Subnet Masking) 7

1.7.5 Subnetting in IPv6 7

Chapter 1

Introduction to Networking

1.1 MAC Addresses in LAN

Media Access Control (MAC) addresses are fundamental to network communication at the data link layer. These 48-bit hexadecimal numbers are unique identifiers assigned to network interface cards (NICs) by manufacturers. MAC addresses serve as the physical address of a device on a local area network (LAN).

The structure of a MAC address consists of two main parts:

- The first 24 bits represent the Organizationally Unique Identifier (OUI), assigned to the manufacturer by the IEEE.
- The last 24 bits are uniquely assigned by the manufacturer to each NIC.

MAC addresses are crucial for local network communication, allowing devices to identify and communicate with each other within the same network segment. They are used in the Address Resolution Protocol (ARP) to map IP addresses to MAC addresses, enabling the creation of Ethernet frames for data transmission.

Note

While MAC addresses work well for local communication, they have limitations when it comes to global networking:

- Lack of hierarchical structure makes routing based on MAC addresses inefficient for large networks.
- The flat address space doesn't provide information about the network topology.
- MAC addresses are typically hardcoded, making it difficult to change or reassign addresses as network needs evolve.

These limitations necessitate the use of IP addressing at the network layer for global communication.

1.2 Introduction to IP Addresses

Internet Protocol (IP) addresses are crucial for enabling communication across diverse networks that make up the internet. Unlike MAC addresses, IP addresses are logical addresses assigned to devices by network administrators or dynamically through protocols like DHCP.

IP addresses come in two main versions:

- IPv4: 32-bit addresses, typically represented in dotted-decimal notation (e.g., 192.168.1.1).

- IPv6: 128-bit addresses, represented in hexadecimal notation (e.g., 2001:0db8:85a3:0000:0000:8a2e

The hierarchical nature of IP addresses allows for efficient routing across the internet. They are divided into network and host portions, enabling routers to make decisions based on the network part of the address.

Key features of IP addresses include:

- Hierarchical structure for efficient routing
- Flexibility in assignment and reassignment
- Support for subnetting and supernetting
- Ability to represent both public and private networks

Important

Understanding IP addresses is crucial for network communication because:

- They enable global routing across the internet
- They allow for logical network segmentation
- They support various networking protocols and services
- They are essential for network security and access control

1.3 IP Datagram Structure

The IP datagram is the fundamental unit of data transfer in IP networks. It consists of two main parts: the header and the payload. The header contains crucial information for routing and handling the datagram, while the payload carries the actual data being transmitted.

1.3.1 Header Fields

The IP header contains several fields that provide essential information for network devices to process and route the datagram correctly. The main fields in an IPv4 header include:

- **Version (4 bits):** Indicates the IP version (4 for IPv4).
- **Internet Header Length (IHL) (4 bits):** Specifies the header length in 32-bit words.
- **Type of Service (8 bits):** Used for Quality of Service (QoS) prioritization.
- **Total Length (16 bits):** The total length of the datagram, including header and payload.
- **Identification (16 bits):** Used for uniquely identifying fragments of an original IP datagram.

- **Flags (3 bits):** Control fragmentation and indicate more fragments.
- **Fragment Offset (13 bits):** Indicates the position of the fragment in the original datagram.
- **Time to Live (TTL) (8 bits):** Limits the lifespan of the datagram in the network.
- **Protocol (8 bits):** Indicates the next level protocol used in the payload.
- **Header Checksum (16 bits):** Used to check for errors in the header.
- **Source IP Address (32 bits):** The IP address of the sender.
- **Destination IP Address (32 bits):** The IP address of the intended recipient.
- **Options:** Variable length field for additional options (if IHL ¿ 5).

Important

Understanding the IP datagram structure is crucial for network communication because:

- It allows network devices to process and route packets efficiently.
- It enables fragmentation and reassembly of large data packets.
- It provides mechanisms for quality of service and error checking.
- It supports various upper-layer protocols through the protocol field.

1.4 IP Address Classes

IP address classes were introduced in the early days of IP networking to provide a structured way of allocating IP addresses to different types of networks. Although classful addressing has been largely replaced by Classless Inter-Domain Routing (CIDR), understanding these classes is still important for grasping the fundamentals of IP addressing.

The five address classes are:

- **Class A:**
  - First bit always 0
  - Range: 1.0.0.0 to 126.255.255.255
  - Default subnet mask: 255.0.0.0
  - Supports up to 16,777,214 hosts per network
- **Class B:**
  - First two bits always 10
  - Range: 128.0.0.0 to 191.255.255.255
  - Default subnet mask: 255.255.0.0

  - Supports up to 65,534 hosts per network

- **Class C:**
  - First three bits always 110
  - Range: 192.0.0.0 to 223.255.255.255
  - Default subnet mask: 255.255.255.0
  - Supports up to 254 hosts per network

- **Class D:**
  - First four bits always 1110
  - Range: 224.0.0.0 to 239.255.255.255
  - Used for multicast group addresses

- **Class E:**
  - First four bits always 1111
  - Range: 240.0.0.0 to 255.255.255.255
  - Reserved for experimental use

Note

While IP address classes are no longer strictly adhered to in modern networking, understanding them helps in:

- Recognizing the historical context of IP addressing
- Understanding the basics of subnetting and network design
- Interpreting legacy network configurations
- Appreciating the evolution towards more flexible addressing schemes like CIDR

1.5 Address Resolution Protocol (ARP)

The Address Resolution Protocol (ARP) is a crucial networking protocol that bridges the gap between Layer 2 (Data Link Layer) and Layer 3 (Network Layer) of the OSI model. Its primary function is to map IP addresses to MAC addresses, which is essential for communication within a local area network (LAN).

Key aspects of ARP include:

- **Purpose:** To resolve IP addresses to MAC addresses for local network communication.
- **Operation:**

1. When a device needs to send data to an IP address on the same network, it checks its ARP cache.
2. If the MAC address is not in the cache, the device broadcasts an ARP request.
3. The device with the matching IP address responds with its MAC address.
4. The sender updates its ARP cache and sends the data using the resolved MAC address.

- **ARP Cache:** A temporary storage of IP-to-MAC address mappings to reduce network traffic.
- **Gratuitous ARP:** An unsolicited ARP response sent to update ARP caches on other devices.
- **Proxy ARP:** Allows a device to respond to ARP requests on behalf of another device.

Important

ARP is essential for network communication because:

- It enables the creation of Ethernet frames by providing the necessary MAC address.
- It reduces the need for constant broadcasting by caching address mappings.
- It supports communication between different subnets through proxy ARP.
- It helps in detecting IP address conflicts and updating network changes.

However, ARP's lack of authentication makes it vulnerable to attacks like ARP spoofing, highlighting the need for security measures in network design.

1.6 Detailed Content: IPv4 vs IPv6

As the internet continues to grow, the limitations of IPv4 have become increasingly apparent. IPv6 was developed to address these limitations and provide additional features. Here's a comparison of IPv4 and IPv6:

1.6.1 Address Space

- IPv4: 32-bit address space (approximately 4.3 billion addresses)
- IPv6: 128-bit address space (approximately 340 undecillion addresses)

1.6.2 Notation

- IPv4: Dotted-decimal (e.g., 192.168.1.1)
- IPv6: Hexadecimal with colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334)

1.6.3 Header

- IPv4: Variable length, with options
- IPv6: Fixed length (40 bytes), with extension headers for additional options

1.6.4 Security

- IPv4: Security is optional (IPsec)

- IPv6: Built-in support for IPsec

1.6.5 Quality of Service (QoS)

- IPv4: Limited QoS capabilities
- IPv6: Enhanced QoS support with Flow Label field

1.6.6 Fragmentation

- IPv4: Routers can fragment packets
- IPv6: Only end nodes can fragment packets

1.6.7 Address Configuration

- IPv4: Manual or DHCP
- IPv6: Stateless address autoconfiguration (SLAAC), DHCPv6, or manual

While IPv6 offers significant improvements over IPv4, the transition has been slow due to the complexity of updating existing infrastructure and the effectiveness of Network Address Translation (NAT) in extending the lifespan of IPv4.

1.7 Subnetting

Subnetting is a crucial technique in IP networking that allows network administrators to divide a large network into smaller, more manageable subnetworks or subnets. This process enhances network efficiency, security, and address utilization.

1.7.1 Basics of Subnetting

Subnetting involves borrowing bits from the host portion of an IP address to create additional network bits. This process is achieved by extending the subnet mask beyond its default class boundaries.

Key concepts in subnetting include:

- **Subnet Mask:** A 32-bit number that defines the network and host portions of an IP address.
- **Network Bits:** The part of the IP address that identifies the network.
- **Host Bits:** The part of the IP address that identifies individual hosts within a network.
- **CIDR Notation:** A compact way to specify a subnet mask (e.g., /24 for 255.255.255.0).

1.7.2 Subnetting Process

The process of subnetting involves several steps:

1. Determine the number of required subnets or hosts per subnet.
2. Calculate the number of bits to borrow from the host portion.
3. Determine the new subnet mask.
4. Calculate the subnet addresses, broadcast addresses, and usable IP ranges.

1.7.3 Subnetting Example

Let's consider an example of subnetting a Class C network:

Given IP address: 192.168.1.0/24 (Default Class C mask) Requirement: Create 4 subnets

- Step 1: To create 4 subnets, we need to borrow 2 bits ($2^2 = 4$).
- Step 2: New subnet mask: 255.255.255.192 (/26)
- Step 3: Subnet calculations:
  - Subnet 0: 192.168.1.0 - 192.168.1.63
  - Subnet 1: 192.168.1.64 - 192.168.1.127
  - Subnet 2: 192.168.1.128 - 192.168.1.191
  - Subnet 3: 192.168.1.192 - 192.168.1.255

1.7.4 VLSM (Variable Length Subnet Masking)

VLSM is an advanced subnetting technique that allows for more efficient use of IP address space by using different subnet masks for different subnets within the same network.

Benefits of VLSM include:

- More efficient use of IP address space
- Flexibility in network design
- Support for hierarchical network structures

Important

Subnetting is crucial for network design and management because:

- It improves network performance by reducing broadcast domains
- It enhances security by allowing for better network segmentation
- It enables more efficient use of IP address space
- It supports the implementation of hierarchical network structures
- It is fundamental to understanding and implementing routing in IP networks

1.7.5 Subnetting in IPv6

While the principles of subnetting remain similar in IPv6, the vast address space allows for more straightforward subnet allocation. In IPv6:

- The standard subnet size is /64, leaving 64 bits for host addressing.
- Subnets are typically created by adjusting the bits between /48 and /64.

- IPv6 subnetting focuses more on logical network division rather than conserving addresses.

Note

Proficiency in subnetting is essential for:

- Network administrators and engineers
- IT professionals preparing for networking certifications
- Anyone involved in network design and implementation
- Understanding routing protocols and network traffic flow

Regular practice with subnetting calculations is recommended to maintain and improve this crucial networking skill.