IP Address (Internet Protocol Address)

What is an IP Address?

An **IP address** is a **unique identifier** assigned to each device on a network that uses the **Internet Protocol** to communicate. It acts like a **digital address** to send/receive data.

Just like your **home address** tells where to deliver a letter, your **IP address** tells where to send data online.

Two Main Versions of IP

Type	Full Form	Address Format	Total Addresses
IPv4	Internet Protocol v4	4 blocks (e.g. 192.168.1.1)	~4.3 billion (32-bit)
IPv6	Internet Protocol v6	8 blocks (e.g. 2001:0db8::1)	~340 undecillion (128-bit)

IPv4 Address Structure:

Example: 192.168.1.10

- Each block is called an **octet** (8 bits)
- Separated by **dots**
- Ranges from 0.0.0.0 to 255.255.255.255

IPv6 Address Structure:

Example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

- 8 groups of 4 hexadecimal digits
- Much larger address space
- Designed to replace IPv4

Types of IP Addresses

1. Based on Use:

Type	Purpose	Example
Private IP	Used within a local network	192.168.0.1
Public IP	Globally unique, internet-facing	49.207.65.101

Private IPs can't access the internet directly — need **NAT** via a router.

2. Based on Assignment:

Type	**Who Assigns?**	**Description**
Static IP	Manually assigned	Doesn't change; used for servers
Dynamic IP	Assigned by DHCP	Changes periodically (default for most)

Reserved Private IP Ranges (IPv4)

Class	**IP Range**	**Example Device Use**
A	10.0.0.0 – 10.255.255.255	Large LANs, Enterprises
B	172.16.0.0 – 172.31.255.255	Medium Networks
C	192.168.0.0 – 192.168.255.255	Homes & Small offices

IP Address Classes (Legacy, IPv4 only)

Class	**Range**	**Purpose**	**Hosts**
A	1.0.0.0 – 126.255.255.255	Large Networks	16 million
B	128.0.0.0 – 191.255.255.255	Medium Networks	65,000+
C	192.0.0.0 – 223.255.255.255	Small Networks	254
D	224.0.0.0 – 239.255.255.255	Multicast	-
E	240.0.0.0 – 255.255.255.255	Experimental	-

IP & Cyber Security:

Concern	Role of IP Address
IP Spoofing	Attacker fakes source IP to fool systems
Blacklisting	Block bad IPs to stop spam/attacks
Geolocation	Find region based on IP
DDoS Attacks	Attack many IPs or from fake ones

Tools to Check/Use IP Address:

Tool/Command	Purpose
ipconfig (Windows)	Show IP, subnet, gateway
ifconfig / ip a (Linux)	Show IP settings
Websites like whatismyip.com	Shows your public IP
ping <IP>	Test connectivity
tracert / traceroute	Track route to a remote IP

Subnetting (Advanced)

- Breaks an IP network into **smaller sub-networks**
- Uses **CIDR notation**, e.g., /24 (means 256 IPs)
- Helps in **efficient IP address management**
- Example: 192.168.1.0/24 gives 254 usable addresses

Example in Real Life:

You're at home:

- Your phone gets **192.168.0.2** (private IP)
- Your router has **49.207.65.101** (public IP)
- Router uses **NAT** to forward traffic between both

Summary Mind Map (Text Format):

IP Address

├── Versions: IPv4, IPv6

├── Types

| ├── Public / Private

| ├── Static / Dynamic

├── Tools: ipconfig, ping, traceroute

├── Classes: A, B, C, D, E

├── Use in Security: Spoofing, DDoS, Blacklist

├── Subnetting: CIDR (/24, /16 etc.)

Why IP Addresses Use 0–255

IP addresses (IPv4) are made up of 4 numbers (called octets), like this:

192.168.1.10

Each number (octet) in this format can range from **0 to 255**.

Reason: Binary System

Each **octet** is an **8-bit binary number**.

Bits	Total Possible Values
8	28=2562^8 = 25628=256 values

That means:

- 8 bits can represent **256 different combinations**
- But counting starts from **0**, not 1
- So the range is:

0 to 255=256 values0 \text{ to } 255 = 256 \text{ values}0 to 255=256 values

Binary to Decimal Example:

Binary (8-bit)	Decimal
00000000	0
00000001	1
11111111	255

So the maximum number you can represent with 8 bits is 255.

Structure of IPv4:

- IPv4 has **4 octets** (32 bits total)
- Example: 192.168.0.1
  - 192 → 8 bits
  - 168 → 8 bits
  - 0 → 8 bits
  - 1 → 8 bits

That's why **each block is limited from 0 to 255**.

Real-World Analogy:

Imagine you have a digital **counter with 8 switches** (each can be ON or OFF):

- You can make **256 combinations** (like binary counting)
- First is all OFF → 0
- Last is all ON → 255

⚠️ Note:

Not all 0–255 addresses are **usable**:

- 0.0.0.0 = special meaning (default route)
- 255.255.255.255 = broadcast
- Network and broadcast addresses in subnets are **reserved**

Final Summary:

Reason	**Explanation**
Binary math	8 bits = 2^8 = 256 values
Valid range	Starts from 0 → ends at 255
IP format	Each of the 4 parts (octets) uses this range

What is IPv6?

IPv6 stands for **Internet Protocol version 6** — it's the **newer version of IP**, designed to replace **IPv4** due to **IP address exhaustion**.

The world is running out of IPv4 addresses (only ~4.3 billion), so IPv6 was introduced to handle the **huge number of devices** connected today (phones, IoT, sensors, etc.).

IPv6 Address Format

An **IPv6 address** is:

- **128 bits long**
- Written in **hexadecimal (base 16)** format
- Divided into **8 groups**, separated by **colons :**

Example:

2001:0db8:85a3:0000:0000:8a2e:0370:7334

Each group is called a **hextet** (16 bits = 4 hex digits).
IPv6 can represent **2^{128} addresses** ≈ **340 undecillion** (that's 340 followed by 36 zeros!)

IPv6 Shortening Rules (Simplified Format)

IPv6 allows simplification:

1. **Leading zeros** in a block can be **removed**
2. Consecutive 0000 blocks can be replaced with **double colon ::** (only once)

Example:

Original:

makefile

2001:0db8:0000:0000:0000:0000:abcd:1234

Shortened:

2001:db8::abcd:1234

Structure of an IPv6 Address

Section	**Bits**	**Purpose**
Global Routing Prefix	First 48 bits	Network identification
Subnet ID	Next 16 bits	Internal subnetwork
Interface ID	Last 64 bits	Device identification

IPv4 vs IPv6 Comparison

Feature	**IPv4**	**IPv6**
Length	32-bit	128-bit
Format	Decimal (e.g., 192.168.0.1)	Hexadecimal (e.g., 2001:db8::1)
Address Space	~4.3 billion	~340 undecillion
NAT Required	Yes (for private IPs)	No (end-to-end addressing possible)
Broadcast	Yes	No (uses multicast instead)
Security (IPSec)	Optional	**Built-in**

IPv6 in Cybersecurity

Feature	Benefit
No NAT	True end-to-end communication, easier encryption
IPSec Mandatory	Encrypts data at IP level by default
No Broadcast	Reduces DDoS attack surface
Unique Global Addresses	Makes tracking easier and also raises privacy concerns

Real-Life Examples of IPv6 Usage

Scenario	IPv6 Use
Smartphones (Android/iOS)	Support IPv6 over 4G/5G networks
ISPs (like Jio, Airtel, ACT)	Start assigning IPv6 addresses
Google, YouTube, Facebook	Fully support IPv6 access
IoT Devices	Use IPv6 for direct communication

Check Your IPv6 Address (Practical)

Platform	Command
Windows	ipconfig
Linux/Mac	ifconfig or ip a
Web	Visit https://test-ipv6.com

Why IPv6 is the Future

- World population = 8+ billion
- Devices per person = 5–10+
- IPv4 can't scale anymore
- IPv6 = enough addresses for **every grain of sand on Earth** (literally!)

Summary Chart

IPv6 Feature	**Description**
Address Length	128 bits
Notation	Hexadecimal, 8 groups, colon-separated
Simplification	:: for multiple 0s, omit leading 0s
Total Addresses	2^{128} (virtually unlimited)
NAT Usage	Not required
Security	IPSec built-in

What is NAT?

NAT stands for **Network Address Translation**.

Definition:

NAT is a **technique used by routers** to **translate private IP addresses** (used inside a home or office) to a **public IP address** (used on the internet), and vice versa.

NAT allows **many devices** in a private network to share **one public IP** when accessing the internet.

Why NAT is Needed?

Problem:

- **IPv4 has limited addresses** (only ~4.3 billion)
- We have **billions of devices** (phones, TVs, laptops)

Solution:

- Use **Private IP addresses** inside homes/offices (free and reusable)
- Use **NAT** to connect those private devices to the internet through **one public IP**

Real-Life Example: Your Home

Device	**IP Address (Private)**
Laptop	192.168.0.2
Phone	192.168.0.3
Smart TV	192.168.0.4

Your **Wi-Fi router** has:

- **Private IP inside home**: 192.168.0.1
- **Public IP from ISP**: e.g., 49.207.65.101

When your devices access the internet:

- NAT **changes** their private IPs to **your public IP**
- Internet sees only **49.207.65.101**
- NAT keeps track of who requested what

Types of NAT:

Type	**What It Does**	**Example Use**
SNAT (Source NAT)	Changes **source IP** from private to public	Outgoing internet traffic
DNAT (Destination NAT)	Changes **destination IP** for incoming traffic	Hosting servers
PAT (Port Address Translation)	Many devices share one IP using different ports	Home Wi-Fi usage

Benefits of NAT:

Benefit	**Explanation**
Saves IPv4 addresses	Reuses private IPs
Hides internal IP addresses	Adds a layer of **security**
Allows multiple devices to access internet with one IP	Saves money
Enables **internal networking** without global IPs	Useful in homes/offices

Limitations of NAT:

Limitation	**Description**
Breaks **end-to-end communication**	Peer-to-peer apps or video calls may need special handling (like port forwarding)
Not needed in **IPv6**	Because IPv6 has **enough public IPs** for everyone

NAT Diagram (Text version)

```
[Phone] 192.168.0.2     ┐
[Laptop] 192.168.0.3    ├──> [Router with NAT] --> Internet (Public IP)
[TV] 192.168.0.4        ┘      (49.207.65.101)
```

Router keeps a **NAT table**:

Private IP	**Port**	**Public IP**	**Port**
192.168.0.2	2345	49.207.65.101	45001
192.168.0.3	2346	49.207.65.101	45002

Summary Table

Feature	**NAT**
Full Form	Network Address Translation
Main Use	Connect private devices to public internet
Used In	Routers, firewalls, ISPs
Helps With	IP saving, basic security
Needed In IPv4?	Yes
Needed In IPv6?	No (usually)

Easy Analogy:

Think of NAT like a **reception desk** in a company:

- Employees (devices) inside the office (private network)
- Visitors (internet) only see the **reception's number (public IP)**
- Receptionist (router) knows **who called who**