IP Addressing and Subnetting: A Comprehensive Guide for IPv4 and IPv6

1 Introduction

An IP address uniquely identifies devices on a network, enabling communication across the internet or local networks. IPv4, with its 32-bit addresses, has been the backbone of networking but faces address exhaustion. IPv6, with 128-bit addresses, provides a vast address space to meet modern demands. Subnetting divides networks into smaller subnetworks, enhancing efficiency, security, and management. This document explains IP addressing and subnetting for both IPv4 and IPv6, covering natural masks, subnet masks, CIDR notation, and host calculations, with practical examples for network design.

2 IPv4 Addressing

2.1 Structure

IPv4 addresses are 32-bit numbers, expressed in dotted-decimal notation (e.g., 192.168.1.1), where each octet represents 8 bits. The address comprises a network portion, identifying the network, and a host portion, identifying a device within that network.

2.2 Classes and Natural Masks

IPv4 addresses are divided into classes based on the first octet, each with a default subnet mask, known as the natural mask:

- **Class A**: 1–126 (e.g., 10.0.0.0), mask 255.0.0.0 (/8), 16,777,214 hosts.
- **Class B**: 128–191 (e.g., 172.16.0.0), mask 255.255.0.0 (/16), 65,534 hosts.
- **Class C**: 192–223 (e.g., 192.168.0.0), mask 255.255.255.0 (/24), 254 hosts.
- **Class D**: 224–239, used for multicast.
- **Class E**: 240–255, reserved.

Note: 127.0.0.0 is reserved for loopback.

2.3 Subnet Masks and CIDR

A subnet mask (e.g., 255.255.255.0) separates the network and host portions. In binary, 1s represent network bits, and 0s represent host bits. CIDR notation (e.g., /24) indicates the

number of network bits, allowing flexible subnet sizing beyond class boundaries (Microsoft Learn).

2.4 Subnetting

Subnetting divides a network into smaller subnetworks by borrowing host bits. For a network with prefix length n, borrowing m bits creates a new prefix length of $n+m$. The formulas are:

- Number of subnets: 2^m
- Host bits: $32-(n+m)$
- Total hosts per subnet: $2^{\text{host bits}}$
- Usable hosts: $2^{\text{host bits}}-2$ (for prefixes < 31)

For example, for 192.168.1.0/24, borrowing 2 bits (new prefix /26):

- Subnets: $2^2=4$
- Host bits: $32-26=6$
- Total hosts: $2^6=64$
- Usable hosts: $64-2=62$

The subnets are:

- 192.168.1.0/26 (0–63, usable: 1–62)
- 192.168.1.64/26 (64–127, usable: 65–126)
- 192.168.1.128/26 (128–191, usable: 129–190)
- 192.168.1.192/26 (192–255, usable: 193–254)

2.5 Example

For 192.168.10.0/26:

- Host bits: $32-26=6$
- Total hosts: $2^6=64$
- Usable hosts: $64-2=62$
- Range: 192.168.10.0 (network) to 192.168.10.63 (broadcast), usable: 192.168.10.1–192.168.10.62

3 IPv6 Addressing

3.1 Structure

IPv6 addresses are 128-bit numbers in hexadecimal, divided into eight 16-bit groups separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334). Leading zeros can be

omitted, and consecutive zero groups can be replaced with "::" once (subnettingpractice.com). The address typically includes a 64-bit network prefix (48-bit global routing prefix + 16-bit subnet ID) and a 64-bit interface ID.

3.2 Types

IPv6 addresses include:

- **Unicast**: Identifies a single interface.
- **Multicast**: Identifies a group of interfaces.
- **Anycast**: Identifies a set of interfaces, with delivery to the nearest.

Special addresses include fe80::/10 (link-local), ::1/128 (loopback), and 2001:db8::/32 (documentation).

3.3 Subnetting

IPv6 subnetting uses a /64 prefix for end hosts, as recommended by the IETF, providing 2^{64} addresses per subnet. Organizations often receive a /48 prefix, allowing $2^{64-48} = 65,536$ /64 subnets (ipcisco.com). Subnetting focuses on route summarization and management, not address conservation. For a prefix length p subnetted to s:

- Subnets: 2^{s-p}
- Hosts per /64: 2^{64}

For example, a /48 prefix to /64 subnets:

- Subnets: $2^{64-48} = 65,536$
- Subnets range: 2001:db8:1234:0000::/64 to 2001:db8:1234:ffff::/64
- Hosts per subnet: 2^{64}

3.4 Example

For 2001:db8:abcd:0012::/64:

- Total hosts: $2^{128-64} = 2^{64}$
- Range: 2001:db8:abcd:0012:0000:0000:0000:0000 to 2001:db8:abcd:0012:ffff:ffff:ffff:ffff

4 Comparison of IPv4 and IPv6 Subnetting

- **Address Space**: IPv4 (32 bits, 4.3 billion addresses) vs. IPv6 (128 bits, vast address space).
- **Notation**: IPv4 uses dotted-decimal and subnet masks; IPv6 uses hexadecimal and prefix length.
- **Subnetting Purpose**: IPv4 conserves addresses; IPv6 focuses on organization and scalability.

- **Usable Hosts**: IPv4 subtracts network and broadcast addresses; IPv6 typically uses all addresses in a /64 subnet.

5 Practical Assignment

5.1 Creating Subnets with Natural Masks

In IPv4, natural masks are the default class masks (/8, /16, /24). To create subnets, adjust the prefix length. For example, for 172.16.0.0/16 (Class B):

- Natural mask: /16, 65,534 usable hosts.
- Subnet to /18: $2^{18-16} = 4$ subnets, each with $2^{32-18} - 2 = 16,382$ usable hosts.

In IPv6, use /64 prefixes. For a /48 prefix, create 65,536 /64 subnets.

5.2 Using Subnet Masks and CIDR

For IPv4, convert subnet masks to CIDR (e.g., 255.255.255.192 = /26). For IPv6, use slash notation (e.g., /64). Calculate subnets and hosts as shown above.

5.3 Counting Hosts

For a given IP range:

- **IPv4 Example**: 192.168.10.0/27
  - Host bits: $32 - 27 = 5$
  - Total hosts: $2^5 = 32$
  - Usable hosts: $32 - 2 = 30$
  - Range: 192.168.10.0–192.168.10.31
- **IPv6 Example**: 2001:db8:abcd:0012::/64
  - Total hosts: 2^{64}
  - Usable hosts: Typically all 2^{64}

6 IPv4 Subnet Reference Table

Prefix	Subnet Mask	Total Hosts	Usable Hosts
/24	255.255.255.0	256	254
/25	255.255.255.128	128	126
/26	255.255.255.192	64	62
/27	255.255.255.224	32	30
/28	255.255.255.240	16	14

Table 1: Common IPv4 subnet sizes and host counts.

7 IPv6 Subnet Reference Table

Prefix	/64 Subnets (from /48)	Hosts per /64
/48	65,536 (2^{16})	2^{64}
/56	256 (2^{8})	2^{64}
/64	1	2^{64}

Table 2: IPv6 subnet counts from a /48 prefix.

8 Conclusion

Understanding IP addressing and subnetting is crucial for network design. IPv4 and IPv6 differ significantly in structure and approach, but both enable efficient network management through subnetting. This guide provides the tools to create subnets, use CIDR notation, and calculate host counts, supporting practical network assignments.

References

[1] Microsoft Learn, "TCP/IP Addressing and Subnetting," https://learn.microsoft.com/en-us/troubleshoot/windows-client/networking/tcpip-addressing-and-subnetting.

[2] Subnettingpractice.com, "How to Subnet IPv6," https://subnettingpractice.com/how-to-subnet-ipv6.html.

[3] IPCisco, "IPv6 Subnetting," https://ipcisco.com/lesson/subnetting-in-ipv6/.

[4] RFC 950, "Internet Standard Subnetting Procedure," https://tools.ietf.org/html/rfc950.

[5] RFC 4291, "IP Version 6 Addressing Architecture," https://tools.ietf.org/html/rfc4291.

Basics of MAC Addressing and Functionality of ARP & RARP

1 Introduction

In computer networking, seamless communication between devices relies on precise addressing mechanisms. The Media Access Control (MAC) address, Address Resolution Protocol (ARP), and Reverse Address Resolution Protocol (RARP) are critical components that facilitate this process. MAC addresses provide unique identifiers for network interfaces, while ARP and RARP handle the translation between IP and MAC addresses. This document explores the fundamentals of MAC addressing and the operational details of ARP and RARP, emphasizing their roles in enabling efficient network communication. Understanding these concepts is essential for networking professionals, as they form the backbone of local area network (LAN) operations.

2 MAC Addressing

2.1 Definition

A Media Access Control (MAC) address is a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment. It is integral to IEEE 802 networking technologies, including Ethernet, Wi-Fi, and Bluetooth, and operates at the medium access control sublayer of the data link layer in the Open Systems Interconnection (OSI) model (MAC address - Wikipedia). Often referred to as a burned-in address, Ethernet hardware address, or physical address, the MAC address ensures accurate data delivery within a local network.

2.2 Structure and Format

MAC addresses are 48 bits long, represented as six groups of two hexadecimal digits, separated by hyphens, colons, or no separator (e.g., 01-23-45-67-89-AB). The first 24 bits (three octets) form the Organizationally Unique Identifier (OUI), assigned by the IEEE to manufacturers, while the remaining 24 bits are vendor-specific, ensuring global uniqueness (What is MAC Address? - GeeksforGeeks). The IEEE manages the 48-bit address space (EUI-48), which supports over 281

trillion possible addresses, with a transition to EUI-64 for non-Ethernet applications (IEEE EUI Tutorial).

2.3 Assignment and Types

MAC addresses are categorized based on their assignment:

- **Universally Administered Address (UAA)**: Assigned by the device manufacturer, with the first three octets as the OUI. The second-least-significant bit of the first octet is 0.
- **Locally Administered Address (LAA)**: Assigned by a network administrator or software, overriding the burned-in address. The second-least-significant bit is 1 (MAC address - Wikipedia).

MAC addresses can be changed using utilities like `ifconfig` on Unix-like systems, and modern operating systems (e.g., iOS, Android, Windows 10) may randomize MAC addresses to enhance privacy.

2.4 Unicast, Multicast, and Broadcast

MAC addresses support different communication types:

- **Unicast**: Targets a single device, with the least significant bit of the first octet set to 0.
- **Multicast**: Targets multiple devices, with the least significant bit set to 1, allowing configurable group communication.
- **Broadcast**: Uses the address FF:FF:FF:FF:FF:FF, received by all devices on the LAN (What is MAC Address? - GeeksforGeeks).

The following table summarizes MAC address ranges based on the Universal/Local (U/L) and Individual/Group (I/G) bits:

U/L I/G	Universally Administered	Locally Administered
Unicast (0)	X0-XX-XX-XX-XX-XX, X4-XX-XX-XX-XX, X8-XX-XX-XX-XX, XC-XX-XX-XX-XX	X2-XX-XX-XX-XX-XX, X6-XX-XX-XX-XX, XA-XX-XX-XX-XX-XX, XE-XX-XX-XX-XX
Multicast (1)	X1-XX-XX-XX-XX-XX, X5-XX-XX-XX-XX, X9-XX-XX-XX-XX, XD-XX-XX-XX-XX	X3-XX-XX-XX-XX-XX, X7-XX-XX-XX-XX, XB-XX-XX-XX-XX-XX, XF-XX-XX-XX-XX

Table 1: MAC Address Ranges

2.5 Applications

MAC addresses are used in IEEE 802 networks (Ethernet, Wi-Fi), as well as in FireWire, InfiniBand, and IPv6 (using modified EUI-64). They are critical for network virtualization, MAC spoofing, and device identification, though their lack of encryption makes them vulnerable to interception (What is MAC Address? - GeeksforGeeks).

3 Address Resolution Protocol (ARP)

3.1 Definition

The Address Resolution Protocol (ARP) is a communication protocol that maps a known IPv4 address to a MAC address within a local network. Defined in 1982 by RFC 826 (RFC 826), ARP is a cornerstone of the Internet protocol suite, operating between Layer 2 (data link) and Layer 3 (network) of the OSI model (Address Resolution Protocol - Wikipedia). It enables devices to communicate by resolving the MAC address needed for data link layer transmission.

3.2 How ARP Works

ARP facilitates communication by translating IP addresses to MAC addresses through the following steps:

1. **Cache Check**: The sending device checks its ARP cache for the MAC address corresponding to the destination IP address.
2. **ARP Request**: If no entry exists, the device broadcasts an ARP request packet containing the destination IP address to all devices on the LAN.
3. **ARP Reply**: The device with the matching IP address responds with its MAC address.
4. **Cache Update**: The sender updates its ARP cache with the IP-to-MAC mapping and proceeds with communication (How Address Resolution Protocol (ARP) Works? - GeeksforGeeks).

ARP requests are sent to the broadcast address (FF:FF:FF:FF:FF:FF for Ethernet), ensuring all devices on the subnet receive the request. The ARP cache has a limited size, with entries typically retained for a few minutes to optimize performance (What is Address Resolution Protocol (ARP)? - TechTarget).

3.3 ARP Message Format

ARP messages are carried as raw payload at the data link layer, identified by EtherType 0x0806 in Ethernet. The packet structure for IPv4 over Ethernet (28 bytes) includes:

This structure ensures compatibility across various network technologies, including FDDI, X.25, and ATM (Address Resolution Protocol - Wikipedia).

3.4 Role in Networking

ARP is critical for enabling communication within a LAN, as it bridges the gap between logical IP addresses and physical MAC addresses. Without ARP, devices would be unable to send data packets to the correct hardware destination, disrupting network operations (ARP Protocol - GeeksforGeeks).

Field	Bits	Description
Hardware Type (HTYPE)	16	Specifies network link protocol (1 for Ethernet).
Protocol Type (PTYPE)	16	Internetwork protocol (0x0800 for IPv4).
Hardware Length (HLEN)	8	Length of hardware address (6 octets for Ethernet)
Protocol Length (PLEN)	8	Length of internetwork address (4 octets for IPv4).
Operation (OPER)	16	1 for request, 2 for reply.
Sender Hardware Address (SHA)	48	Media address of sender.
Sender Protocol Address (SPA)	32	Internetwork address of sender.
Target Hardware Address (THA)	48	Media address of receiver (ignored in request).
Target Protocol Address (TPA)	32	Internetwork address of receiver.

Table 2: ARP Message Format

4 Reverse Address Resolution Protocol (RARP)

4.1 Definition

The Reverse Address Resolution Protocol (RARP) is an obsolete protocol that maps a MAC address to an IPv4 address. Introduced in 1984 by RFC 903 (RFC 903), RARP was designed for devices, such as diskless workstations, that lack the ability to store an IP address and need to request one from a server (Reverse Address Resolution Protocol - Wikipedia).

4.2 How RARP Works

RARP operates as follows:

1. **RARP Request**: A device broadcasts a RARP request containing its MAC address to all devices on the LAN.
2. **Server Response**: A RARP server, maintaining a table of MAC-to-IP mappings, responds with the corresponding IP address.
3. **Configuration**: The requesting device configures itself with the received IP address for network communication (What is RARP? - GeeksforGeeks).

RARP requests are broadcast to the network, and only designated RARP servers respond. The server's response is typically unicast to the requesting device.

4.3 Differences from ARP

The primary difference between ARP and RARP lies in their mapping direction:

- **ARP**: Maps a 32-bit IP address to a 48-bit MAC address, used when a device knows the destination IP but needs the MAC address.
- **RARP**: Maps a 48-bit MAC address to a 32-bit IP address, used when a device knows its MAC address but needs an IP address (Difference between ARP and RARP - GeeksforGeeks).

RARP is limited to IP address assignment and requires manual configuration of MAC-to-IP mappings on the server, making it less flexible than modern protocols.

4.4 Current Status

RARP is obsolete, having been superseded by the Bootstrap Protocol (BOOTP) and Dynamic Host Configuration Protocol (DHCP), which offer dynamic IP allocation and additional configuration options. However, RARP's concepts are still relevant in specific contexts, such as MAC migration in virtual machines (Reverse Address Resolution Protocol - Wikipedia).

5 Conclusion

MAC addressing, ARP, and RARP are foundational to local network communication. MAC addresses provide unique identifiers for network interfaces, ensuring precise data delivery. ARP enables devices to map IP addresses to MAC addresses, facilitating seamless LAN communication. RARP, though obsolete, historically allowed devices to obtain IP addresses using their MAC addresses, paving the way for more advanced protocols like DHCP. Understanding these mechanisms is crucial for networking professionals, as they underpin the functionality of modern network architectures.