IP Addresses

Ashish Pratap Singh

Every time you visit a website, send an email, or make an API call, your device uses an **IP address** to identify itself.

This address ensures that the data you request finds its way back to you, and the data you send reaches its intended destination.

The **Internet Protocol (IP)** is the set of rules that governs this addressing system. It operates at Layer 3 (the Network Layer) of the OSI Model, where its primary job is to provide logical addressing and route packets of data from a source device to a destination device across one or more networks.

1. What Is an IP Address?

An **IP address** is a unique numerical label assigned to each device connected to a network that uses the Internet Protocol for communication. Think of it as a phone number for your computer or a mailing address for your laptop.

It serves two primary functions:

1. **Identification**: It uniquely identifies a device (or more accurately, a network interface) on the network. This tells other devices who is sending or receiving information.
2. **Location Addressing**: It specifies the location of the device in the network, providing a path for data to be delivered.

Real-World Analogy: Postal System

Your IP address is like your home address. The street name and city identify your neighborhood (the network), while your house number identifies your specific home (the device).

Mail carriers (routers) use this address to deliver packages (data packets) to the correct location.

2. IP Address Structure

An IP address isn't just a random number; it has a clear structure that is split into two main parts:

- **Network ID**: This part of the address identifies the specific network the device is on. All devices on the same local network share the same Network ID.
- **Host ID**: This part of the address identifies a specific device (like a computer, server, or smartphone) within that network.

For example, in the common IPv4 address `192.168.1.10` with a standard subnet mask, the breakdown is:

- **Network ID**: `192.168.1`
- **Host ID**: `10`

Routers primarily look at the **Network ID**. They don't need to know about every single device in the world, only which network a packet is destined for. They use this information to forward the packet to the next router closer to the destination network.

---

3. IPv4: The Classic Address Format

Internet Protocol version 4 (IPv4) is the original and most widely used IP addressing system.

It's a **32-bit** address, meaning there are 232 (approximately 4.3 billion) possible unique addresses.

Format

It is written as four numbers separated by dots (dotted-decimal notation), where each number is an "octet" ranging from 0 to 255 (e.g., `172.217.167.78`).

Address Classes

Historically, IPv4 addresses were divided into classes (A, B, C) to define the split between network and host IDs. While this system is now largely replaced by CIDR (see below), it's useful historical context.

- **Class A**: For very large networks (e.g., `10.0.0.0`).
- **Class B**: For medium-sized networks (e.g., `172.16.0.0`).
- **Class C**: For small networks (e.g., `192.168.1.0`).

Limitation

The biggest issue with IPv4 is **address exhaustion**. With the explosion of internet-connected devices, the ~4.3 billion addresses have effectively run out.

---

4. IPv6: The Modern Standard

To solve the address exhaustion problem, **Internet Protocol version 6 (IPv6)** was developed.

It's a **128-bit** address, providing a staggering 2128 (or 340 undecillion) unique addresses. This is enough to assign an IP address to every atom on the surface of the Earth, and still have addresses left over.

Format

It is written as eight groups of four hexadecimal digits, separated by colons (e.g., `2001:0db8:85a3:0000:0000:8a2e:0370:7334`). Zeros can be compressed for brevity.

IPv6 isn't just bigger; it's better. It includes several built-in improvements:

- **Stateless Address Autoconfiguration (SLAAC)**: Devices can generate their own IP address without needing a DHCP server.
- **No NAT**: The massive address space eliminates the need for Network Address Translation (NAT), simplifying networks.
- **Built-in Security**: IPsec, a suite of protocols for securing communications, is a mandatory part of IPv6.
- **Efficient Routing**: Simplified packet headers allow for faster processing by routers.

---

5. Public vs Private IP Addresses

Not all IP addresses are created equal. They are divided into two main categories:

- **Public IP Address**: This is a globally unique address that is routable on the internet. Your Internet Service Provider (ISP) assigns one to your router. When you visit a website, your request is sent from your public IP.
- **Private IP Address**: This is an address used within a local, private network (like your home Wi-Fi or an office LAN). These addresses are not routable on the internet and are reused in millions of private networks worldwide.

The standard private IP ranges are:

- **10.0.0.0** to **10.255.255.255**
- **172.16.0.0** to **172.31.255.255**
- **192.168.0.0** to **192.168.255.255**

So how do devices with private IPs access the internet?

Through **Network Address Translation (NAT)**.

Your home router acts as a NAT gateway. It takes requests from devices on your private network, replaces their private source IP with its single public IP, and sends the request to the internet. When the response comes back, the router knows which private device to forward it to.

---

6. Static vs Dynamic IP Addresses

IP addresses can be assigned in two ways:

- **Static IP**: A static IP address is manually configured for a device and does not change. This is essential for servers, printers, and other devices that need to be consistently reachable at the same address. They are reliable but often cost more and require manual management.
- **Dynamic IP**: A dynamic IP address is assigned automatically by a **DHCP (Dynamic Host Configuration Protocol)** server. Most consumer devices (laptops, phones) get dynamic IPs. The address is leased for a period and can change the next time you connect. This is highly efficient for managing large numbers of devices.

---

7. Subnetting and CIDR

As networks grow, it's often necessary to divide them into smaller, more manageable segments. This process is called **subnetting**. It helps improve performance, enhance security, and organize the network logically.

Subnetting involves "borrowing" bits from the Host ID part of an IP address to create more Network IDs. A **subnet mask** is used to tell devices which part of the address is the network and which is the host.

This is where **CIDR (Classless Inter-Domain Routing)** comes in. CIDR abandoned the old classful system and introduced a more flexible way to define the network portion of an address. CIDR notation uses a slash followed by a number to represent the number of bits in the Network ID.

- `192.168.1.0/24` means the first 24 bits are the Network ID.
  - Subnet Mask: `255.255.255.0`
  - Hosts: 254
- `192.168.1.0/26` means the first 26 bits are the Network ID.
  - Subnet Mask: `255.255.255.192`
  - This splits the `/24` network into four smaller subnets, each with 62 hosts.

---

8. Loopback and Special Addresses

Besides public and private addresses, there are several special-purpose IP addresses:

- **Loopback Address**: `127.0.0.1` (IPv4) and `::1` (IPv6). This address, also known as "localhost," always refers to the local device itself. It's used for testing network applications without sending packets out onto the network.
- **Broadcast Address**: An address used to send a message to all devices on a local subnet simultaneously (e.g., `192.168.1.255` for the `192.168.1.0/24` network).
- **Link-local Address**: The `169.254.0.0/16` range. If a device is configured for DHCP but cannot find a DHCP server, it will assign itself an address from this range to communicate on the local network.
- **Multicast Addresses**: A special block of addresses used for one-to-many communication, where a single packet is sent to a "group" of interested receivers.