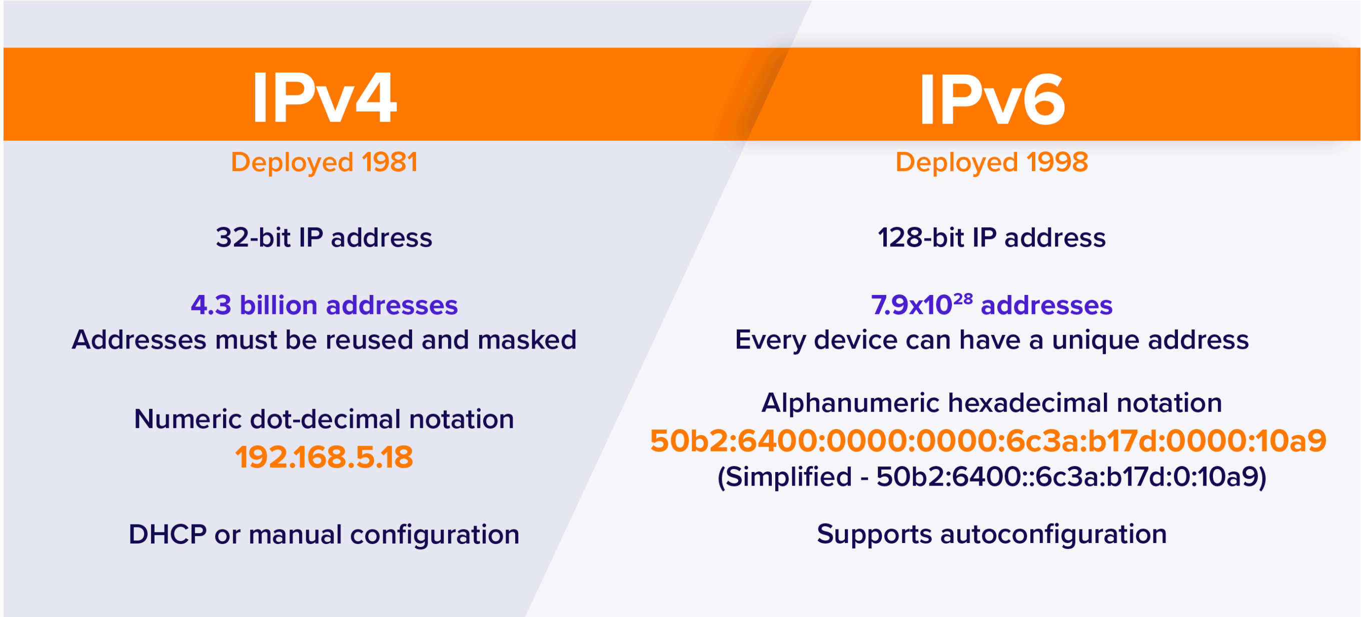
# 7. IPv4, Ipv6



| IPv4 | IPv6 |
|---|---|
| Deployed 1981 | Deployed 1998 |
| 32-bit IP address | 128-bit IP address |
| 4.3 billion addresses<br>Addresses must be reused and masked | $7.9x10^{28}$ addresses<br>Every device can have a unique address |
| Numeric dot-decimal notation<br>192.168.5.18 | Alphanumeric hexadecimal notation<br>50b2:6400:0000:0000:6c3a:b17d:0000:10a9<br>(Simplified - 50b2:6400::6c3a:b17d:0:10a9) |
| DHCP or manual configuration | Supports autoconfiguration |

## IPv4

- IPv4 : Internet protocol version 4
- IPv4 address is of 4 bytes in length each octet of 1 byte.
- In ipv4 their are 4 number separated by dot each of them is called octet. `192.168.1.22`

IP address in binary. 2. Networking Fundamentals > no. to binary
192 = 11000000, 168 = 10101000 , 1 = 00000001 , 22 = 11111110
its difficult to read binary no. so we write it in dotted decimal like this `192.168.1.22`

192.168.1 = network ID
22 = is host ID (only in class c) it change according to classes.
network portion is same in local network only the host address is different .

## IP address classes

Reference

- Total 4,294,967,296 4 billion IPV4 are their. **why only 4 billion ipv4 address?**

> IPv4 addresses are (4 bytes) 32 bits long, which allows for a total of 2^32 possible addresses.

- To **manage** these 4 billion IP `IP address classes` are introduce.
  Here's a table summarizing the IP address classes:

| Class | Range | Leading Bits | Subnet Mask | Hosts per Network | Usage |
|---|---|---|---|---|---|
| A | 0.0.0.0 to 127.255.255.255 | 0 | 255.0.0.0 | ~16 million | Very large networks |
| B | 128.0.0.0 to 191.255.255.255 | 10 | 255.255.0.0 | ~65,000 | Medium to large networks |
| C | 192.0.0.0 to 223.255.255.255 | 110 | 255.255.255.0 | Up to 254 | Small networks |
| D | 224.0.0.0 to 239.255.255.255 | 1110 | N/A | N/A | Multicast address |
| E | 240.0.0.0 to 255.255.255.255 | 1111 | N/A | N/A | Experimental purposes |

## Special Addresses

| Type | Range | Usage |
|---|---|---|
| Private IP Addresses | 10.0.0.0 to 10.255.255.255 | Internal networks |
|  | 172.16.0.0 to 172.31.255.255 | Internal networks |
|  | 192.168.0.0 to 192.168.255.255 | Internal networks |
| Loopback Address | 127.0.0.1 | Testing and internal communications |

| Class | Bits | Network | Host | Subnet Mask |
|---|---|---|---|---|
| A | 8 bits | Network (1st Octet) | 24 bits (3 Octets) | /8 or 255.0.0.0 |
| B | 16 bits | Network (1st & 2nd) | 16 bits (2 Octets) | /16 or 255.255.0.0 |
| C | 24 bits | Network (1st, 2nd, & 3rd) | 8 bits (1 Octet) | /24 or 255.255.255.0 |

| class | starting address | ending address |
|---|---|---|
| A | 0.0.0.0 | 127.255.255.255 |
| B | 128.0.0.0 | 191.255.255.255 |

| class | starting address | ending address |
|---|---|---|
| C | 192.0.0.0 | 223.255.255.255 |

### **question :** PCI has art IP address of `43.109.23.12/8`

Find the following:

1. Network address: 43.0.0.0 `as /8 indicate class A and it have 1 octet of network and 3 are host octet`
2. Maximum number of hosts in the network: 16,777,214 `3 host octet that have 24 bites so max host is 2^24` and sub 2.
3. Network broadcast address: 43.255.255.255 `last addrss of network`
4. First usable address of the network: 43.0.0.1 `first ip - 1 to get first usable ip of network`
5. Last usable address of the network: 43.255.255.254 `last ip - 1 to get last useable ip of network`

## How to find from which class this IP belongs?

To find it see the first Octet of the IP address.
example:
`1.2.3.4` first octet is 1 and it belong to class A.
`191.168.1.12` first octet is 191 and it belong to class B
`192.168.1.12` first octet is 192 and it belong to class C

- The network address CANNOT be assigned to a host.
  network address is first address of network like `192.168.1.1`

## Loopback Address

Address range 127.0.0.0 to 127.255.255.255
Used to test the network stack' (think OSI, TCP/IP model) on the local device.

| Class | First Octet Range | Leading Bits | Prefix Length | Subnet Mask |
|---|---|---|---|---|
| A | 0 - 127 | `0xxxxxxx` | /8 | 255.0.0.0 |
| B | 128 - 191 | `10xxxxxx` | /16 | 255.255.0.0 |
| C | 192 - 223 | `110xxxxx` | /24 | 255.255.255.0 |

### Breakdown:

- **Class A**:
  - **First Octet**: 0 to 127
  - **Prefix Length**: /8 (8 bits for the network)
- **Class B**:
  - **First Octet**: 128 to 191
  - **Prefix Length**: /16 (16 bits for the network)
- **Class C**:
  - **First Octet**: 192 to 223
  - **Prefix Length**: /24 (24 bits for the network)

> Class A have much host and less network
> Class C have much Network and less host.

| Class | Number of Networks | host id | Prefix Length | Subnet Mask |
|---|---|---|---|---|
| Class A | 128 (2^7) | 16,777,216 (2^24) | /8 | 255.0.0.0 |
| Class B | 16,384 (2^14) | 65,536 (2^16) | /16 | 255.255.0.0 |
| Class C | 2,097,152 (2^21) | 256 (2^8) | /24 | 255.255.255.0 |

## Netmask

A netmask, also known as a **subnet mask.**

> Sub netting is done to make a big network into small networks.

- Netmask define the network portion and host portion of an IP address.

In a typical IPv4 address, such as `192.168.1.1`, the netmask might look like `255.255.255.0`. This means that the first three octets (255.255.255) represent the network, while the last octet **(0)** is used for **host** addresses within that network.

prefix length / Netmask :
is a 32-bit number

| Class | CIDR | Subnet Mask |
|---|---|---|
| Class A | /8 | 255.0.0.0 |
| Class B | /16 | 255.255.0.0 |

| Class | CIDR | Subnet Mask |
|---|---|---|
| Class C | /24 | 255.255.255.0 |

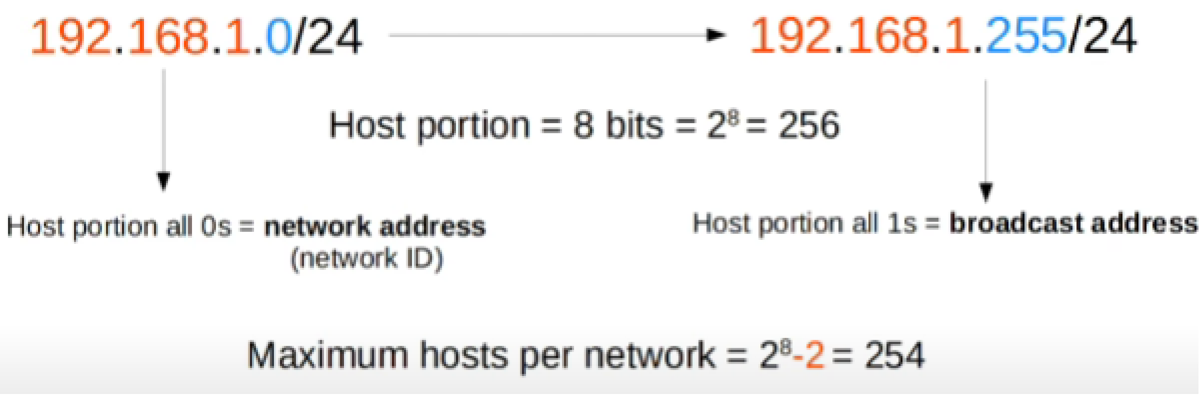
> CIDR (Classless Inter-Domain Routing) is a notation used to specify IP addresses and their associated routing prefix. It represents the number of bits in the subnet mask.

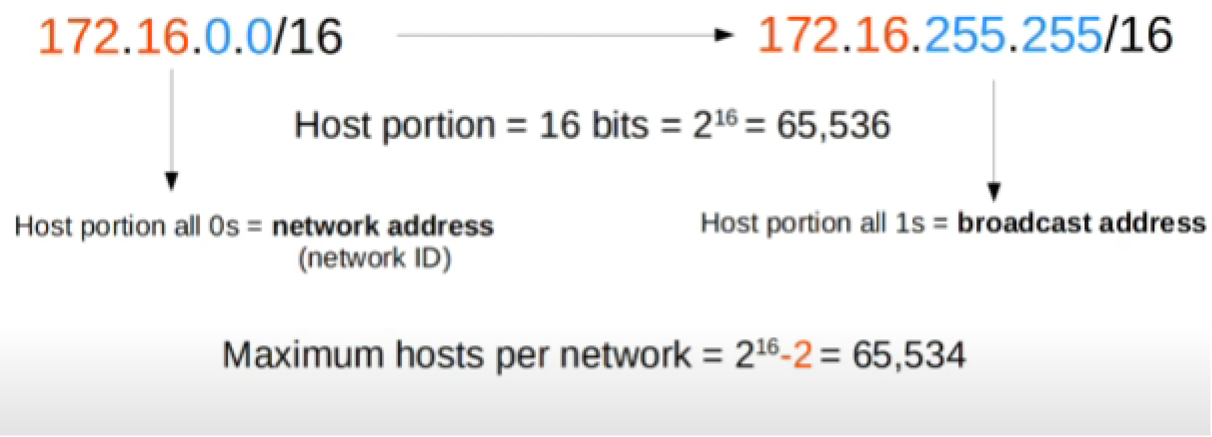
CIDR help to write ip address and sub netmask together in short form.

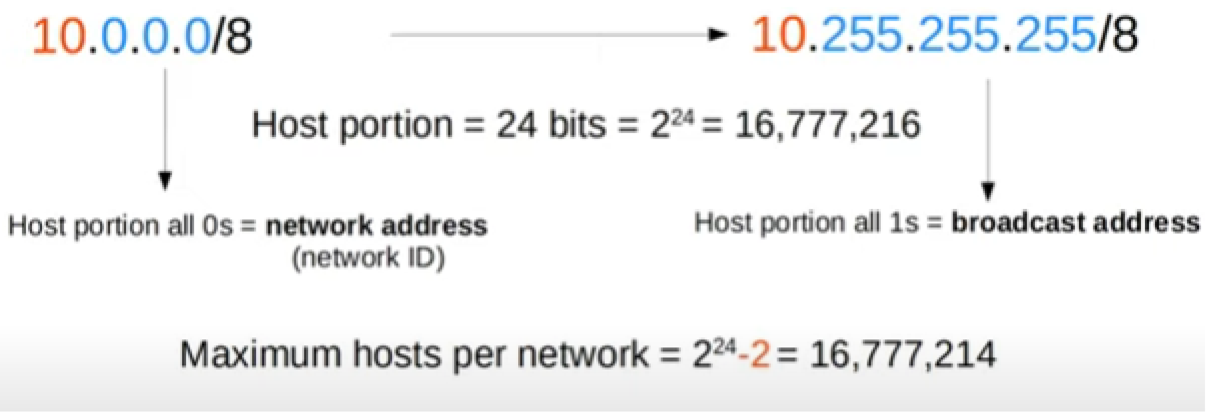
Netmasks can also be expressed in CIDR (Classless Inter-Domain Routing) notation, which indicates the number of bits in the subnet mask. For example, the netmask `255.255.255.0` can be represented as `/24`, meaning the first 24 bits are used for the network address.

## Max hosts per network

- To find max host, as we know is host octet is 1 that mean 8 bite so to get /8 netmask max host 2^8 and subtract 2 from it.
- as we know is host octet is 2 that mean 16 bite so to get /16 netmask max host 2^16 and subtract 2 from it.


192.168.1.0/24
192.168.1.255/24
Host portion = 8 bits = 2⁸ = 256
Host portion all 0s = network address (network ID)
Host portion all 1s = broadcast address
Maximum hosts per network = 2⁸-2 = 254


172.16.0.0/16
172.16.255.255/16
Host portion = 16 bits = 2¹⁶ = 65,536
Host portion all 0s = network address (network ID)
Host portion all 1s = broadcast address
Maximum hosts per network = 2¹⁶-2 = 65,534



10.0.0.0/8 → 10.255.255.255/8

Host portion = 24 bits = $2^{24}$ = 16,777,216

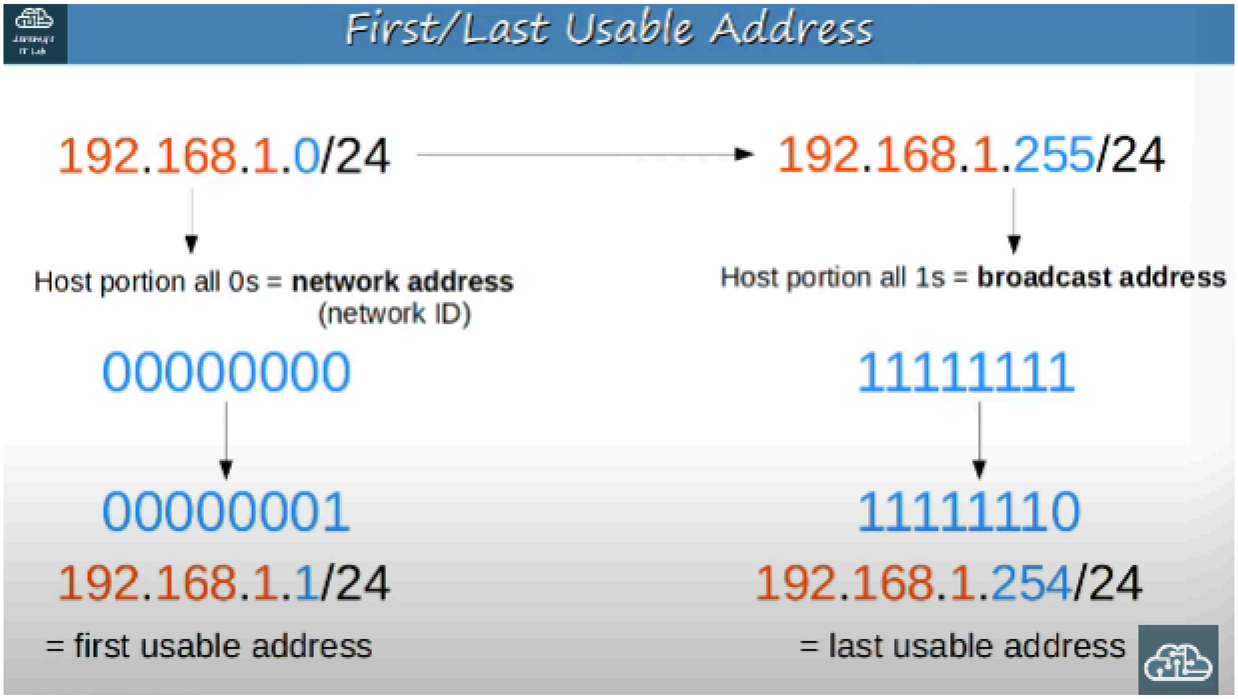
Host portion all 0s = **network address** (network ID)

Host portion all 1s = **broadcast address**

Maximum hosts per network = $2^{24}$-2 = 16,777,214

## First/ Last usable address

ip 192.168.1.1 for router.
ip 192.168.1.254 is used as broadcasting address.



First/Last Usable Address

192.168.1.0/24 → 192.168.1.255/24

Host portion all 0s = **network address** (network ID)

Host portion all 1s = **broadcast address**

00000000 → 00000001

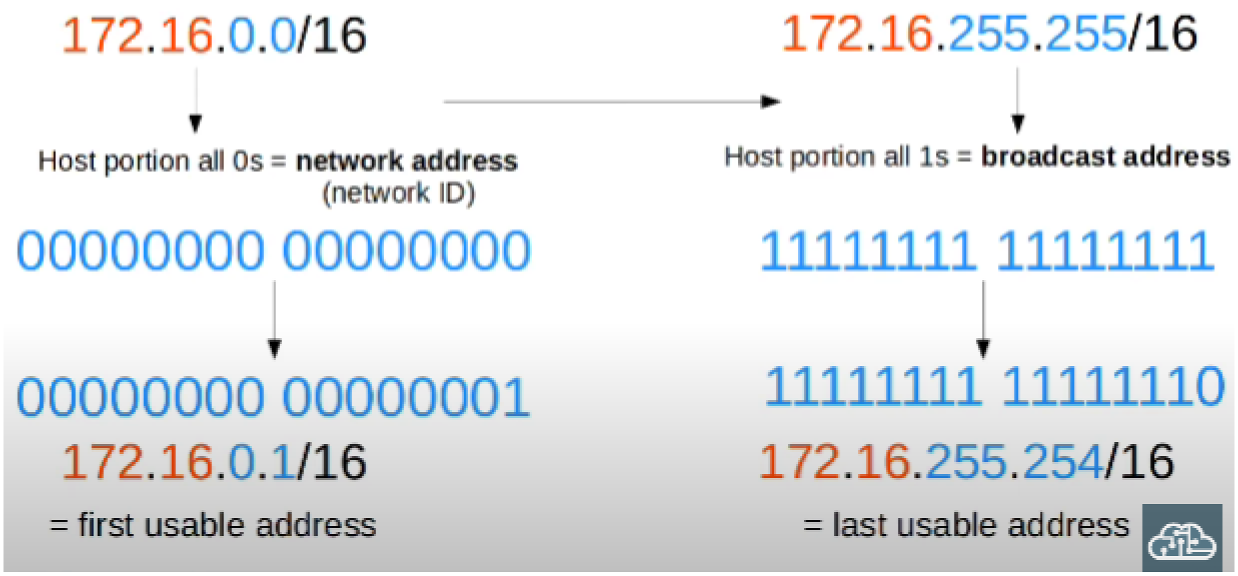
192.168.1.1/24

= first usable address

11111111 → 11111110

192.168.1.254/24

= last usable address



172.16.0.0/16 → 172.16.255.255/16

Host portion all 0s = **network address** (network ID)

Host portion all 1s = **broadcast address**

00000000 00000000 → 00000000 00000001

172.16.0.1/16

= first usable address

11111111 11111111 → 11111111 11111110

172.16.255.254/16

= last usable address

# IPV6

IPv6 have 2^128 ip addresses , sufficient for 50-60 years.

- IPv6 provide Realtime data transmission
- IPv6 **provide Authentication** so anyone can't send a mess on the behalf of someone else.
- **Enable encryption** : In IPv6 if even application layer don't encrypt data IPv6 do it.
- IT is fast than IPv4 as it IPv6 has a more streamlined header compared to IPv4, which reduces the processing time for routers and devices.

IPv6 is need because as increasing in IOT device IPv4 don't have sufficient ip address.

## IPv6 subnetting

> The first 64 bits identify the network and the last 64 bits identify the host.

fc00:1948:0420:0000 : 0000:0000:0000:0001
The Network portion is in blue and the host portion is in red. In IPv6, a /64 is recommended not only for management ease but because stateless auto configuration requires it. If you want a network smaller than a /64 (yes it is technically possible), you better use DHCPv6. However, keeping /64s is the recommended best practice.

## Dynamic vs. Static IP Addresses in IPv6:

Just like in IPv4, IPv6 addresses can be assigned dynamically or statically:

- Dynamic Host Configuration Protocol (DHCP): DHCP servers automatically assign IPv6 addresses to devices on a network. This simplifies address management for a large number of devices.
- Static IP Addresses: These addresses are manually configured and remain constant for specific devices like servers or routers.

# NAT

Network Address Translation (NAT)

- NAT allows multiple devices on a local network to **share a single public IP** address when accessing the internet.
- This conserves the limited number of available IP addresses and enhances security by hiding internal IP addresses.

## Types of NAT

1. **Static NAT**:
    - Maps a single private IP address to a single public IP address.
    - Useful for servers that need a constant IP address for external access (like a web server).
2. **Dynamic NAT**:
    - Maps a private IP address to a public IP address from a pool of public addresses.
    - The mapping is temporary; when the session ends, the public address can be reassigned to another internal device.

> Protect against Ip spoofing attack by verifying source and destination Ip address.

# PAT

Port Address Translation (PAT) is a specific type of Network Address Translation (NAT) that allows multiple devices on a local network to be mapped to a single public IP address, but with a different port number for each session.

- AT translates private IP addresses and their corresponding port numbers into a single public IP address with different port numbers. This allows multiple devices to share the same public IP while maintaining separate sessions.

**Translation Table**: The router maintains a table like this:

| Internal IP | Internal Port | Public IP | Public Port |
|---|---|---|---|
| 192.168.1.2 | 5000 | 203.0.113.5 | 10000 |
| 192.168.1.3 | 5001 | 203.0.113.5 | 10001 |
| 192.168.1.4 | 5002 | 203.0.113.5 | 10002 |

# Automatic Ip assignment (DHCP)

### Explanation

DHCP automates by assigning Ip address to device on the network when a device connects to a network, it sends a Dhcp request , and the Dhcp server dynamically assigns an available Ip address along with over network configuration parameters.

## Apipac (Automate Private Ip addressing)

APIPA is a callback mechanism used when a device cannot obtain an Ip address from DHCP.

It assign a temporary IP address from the reversed APIPA range (169.154.0.1) to 169.254.255.224 to Facaliates local network communication