IP

IPv4 was designed as a 32-bit addressing system due to the initial needs and scale of the internet at the time of its development in the late 1970s and early 1980s. Here’s why 32 bits were chosen and the thinking behind this decision:

2^32=4,294,967,296

Four billion, two hundred ninety-four million, nine hundred sixty-seven thousand, two hundred ninety-six.

1. Initial Expectations of the Internet’s Scale
In the early days of networking, there was no expectation that the internet would grow to the massive scale we see today. The designers of IPv4 estimated that a 32-bit address space—allowing for around 4.3 billion unique addresses (2^32 addresses)—would be sufficient for the foreseeable future.

At the time:

- Most networks were isolated (e.g., university and research lab networks), and large-scale commercial and residential use was not anticipated.
- Only a limited number of devices were connected, and the idea of billions of interconnected devices (like IoT devices) was unimaginable.

2. Balance Between Address Space and Efficiency
IPv4 was designed to balance address space size with network processing efficiency. Using a 32-bit address format allowed:

- A sufficient number of addresses for the expected number of networked devices, while keeping address processing efficient, as 32-bit processing was manageable for the hardware of that time.
- A larger address space (e.g., 64-bit) would have required more data storage and processing power, which was costly and difficult to implement with the technology available in the 1970s and 1980s.

3. Compatibility with 32-bit Architecture
The 32-bit structure was compatible with the computer architecture and processing power of the time:

- 32-bit architecture was common in computer systems, so a 32-bit address could be easily handled in a single processing cycle.
- This made routing, packet handling, and network management more efficient and less resource-intensive.

4. Classful Addressing System
IPv4 originally used a classful addressing system, where different address classes (A, B, C) were allocated specific portions of the address space to accommodate networks of various sizes. This structure was deemed sufficient at the time for organizing different types of networks, especially for institutional and government networks, which were the primary users.

Limitations and the Move to IPv6
As the internet rapidly expanded, the limitations of IPv4 became clear:

- IP address exhaustion occurred due to the limited number of IPv4 addresses and the growth of the internet beyond original expectations.
- Network Address Translation (NAT) was introduced to extend IPv4's life by allowing multiple devices to share a single public IP address.
- Ultimately, these limitations led to the development of IPv6, which uses 128 bits for addressing, providing an exponentially larger address space and other improvements suited for modern networking needs.

In summary, IPv4 was designed as a 32-bit protocol to meet the technical and anticipated usage needs of its time, striking a balance between address space, efficiency, and the processing capability of 1970s and 1980s technology.

Structure of an IPv4 Address

An IPv4 address is a 32-bit number, usually represented as four decimal numbers separated by periods (known as "dotted-decimal notation"). Each of the four numbers represents an octet (8 bits), so an IPv4 address looks like this: 192.168.1.1.

Each octet can range from 0 to 255, allowing IPv4 addresses to go from 0.0.0.0 to 255.255.255.255.

Example
For an IP address 192.168.1.10:

192 is the first octet, representing the first 8 bits.
168 is the second octet.
1 is the third octet.
10 is the fourth octet.

Classes of IPv4 Addresses

IPv4 addresses were initially divided into five classes (A, B, C, D, and E) based on the first few bits. This classification, known as classful addressing, helped allocate IP addresses based on the network size.

Class A: For very large networks (e.g., large corporations and ISPs).

Range: 0.0.0.0 to 127.255.255.255
Network bits: 8 bits
Host bits: 24 bits
Default Subnet Mask: 255.0.0.0

Class B: For medium-sized networks (e.g., universities, larger organizations).

Range: 128.0.0.0 to 191.255.255.255
Network bits: 16 bits
Host bits: 16 bits
Default Subnet Mask: 255.255.0.0

Class C: For smaller networks (e.g., small businesses, local networks).

Range: 192.0.0.0 to 223.255.255.255
Network bits: 24 bits
Host bits: 8 bits
Default Subnet Mask: 255.255.255.0

Class D: Used for multicasting.

Range: 224.0.0.0 to 239.255.255.255

Class E: Reserved for experimental purposes.

Range: 240.0.0.0 to 255.255.255.255

Subnetting

Subnetting is a method of dividing a large network into smaller, more manageable subnetworks (subnets). It allows better use of IP address space by using custom subnet masks.

A subnet mask determines which portion of an IP address refers to the network and which part refers to the host.
For example, the subnet mask 255.255.255.0 in a Class C network means the first 24 bits are for the network, and the last 8 bits are for the hosts within that network.
CIDR (Classless Inter-Domain Routing) notation, such as 192.168.1.0/24, indicates how many bits are allocated to the network part. Here, /24 means the first 24 bits are the network, and the rest are for hosts.

Types of IPv4 Addresses

IPv4 addresses can be classified as public or private:

Public IP addresses: Used to connect devices to the internet and are unique across the global network.
Private IP addresses: Used within private networks and cannot be routed on the internet. They allow devices within a local network to communicate with each other.

Private IPv4 Address Ranges:
Class A: 10.0.0.0 to 10.255.255.255 = 16 Million addresses
Class B: 172.16.0.0 to 172.31.255.255 = 1 Million addresses
Class C: 192.168.0.0 to 192.168.255.255 = 65,536 addresses

Special IPv4 Addresses

Loopback address: 127.0.0.1, used by a host to test network configuration. Data sent to this address will loop back to the device itself.

Broadcast address: Used to send data to all devices in a network. In a subnet, the last address is typically the broadcast address **(e.g., 192.168.1.255 in a 192.168.1.0/24 network)**.

APIPA (Automatic Private IP Addressing): 169.254.0.0 to 169.254.255.255, used when a device cannot get an IP from a DHCP server.

Multicast IP Address: Used for sending data to multiple devices simultaneously, within a specified range (**224.0.0.0 to 239.255.255.255** for IPv4).

Class	Address Range	First Octet Range	Default Subnet Mask	Network ID Bits	Host ID Bits	Usage
A	`0.0.0.0` - `127.255.255.255`	`0` - `127`	`255.0.0.0` or `/8`	8	24	Large networks
B	`128.0.0.0` - `191.255.255.255`	`128` - `191`	`255.255.0.0` or `/16`	16	16	Medium networks
C	`192.0.0.0` - `223.255.255.255`	`192` - `223`	`255.255.255.0` or `/24`	24	8	Small networks
D	`224.0.0.0` - `239.255.255.255`	`224` - `239`	None	N/A	N/A	Multicasting
E	`240.0.0.0` - `255.255.255.255`	`240` - `255`	None	N/A	N/A	Experimental

Class	Private IP Range	Default Subnet Mask	Network Size
A	`10.0.0.0` - `10.255.255.255`	`255.0.0.0` or `/8`	Very large networks
B	`172.16.0.0` - `172.31.255.255`	`255.240.0.0` or `/12`	Medium networks
C	`192.168.0.0` - `192.168.255.255`	`255.255.255.0` or `/24`	Small networks