Understanding IP Addressing, Subnetting, MAC Addressing, and ARP/RARP

A Comprehensive Look at OSI Model, TCP/IP Model, TCP, UDP, HTTP, HTTPS, and ICMP

Aniket Das

Introduction to IP Addressing

IP addresses are the fundamental building blocks of modern digital networks, enabling seamless communication between devices. Understanding the core concepts of IP addressing is crucial for network design, troubleshooting, and effective management.

Overview of IP Addressing

Fundamental Building Blocks

IP addresses are the unique numeric identifiers assigned to devices on a network, enabling communication and data exchange across the internet.

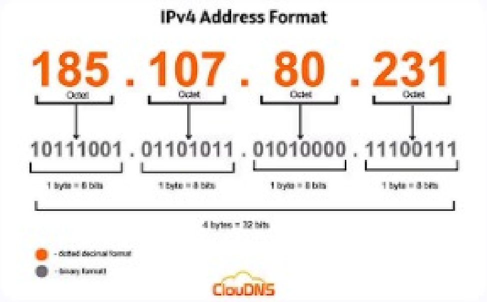
Address Formats

IP addresses come in two primary versions: IPv4 (32-bit) and the newer IPv6 (128-bit), each with distinct formats and capabilities.

Hierarchical Structure

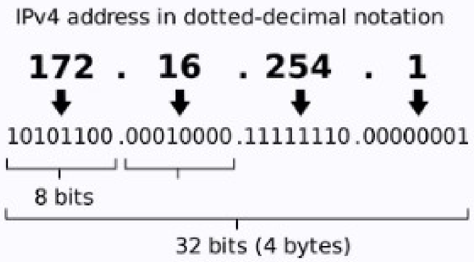
IP addresses follow a hierarchical structure, allowing for efficient routing and management of network traffic through logical divisions like subnets.

IPv4 Addressing



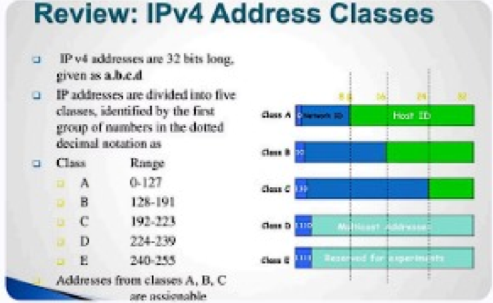
IPv4 Address Format

IPv4 addresses are expressed in dotted-decimal notation, where four octets (8-bit numbers) are separated by periods. This format allows for over 4 billion unique addresses in the IPv4 space.



Address Structure

IPv4 addresses are composed of a network portion and a host portion. The network portion identifies the logical network, while the host portion identifies a specific device within that network.



Review: IPv4 Address Classes

- IP v4 addresses are 32 bits long, given as **a.b.c.d**
- IP addresses are divided into five classes, identified by the first group of numbers in the dotted decimal notation as

Class	Range
A	0-127
B	128-191
C	192-223
D	224-239
E	240-255

- Addresses from classes A, B, C are assignable

8
16
24
32
Class A
0
Network ID
Host ID
Class B
10
Class C
110
Class D
1110
Multicast Address
Class E
1111
Reserved for experiments

Address Ranges

IPv4 addresses are divided into different classes (A, B, C, D, and E) based on the network and host portions. This classification scheme helps organize and manage the address space efficiently.

IPv4 Address Classes

1

Class A

Reserved for large networks with a high number of hosts. Uses the first octet to identify the network, leaving the remaining three octets for host addresses.

2

Class B

Designed for medium-sized networks. The first two octets identify the network, and the last two octets are used for host addresses.

3

Class C

Intended for smaller networks. The first three octets identify the network, leaving only the last octet for host addresses.

4

Class D and Class E

Class D is reserved for multicast addresses, while Class E is reserved for experimental and future use.

Subnet Masks and Subnetting

Subnet Masks

A subnet mask is a 32-bit number that defines the network and host portions of an IP address. It determines which part of the address belongs to the network and which part belongs to the host.

Subnetting

Subnetting is the process of dividing a larger network into smaller, more manageable subnetworks. This allows for more efficient use of IP addresses and improved network performance.

CIDR Notation

Classless Inter-Domain Routing (CIDR) notation is a compact way of representing subnet masks. It specifies the number of bits in the subnet mask, such as /24 for a 255.255.255.0 subnet mask.

CIDR Notation

Definition

CIDR (Classless Inter-Domain Routing) notation is a way to represent and manage IP addresses and subnets more efficiently than the traditional class-based system.

Format

CIDR notation combines the IP address and subnet mask into a single value, expressed as an IP address followed by a forward slash and the subnet prefix length (e.g., 192.168.1.0/24).

Benefits

CIDR allows for flexible subnet sizing, efficient use of IP address space, and better routing table management, making it a key concept in modern network design and administration.

Prefix Length

The prefix length indicates the number of bits in the subnet mask that are set to 1, representing the network portion of the IP address.

MAC Addressing

Uniquely Identified

Media Access Control (MAC) addresses are unique identifiers assigned to network interface cards (NICs) in devices, enabling direct communication on a local network.

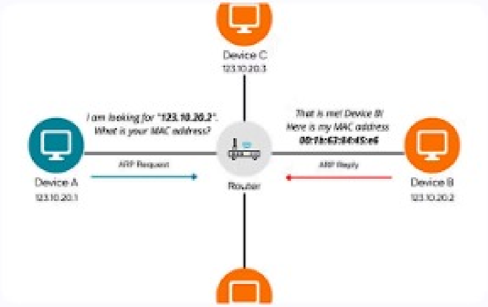
Hierarchical Structure

MAC addresses are 48-bit hexadecimal numbers, typically written in the format XX:XX:XX:XX:XX:XX, with the first 24 bits representing the manufacturer and the last 24 bits the unique device identifier.

Physical Layer Addressing

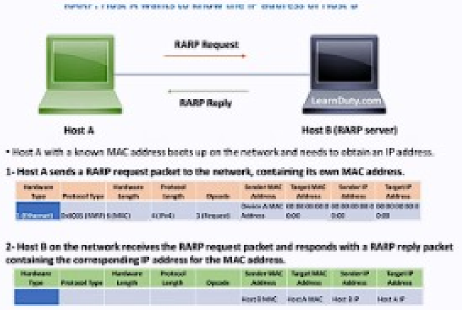
MAC addresses operate at the data link layer (Layer 2) of the OSI model, providing a direct means of addressing devices on the same network segment, without the need for routing or IP addressing.

ARP and RARP



ARP (Address Resolution Protocol)

ARP is a protocol that maps a device's IP address to its corresponding MAC address on a local network. It enables communication between devices by translating logical IP addresses into physical MAC addresses.



RARP : Host A wants to know the IP address of Host B

- Host A with a known MAC address boots up on the network and needs to obtain an IP address.

1- Host A sends a RARP request packet to the network, containing its own MAC address.

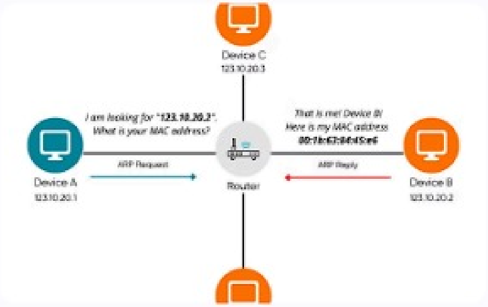
Hardware Type	Protocol Type	Hardware Length	Protocol Length	Opcode	Sender MAC Address	Target MAC Address	Sender IP Address	Target IP Address
1 (Ethernet)	0x8035 (RARP)	6 (MAC)	4 (IPv4)	3 (Request)	Device A MAC Address	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00

2- Host B on the network receives the RARP request packet and responds with a RARP reply packet containing the corresponding IP address for the MAC address.

Hardware Type	Protocol Type	Hardware Length	Protocol Length	Opcode	Sender MAC Address	Target MAC Address	Sender IP Address	Target IP Address
					Host B MAC	Host A MAC	Host B IP	Host A IP

RARP (Reverse ARP)

RARP is the reverse process of ARP, allowing a device to discover its own IP address by providing its MAC address. This is useful for diskless workstations that need to obtain an IP address during the boot process.



ARP and RARP in Action

ARP and RARP work together to facilitate communication on a network by resolving IP and MAC addresses, enabling devices to find each other and exchange data effectively.

Conclusion and Key Takeaways

Comprehensive Concepts

IP addressing, subnetting, MAC addressing, and ARP/RARP provide the fundamental building blocks for understanding network communication and management.

Practical Application

Mastering these concepts is crucial for network administrators, IT professionals, and anyone working with computer networks.

Ongoing Relevance

As networks continue to evolve, these core networking principles remain essential for designing, troubleshooting, and optimizing modern network infrastructures.