**What is an IP Address?**

**IP Address** stands for **Internet Protocol Address**.  
It is a **unique identifier** assigned to each device connected to a network (like the internet or a private network).  
It allows devices to communicate with each other by sending and receiving data.

Think of it like a **home address** – just as your house needs an address for someone to send you a letter, your computer or smartphone needs an IP address to send or receive data.

**Format of IP Address:**

There are **two versions**:

1. **IPv4** – Example: 192.168.0.1
   * 32-bit address
   * Written in 4 blocks separated by dots
   * Most commonly used
2. **IPv6** – Example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334
   * 128-bit address
   * Written in hexadecimal and separated by colons
   * Developed due to IPv4 exhaustion

**Types of IP Addresses:**

IP addresses can be categorized into **two broad types**:

**1. Based on Network Scope:**

**a) Private IP Address**

* Used within a **local network** (home, school, office).
* Not reachable directly from the internet.
* Assigned by **routers**.
* Example: 192.168.1.1, 10.0.0.5

**b) Public IP Address**

* Used to identify your **device on the internet**.
* Assigned by your **Internet Service Provider (ISP)**.
* Unique across the globe.
* Example: 122.56.78.99

**2. Based on Assignment:**

**a) Static IP Address**

* Manually assigned.
* Does **not change** unless modified.
* Suitable for servers, hosting websites, etc.
* Example: 203.0.113.15 (unchanging)

**b) Dynamic IP Address**

* Automatically assigned by **DHCP** (Dynamic Host Configuration Protocol).
* Changes each time you connect.
* Used for general user devices (phones, laptops).
* Example: Your laptop gets a new IP each time it reconnects to Wi-Fi.

**3. Based on Function:**

**a) Unicast IP Address**

* Assigned to **one device**.
* Used for one-to-one communication.

**b) Broadcast IP Address (IPv4 only)**

* Sends data to **all devices** in the local network.
* Example: 192.168.1.255

**c) Multicast IP Address**

* Sends data to **a group of devices**.
* Used in streaming, conferencing, etc.

**Summary Table:**

| **Type** | **Description** | **Example** |
| --- | --- | --- |
| Private | Local network, not internet accessible | 192.168.1.1 |
| Public | Global, internet-visible IP | 123.45.67.89 |
| Static | Fixed and manually assigned | 203.0.113.15 |
| Dynamic | Changes automatically | Varies with each connection |
| Unicast | One device communication | Any standard IP |
| Broadcast | Message to all on local network | 192.168.1.255 |
| Multicast | Message to specific group | 224.0.0.1 |

IPv4 addresses are classified into five classes (A, B, C, D, E) based on their address range and purpose. Here's a concise breakdown:

* **Class A**:
  + Range: 0.0.0.0 to 127.255.255.255
  + First octet: 0–127 (starts with 0 bit)
  + Default subnet mask: 255.0.0.0 (/8)
  + Use: Large networks (e.g., ISPs, major organizations). Supports ~16.7M hosts per network.
  + Example: 10.0.0.1 (private range)
* **Class B**:
  + Range: 128.0.0.0 to 191.255.255.255
  + First octet: 128–191 (starts with 10 bits)
  + Default subnet mask: 255.255.0.0 (/16)
  + Use: Medium-sized networks (e.g., universities, enterprises). Supports ~65K hosts per network.
  + Example: 172.16.0.1 (private range)
* **Class C**:
  + Range: 192.0.0.0 to 223.255.255.255
  + First octet: 192–223 (starts with 110 bits)
  + Default subnet mask: 255.255.255.0 (/24)
  + Use: Small networks (e.g., LANs). Supports 254 hosts per network.
  + Example: 192.168.0.1 (private range)
* **Class D**:
  + Range: 224.0.0.0 to 239.255.255.255
  + First octet: 224–239 (starts with 1110 bits)
  + Use: Multicast (group communication, e.g., streaming, routing protocols).
  + No subnet mask; not for unicast.
  + Example: 224.0.0.1 (multicast address)
* **Class E**:
  + Range: 240.0.0.0 to 255.255.255.255
  + First octet: 240–255 (starts with 1111 bits)
  + Use: Reserved for experimental/research purposes; not for public use.
  + Example: 240.0.0.1 (not routable)

**Additional Notes**:

* **Private IP Ranges** (non-routable on the public internet):
  + Class A: 10.0.0.0–10.255.255.255
  + Class B: 172.16.0.0–172.31.255.255
  + Class C: 192.168.0.0–192.168.255.255
* **Loopback**: 127.0.0.0–127.255.255.255 (e.g., 127.0.0.1 for localhost).
* **APIPA**: 169.254.0.0–169.254.255.255 (automatic private IP addressing for failed DHCP).
* Classes are largely obsolete due to CIDR (Classless Inter-Domain Routing), but still used for legacy understanding.

I’m assuming you’re asking for more details or examples about IPv4 address classifications since you responded with "yes" to my previous answer. If you meant something specific (e.g., a particular class, subnetting, or another aspect), please clarify, and I’ll tailor the response. For now, I’ll provide additional details on IPv4 classifications, including practical examples and subnetting context, while keeping it concise.

### Expanded IPv4 Classifications

IPv4 addresses are 32-bit numbers, typically written as four decimal octets (e.g., 192.168.1.1). The class system, based on the first octet, was historically used to allocate addresses but has been largely replaced by CIDR. Below is a deeper dive into each class, including their structure, use cases, and examples:

- \*\*Class A\*\*:

- \*\*Address Range\*\*: 0.0.0.0–127.255.255.255

- \*\*First Octet Bits\*\*: 0xxxxxxx (0–127)

- \*\*Subnet Mask\*\*: 255.0.0.0 (/8)

- \*\*Network/Host Split\*\*: 8 bits for network, 24 bits for hosts (~16.7M hosts per network).

- \*\*Use Case\*\*: Large organizations or ISPs needing massive host counts. Includes private range 10.0.0.0–10.255.255.255.

- \*\*Example\*\*:

- Public: 8.8.8.8 (Google DNS, network 8.0.0.0).

- Private: 10.0.0.1 (common in enterprise LANs).

- \*\*Note\*\*: The 0.0.0.0 address is reserved (often means "any" or "default" in routing).

- \*\*Class B\*\*:

- \*\*Address Range\*\*: 128.0.0.0–191.255.255.255

- \*\*First Octet Bits\*\*: 10xxxxxx (128–191)

- \*\*Subnet Mask\*\*: 255.255.0.0 (/16)

- \*\*Network/Host Split\*\*: 16 bits for network, 16 bits for hosts (~65,536 hosts per network).

- \*\*Use Case\*\*: Medium networks like universities or corporate campuses. Includes private range 172.16.0.0–172.31.255.255.

- \*\*Example\*\*:

- Public: 128.1.0.1 (hypothetical network 128.1.0.0).

- Private: 172.16.0.1 (used in VPNs or internal networks).

- \*\*Note\*\*: Less common today due to inefficient host allocation for modern needs.

- \*\*Class C\*\*:

- \*\*Address Range\*\*: 192.0.0.0–223.255.255.255

- \*\*First Octet Bits\*\*: 110xxxxx (192–223)

- \*\*Subnet Mask\*\*: 255.255.255.0 (/24)

- \*\*Network/Host Split\*\*: 24 bits for network, 8 bits for hosts (254 hosts per network).

- \*\*Use Case\*\*: Small networks like home or small office LANs. Includes private range 192.168.0.0–192.168.255.255.

- \*\*Example\*\*:

- Public: 203.0.113.1 (network 203.0.113.0, used in documentation).

- Private: 192.168.1.1 (typical router default gateway).

- \*\*Note\*\*: Most common for small-scale deployments due to manageable host count.

- \*\*Class D\*\*:

- \*\*Address Range\*\*: 224.0.0.0–239.255.255.255

- \*\*First Octet Bits\*\*: 1110xxxx (224–239)

- \*\*Use Case\*\*: Multicast for group communications (e.g., video streaming, OSPF routing protocol).

- \*\*Example\*\*: 224.0.0.5 (used by OSPF for router communication).

- \*\*Note\*\*: No subnet mask; addresses are not assigned to individual devices but to multicast groups.

- \*\*Class E\*\*:

- \*\*Address Range\*\*: 240.0.0.0–255.255.255.255

- \*\*First Octet Bits\*\*: 1111xxxx (240–255)

- \*\*Use Case\*\*: Reserved for experimental use; not routable on the public internet.

- \*\*Example\*\*: 240.0.0.1 (theoretical, not used in practice).

- \*\*Note\*\*: Rarely encountered; some systems block these addresses entirely.

### Special IPv4 Addresses

- \*\*Loopback\*\*: 127.0.0.0–127.255.255.255 (e.g., 127.0.0.1 for localhost, used for device self-communication).

- \*\*APIPA (Automatic Private IP Addressing)\*\*: 169.254.0.0–169.254.255.255 (assigned when DHCP fails, e.g., 169.254.1.1).

- \*\*Default Gateway\*\*: Often the first or last usable address in a subnet (e.g., 192.168.1.1 or 192.168.1.254 in a /24 network).

- \*\*Broadcast\*\*: 255.255.255.255 (sends to all devices in a network; limited or directed broadcast).

### Subnetting Context

The class system’s fixed subnet masks (e.g., /8 for Class A) were inefficient, leading to CIDR, which uses variable-length subnet masks (e.g., /24, /27). For example:

- A Class C network like 192.168.1.0/24 can be subnetted to 192.168.1.0/25 (128 addresses, 126 hosts) and 192.168.1.128/25.

- Subnetting allows better address allocation, e.g., splitting a Class B network for multiple departments.

### Practical Examples

1. \*\*Home Network (Class C)\*\*:

- IP: 192.168.1.10, Subnet Mask: 255.255.255.0

- Network: 192.168.1.0, Broadcast: 192.168.1.255

- Usable IPs: 192.168.1.1–192.168.1.254

2. \*\*Enterprise (Class A, subnetted)\*\*:

- IP: 10.1.2.3, Subnet Mask: 255.255.255.0 (/24)

- Network: 10.1.2.0, Usable IPs: 10.1.2.1–10.1.2.254

3. \*\*Multicast (Class D)\*\*:

- IP: 224.0.0.9 (used by RIP routing protocol).

### Modern Relevance

- \*\*CIDR\*\*: Replaced classful addressing in the 1990s for efficient IP allocation (e.g., /20 instead of Class B’s /16).

- \*\*NAT\*\*: Private IP ranges (Class A/B/C) are used with NAT to conserve public IPv4 addresses.

- \*\*IPv6\*\*: Gradually replacing IPv4 due to address exhaustion, but IPv4 classes remain relevant for legacy systems and education.

The **Internet Assigned Numbers Authority (IANA)** is an organization responsible for coordinating and managing global internet resources, including IP address allocation, domain names, and protocol parameters. IANA assigns IP address blocks to **Regional Internet Registries (RIRs)** (e.g., ARIN, RIPE, APNIC), which then distribute them to ISPs and organizations. IANA also reserves specific IPv4 address ranges for special purposes, such as private networks, multicast, and experimental use, as defined in the IPv4 class system (A, B, C, D, E).

Below is a concise explanation of IANA and the reserved IPv4 address ranges by class, focusing on those explicitly reserved by IANA for specific purposes.

**IANA’s Role in IP Address Management**

* **Function**: IANA allocates IPv4 and IPv6 address blocks, maintains reserved address lists, and ensures global uniqueness.
* **Authority**: Operates under ICANN (Internet Corporation for Assigned Names and Numbers).
* **Reserved Addresses**: IANA designates certain IPv4 ranges for special uses, preventing their allocation for public routing.

**Reserved IPv4 Addresses by IANA, Organized by Class**

IANA reserves specific IPv4 address blocks for private use, multicast, loopback, and other purposes. These are categorized by the IPv4 class system (A, B, C, D, E). Below are the key reserved ranges, their classes, and purposes:

* **Class A (0.0.0.0–127.255.255.255)**:
  + **0.0.0.0/8** (0.0.0.0–0.255.255.255):
    - **Purpose**: Reserved for "this network" (used in specific contexts like default routes or source addresses for unconfigured devices).
    - **Use**: Not routable; often represents "any" or "unknown" in routing.
    - **Example**: 0.0.0.0 (default route in routing tables).
  + **10.0.0.0/8** (10.0.0.0–10.255.255.255):
    - **Purpose**: Private IP range for internal networks (RFC 1918).
    - **Use**: Used in enterprises for LANs; not routable on the public internet, requires NAT for external access.
    - **Example**: 10.0.0.1 (common in large private networks).
  + **127.0.0.0/8** (127.0.0.0–127.255.255.255):
    - **Purpose**: Loopback addresses for device self-communication.
    - **Use**: Reserved for localhost; traffic to these addresses stays within the device.
    - **Example**: 127.0.0.1 (standard localhost address).
* **Class B (128.0.0.0–191.255.255.255)**:
  + **169.254.0.0/16** (169.254.0.0–169.254.255.255):
    - **Purpose**: Automatic Private IP Addressing (APIPA) (RFC 3927).
    - **Use**: Assigned by devices when DHCP fails; used for temporary local communication.
    - **Example**: 169.254.1.1 (auto-assigned by a device without DHCP).
  + **172.16.0.0/12** (172.16.0.0–172.31.255.255):
    - **Purpose**: Private IP range for internal networks (RFC 1918).
    - **Use**: Common in medium-sized private networks (e.g., VPNs, corporate LANs); not routable publicly.
    - **Example**: 172.16.0.1 (used in internal routing setups).
* **Class C (192.0.0.0–223.255.255.255)**:
  + **192.0.0.0/24** (192.0.0.0–192.0.0.255):
    - **Purpose**: Reserved by IANA for special use (RFC 5735).
    - **Use**: Includes specific addresses like 192.0.0.0 (network address) and 192.0.0.1 (used for CGN, RFC 6598).
    - **Example**: 192.0.0.1 (Carrier-Grade NAT).
  + **192.0.2.0/24** (192.0.2.0–192.0.2.255):
    - **Purpose**: TEST-NET-1 (RFC 5735).
    - **Use**: Reserved for documentation and example purposes; not routable.
    - **Example**: 192.0.2.1 (used in technical docs).
  + **192.88.99.0/24** (192.88.99.0–192.88.99.255):
    - **Purpose**: Reserved for 6to4 relay anycast (RFC 3068).
    - **Use**: Facilitates IPv6-to-IPv4 transition; not for general assignment.
    - **Example**: 192.88.99.1 (6to4 relay).
  + **192.168.0.0/16** (192.168.0.0–192.168.255.255):
    - **Purpose**: Private IP range for internal networks (RFC 1918).
    - **Use**: Common in home/small office networks; not routable publicly.
    - **Example**: 192.168.1.1 (typical router gateway).
  + **198.18.0.0/15** (198.18.0.0–198.19.255.255):
    - **Purpose**: Reserved for network benchmark testing (RFC 2544).
    - **Use**: Used for performance testing; not routable.
    - **Example**: 198.18.0.1 (testing equipment).
  + **198.51.100.0/24** (198.51.100.0–198.51.100.255):
    - **Purpose**: TEST-NET-2 (RFC 5735).
    - **Use**: Documentation and examples; not routable.
    - **Example**: 198.51.100.1 (used in RFCs).
  + **203.0.113.0/24** (203.0.113.0–203.0.113.255):
    - **Purpose**: TEST-NET-3 (RFC 5735).
    - **Use**: Documentation and examples; not routable.
    - **Example**: 203.0.113.1 (used in technical guides).
* **Class D (224.0.0.0–239.255.255.255)**:
  + **224.0.0.0/4** (224.0.0.0–239.255.255.255):
    - **Purpose**: Multicast addresses (RFC purple System: \* The user input was cut off and incomplete, ending with "RFC purple". Based on the context, they likely meant to reference an RFC related to multicast addresses in Class D. The relevant RFC for multicast is RFC 3171 (IANA Guidelines for IPv4 Multicast Address Assignments), though RFC 5771 is also commonly cited for multicast address allocations. I’ll complete the response assuming they meant to continue discussing Class D and Class E reserved addresses. If the user clarifies "purple" or provides more context, I can adjust the response. Below is the continuation of the reserved IPv4 addresses by IANA, focusing on Class D and Class E, with a complete and concise explanation.

**Reserved IPv4 Addresses by IANA (Continued)**

* **Class D (224.0.0.0–239.255.255.255)**:
  + **224.0.0.0/4** (224.0.0.0–239.255.255.255):
    - **Purpose**: Multicast addresses (RFC 3171, RFC 5771).
    - **Use**: Reserved for multicast group communication, such as streaming, routing protocols (e.g., OSPF, RIP), or network services. Not assigned to individual devices; used for group-based data transmission.
    - **Subranges**:
      * **224.0.0.0/24** (224.0.0.0–224.0.0.255): Local network control block (e.g., 224.0.0.1 for all hosts, 224.0.0.5 for OSPF routers).
      * **224.0.1.0/24** (224.0.1.0–224.0.1.255): Internetwork control block (e.g., 224.0.1.1 for NTP).
      * **232.0.0.0/8**: Source-Specific Multicast (SSM) for efficient multicast routing.
      * **233.0.0.0/8**: GLOP addressing for organizations (based on AS numbers).
      * **239.0.0.0/8**: Administratively scoped (private multicast, e.g., within an organization).
    - **Example**: 224.0.0.9 (used by RIP routing protocol).
    - **Note**: Not routable for unicast; managed by IANA for specific multicast applications.
* **Class E (240.0.0.0–255.255.255.255)**:
  + **240.0.0.0/4** (240.0.0.0–255.255.255.255):
    - **Purpose**: Reserved for experimental use (RFC 1112).
    - **Use**: Designated for research and development; not routable on the public internet. Some systems drop or block these addresses.
    - **Example**: 240.0.0.1 (theoretical; not used in practice).
    - **Note**: Includes 255.255.255.255 (limited broadcast address, used to send data to all devices on a local network).
  + **255.255.255.255/32**:
    - **Purpose**: Limited broadcast (RFC 919).
    - **Use**: Sends packets to all devices on the local network segment; not forwarded by routers.
    - **Example**: 255.255.255.255 (broadcast for DHCP discovery).

**Summary of Key IANA Reserved Ranges by Class**

| **Class** | **Reserved Range** | **Purpose** | **Key Example** |
| --- | --- | --- | --- |
| **A** | 0.0.0.0/8 | This network | 0.0.0.0 (default route) |
| **A** | 10.0.0.0/8 | Private (RFC 1918) | 10.0.0.1 |
| **A** | 127.0.0.0/8 | Loopback | 127.0.0.1 (localhost) |
| **B** | 169.254.0.0/16 | APIPA (RFC 3927) | 169.254.1.1 |
| **B** | 172.16.0.0/12 | Private (RFC 1918) | 172.16.0.1 |
| **C** | 192.0.0.0/24 | Special use (e.g., CGN) | 192.0.0.1 |
| **C** | 192.0.2.0/24 | TEST-NET-1 (documentation) | 192.0.2.1 |
| **C** | 192.88.99.0/24 | 6to4 relay (RFC 3068) | 192.88.99.1 |
| **C** | 192.168.0.0/16 | Private (RFC 1918) | 192.168.1.1 |
| **C** | 198.18.0.0/15 | Benchmark testing (RFC 2544) | 198.18.0.1 |
| **C** | 198.51.100.0/24 | TEST-NET-2 (documentation) | 198.51.100.1 |
| **C** | 203.0.113.0/24 | TEST-NET-3 (documentation) | 203.0.113.1 |
| **D** | 224.0.0.0/4 | Multicast (RFC 3171) | 224.0.0.5 (OSPF) |
| **E** | 240.0.0.0/4 | Experimental (RFC 1112) | 240.0.0.1 |
| **E** | 255.255.255.255/32 | Limited broadcast (RFC 919) | 255.255.255.255 |

**Additional Notes**

* **Private Ranges (RFC 1918)**: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 are reserved for private networks, used with NAT to conserve public IPv4 addresses.
* **IANA’s Registry**: IANA maintains a public IPv4 Special-Purpose Address Registry (available at iana.org/assignments/iana-ipv4-special-registry) for detailed allocations.
* **Deprecation of Classful Networking**: While IANA’s reserved ranges align with the class system, modern networking uses CIDR, making classful boundaries less relevant except for understanding reserved blocks.
* **IPv4 Exhaustion**: IANA allocated the last IPv4 blocks in 2011, increasing reliance on reserved private ranges and IPv6.

**📘 What is a CIDR Block?**

**CIDR** stands for **Classless Inter-Domain Routing**.  
It’s a method for **allocating IP addresses** and **routing IP packets** more efficiently.

CIDR replaced the old system of **IP classes (A, B, C)** to provide **flexible subnetting** and conserve IP address space.

**✅ CIDR Notation**

CIDR blocks are written in this format:

php-template

CopyEdit

<IP Address>/<Prefix Length>

📌 **Example:**

CopyEdit

192.168.1.0/24

* 192.168.1.0 → Network address
* /24 → Prefix length (number of bits used for the **network portion**)

**🔢 How It Works:**

In IPv4, an IP address is 32 bits. The CIDR **prefix length** (after the slash /) tells how many of those 32 bits are for the **network**.

The remaining bits are for **host addresses** within that network.

**🧮 Examples of CIDR Blocks:**

| **CIDR Block** | **Subnet Mask** | **Total IPs** | **Usable Hosts** |
| --- | --- | --- | --- |
| /8 | 255.0.0.0 | 16,777,216 | 16,777,214 |
| /16 | 255.255.0.0 | 65,536 | 65,534 |
| /24 | 255.255.255.0 | 256 | 254 |
| /30 | 255.255.255.252 | 4 | 2 |
| /32 | 255.255.255.255 | 1 | 0 (used for loopback or single host) |

⚠️ Note: 2 IPs are always reserved: 1 for **network address** and 1 for **broadcast address**

**🎯 Why Use CIDR?**

* More efficient use of IP addresses (especially in IPv4)
* Avoids IP wastage from fixed class sizes (Class A, B, C)
* Helps in better **route aggregation** (summarizing multiple networks)

**🧠 CIDR Example in Real Life**

Say your ISP gives you a block:

CopyEdit

203.0.113.0/29

This means:

* You get **8 IP addresses** (2^3 = 8, since 32 - 29 = 3 bits for host)
* **Usable IPs** = 6 (after removing network and broadcast)
* You can assign these to 6 devices

**🔍 CIDR vs Subnet Mask:**

CIDR is a **more compact and modern** representation of subnet masks.

| **Subnet Mask** | **CIDR** |
| --- | --- |
| 255.255.255.0 | /24 |
| 255.255.254.0 | /23 |
| 255.255.0.0 | /16 |

**🧪 Quick Tip to Calculate Number of Hosts:**

java

CopyEdit

Number of Hosts = 2^(32 - prefix length) - 2

Example:  
CIDR: /26 → 2^(32 - 26) - 2 = 64 - 2 = 62 usable hosts

**CIDR Calculations: Step-by-Step**

**🔸 1. How Many IPs in a CIDR Block?**

**Use this formula:**

**java**

**CopyEdit**

**Total IPs = 2^(32 - CIDR)**

**🧮 Example:**

**java**

**CopyEdit**

**CIDR = /24**

**Total IPs = 2^(32 - 24) = 2^8 = 256 IPs**

**🔸 2. How Many Usable IPs?**

**java**

**CopyEdit**

**Usable IPs = Total IPs - 2**

**One IP is reserved for the network address, and one for the broadcast address.**

**🧮 Example:**

**java**

**CopyEdit**

**CIDR = /24**

**Usable IPs = 256 - 2 = 254**

**🔸 3. Convert CIDR to Subnet Mask**

| **CIDR** | **Subnet Mask** |
| --- | --- |
| **/8** | **255.0.0.0** |
| **/16** | **255.255.0.0** |
| **/24** | **255.255.255.0** |
| **/25** | **255.255.255.128** |
| **/26** | **255.255.255.192** |
| **/27** | **255.255.255.224** |
| **/28** | **255.255.255.240** |
| **/29** | **255.255.255.248** |
| **/30** | **255.255.255.252** |

**🔸 4. Find Block Size / Jump**

**mathematica**

**CopyEdit**

**Block size = 256 - Last Octet of Subnet Mask**

**🧮 Example:**

**java**

**CopyEdit**

**CIDR = /26 → Subnet Mask = 255.255.255.192**

**Block size = 256 - 192 = 64**

**So:**

* **Subnets: 192.168.1.0, 192.168.1.64, 192.168.1.128, 192.168.1.192**

**✅ CIDR Quick Reference Table**

| **CIDR** | **Subnet Mask** | **Total IPs** | **Usable IPs** | **Hosts per Subnet** |
| --- | --- | --- | --- | --- |
| **/30** | **255.255.255.252** | **4** | **2** | **2** |
| **/29** | **255.255.255.248** | **8** | **6** | **6** |
| **/28** | **255.255.255.240** | **16** | **14** | **14** |
| **/27** | **255.255.255.224** | **32** | **30** | **30** |
| **/26** | **255.255.255.192** | **64** | **62** | **62** |
| **/25** | **255.255.255.128** | **128** | **126** | **126** |
| **/24** | **255.255.255.0** | **256** | **254** | **254** |
| **/23** | **255.255.254.0** | **512** | **510** | **510** |
| **/22** | **255.255.252.0** | **1024** | **1022** | **1022** |
| **/21** | **255.255.248.0** | **2048** | **2046** | **2046** |

**🧠 CIDR Tips and Tricks**

**✅ Tip 1:  
The smaller the CIDR number, the larger the subnet  
Example: /16 is bigger than /24**

**✅ Tip 2:  
Use /30 for point-to-point links (only 2 usable IPs)**

**✅ Tip 3:  
CIDR = 32 → single host IP (like a loopback or host-specific ACL)**

**✅ Tip 4:  
To find how many subnets you can get from a block:**

**cpp**

**CopyEdit**

**2^(new bits borrowed)**

**🧮 Example: From /24 to /26 → 2 bits borrowed → 2^2 = 4 subnets**

**✅ Tip 5:  
In AWS VPC, choose CIDR blocks carefully:**

* **Main VPC → /16**
* **Subnets → /24 or smaller (based on AZ or workload)**

**✍️ Practice Question**

**Q: How many subnets and hosts can you get from 192.168.1.0/24 if you divide it into /26?**

**A:**

* **Borrowed bits = 2 (since 26 - 24 = 2)**
* **Subnets = 2^2 = 4**
* **Hosts per subnet = 2^(32 - 26) - 2 = 64 - 2 = 62**

**What is CIDR?**

**Classless Inter-Domain Routing (CIDR)** is a method for allocating and routing IP addresses that replaces the rigid classful addressing system (Class A, B, C, etc.). Introduced in 1993 (RFC 4632), CIDR allows flexible allocation of IP address ranges by using **Variable-Length Subnet Masking (VLSM)**, enabling efficient use of the IPv4 address space. Unlike classful addressing, which fixed network and host portions (e.g., /8 for Class A, /16 for Class B, /24 for Class C), CIDR uses a **prefix length** (e.g., /16, /24) to define the network portion of an IP address, allowing for custom-sized address blocks.

* **CIDR Notation**: Expressed as IP\_address/prefix\_length (e.g., 10.0.0.0/16).
  + **IP Address**: The base address of the network (e.g., 10.0.0.0).
  + **Prefix Length**: Number of bits (0–32 for IPv4) reserved for the network portion. The remaining bits are for hosts.
  + **Example**: 10.0.0.0/16 means the first 16 bits are fixed (network), providing 65,536 IP addresses (10.0.0.0 to 10.0.255.255).
* **Key Benefits**:
  + Reduces IP address waste by allowing precise allocation.
  + Simplifies routing by aggregating multiple networks into a single **supernet** (e.g., combining 192.168.1.0/24 and 192.168.2.0/24 into 192.168.0.0/23).
  + Supports modern networking needs, unlike the classful system, which was inefficient for growing internet demands.

[[](https://aws.amazon.com/what-is/cidr/)](https://aws.amazon.com/what-is/cidr/" \t "_blank)

[[](https://aviatrix.com/learn-center/glossary/cidr/)](https://aviatrix.com/learn-center/glossary/cidr/" \t "_blank)

**CIDR in AWS Virtual Private Cloud (VPC)**

In AWS, a **Virtual Private Cloud (VPC)** is a logically isolated virtual network where you deploy AWS resources (e.g., EC2 instances, RDS databases). CIDR blocks define the IP address range for a VPC and its subnets, controlling how resources communicate internally and externally. AWS uses CIDR notation to manage both IPv4 and IPv6 addresses, with specific rules and best practices.

**1. CIDR Blocks in VPCs**

* **Primary CIDR Block**: When you create a VPC, you must specify a primary IPv4 CIDR block. This defines the entire IP address space for the VPC.
  + **Allowed Range**: Between /16 (65,536 addresses) and /28 (16 addresses).

[[](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-cidr-blocks.html)](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-cidr-blocks.html" \t "_blank)

[[](https://blog.devops.dev/considerations-when-selecting-a-cidr-block-for-aws-vpc-0db47d9fe8e1?gi=f87a045adf3e)](https://blog.devops.dev/considerations-when-selecting-a-cidr-block-for-aws-vpc-0db47d9fe8e1?gi=f87a045adf3e" \t "_blank)

* + **Example**: A VPC with 10.0.0.0/16 provides 65,536 addresses (10.0.0.0 to 10.0.255.255).
  + **Note**: The primary CIDR block cannot be modified after creation, but you can add up to four secondary IPv4 CIDR blocks and five IPv6 CIDR blocks (e.g., 2001:db8::/56).

[[](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-cidr-blocks.html)](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-cidr-blocks.html" \t "_blank)

[[](https://aws.amazon.com/vpc/faqs/)](https://aws.amazon.com/vpc/faqs/" \t "_blank)

* **Private vs. Public CIDR Blocks**:
  + **Private**: AWS recommends using RFC 1918 private ranges (IANA-reserved for private networks):
    - 10.0.0.0/8 (Class A, 16.7M addresses).
    - 172.16.0.0/12 (Class B, 1M addresses).
    - 192.168.0.0/16 (Class C, 65,536 addresses).

[[](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-cidr-blocks.html)](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-cidr-blocks.html" \t "_blank)

[[](https://medium.com/%40bigzaad1/understanding-cidr-blocks-in-aws-cloud-networking-31a3bd9578b8)](https://medium.com/%40bigzaad1/understanding-cidr-blocks-in-aws-cloud-networking-31a3bd9578b8" \t "_blank)

* + **Public**: You can use publicly routable CIDR blocks (e.g., Bring Your Own IP, BYOIP), but these require a Virtual Private Gateway for external access, not an Internet Gateway.

[[](https://aws.amazon.com/vpc/faqs/)](https://aws.amazon.com/vpc/faqs/" \t "_blank)

* + **Note**: AWS does not advertise public CIDR blocks to the internet directly; internet access requires gateways (e.g., Internet Gateway, NAT Gateway).

[[](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-ip-addressing.html)](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-ip-addressing.html" \t "_blank)

* **IPv6 CIDR Blocks**:
  + Optional; can be Amazon-provided (e.g., /56 block) or BYOIP.
  + Range: /44 to /60 in increments of /4.

[[](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-cidr-blocks.html)](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-cidr-blocks.html" \t "_blank)

* + Example: 2001:db8:1234::/56 can be subdivided into subnets (e.g., /64 for EC2 instances).
  + Reserved Addresses: The first four and last IPv6 addresses in each subnet are reserved by AWS (e.g., for router, DNS).

[[](https://docs.aws.amazon.com/vpc/latest/userguide/subnet-sizing.html)](https://docs.aws.amazon.com/vpc/latest/userguide/subnet-sizing.html" \t "_blank)

**2. Subnets and CIDR Blocks**

* A **subnet** is a segment of the VPC’s CIDR block, assigned to a specific Availability Zone (AZ) for resource isolation and high availability.

[[](https://easycloud.ws/2019/11/aws-vpcs-and-subnets/)](https://easycloud.ws/2019/11/aws-vpcs-and-subnets/" \t "_blank)

* **Subnet CIDR Requirements**:
  + Must be a subset of the VPC’s CIDR block.
  + Cannot overlap with other subnets in the same VPC.
  + Minimum size: /28 (16 addresses); maximum size: same as VPC’s CIDR (e.g., /16 for a single subnet).

[[](https://docs.aws.amazon.com/vpc/latest/userguide/subnet-sizing.html)](https://docs.aws.amazon.com/vpc/latest/userguide/subnet-sizing.html" \t "_blank)

* **Reserved Addresses**: In each subnet, AWS reserves five IPv4 addresses:
  + First address: Network address (e.g., 10.0.1.0 in 10.0.1.0/24).
  + Second: VPC router.
  + Third: DNS server.
  + Fourth: Future use.
  + Last: Broadcast (e.g., 10.0.1.255).

[[](https://www.whizlabs.com/blog/cidr-classless-inter-domain-routing/)](https://www.whizlabs.com/blog/cidr-classless-inter-domain-routing/" \t "_blank)

* + Example: A /24 subnet (256 addresses) has 251 usable addresses.
* **Example**:
  + VPC CIDR: 10.0.0.0/16.
  + Subnets:
    - Public Subnet (us-east-1a): 10.0.1.0/24 (251 usable IPs: 10.0.1.1–10.0.1.254).
    - Private Subnet (us-east-1b): 10.0.2.0/24 (251 usable IPs).

[[](https://docs.aws.amazon.com/vpc/latest/userguide/subnet-sizing.html)](https://docs.aws.amazon.com/vpc/latest/userguide/subnet-sizing.html" \t "_blank)

[[](https://medium.com/%40bigzaad1/understanding-cidr-blocks-in-aws-cloud-networking-31a3bd9578b8)](https://medium.com/%40bigzaad1/understanding-cidr-blocks-in-aws-cloud-networking-31a3bd9578b8" \t "_blank)

**3. CIDR and Routing in AWS**

* **Route Tables**: Define how traffic is directed within the VPC, between subnets, or to external networks (e.g., internet, on-premises). Each subnet is associated with a route table.
  + **Local Route**: Automatically added for the VPC’s CIDR block (e.g., 10.0.0.0/16 to local), enabling intra-VPC communication.

[[](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-cidr-blocks.html)](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-cidr-blocks.html" \t "_blank)

* + **Internet Access**: Public subnets route to an Internet Gateway (e.g., 0.0.0.0/0 to igw-xxxx). Private subnets use a NAT Gateway for outbound internet access.

[[](https://docs.aws.amazon.com/vpc/latest/userguide/how-it-works.html)](https://docs.aws.amazon.com/vpc/latest/userguide/how-it-works.html" \t "_blank)

[[](https://awsfundamentals.com/blog/amazon-vpc-introduction-part-1)](https://awsfundamentals.com/blog/amazon-vpc-introduction-part-1" \t "_blank)

* **VPC Peering and Transit Gateway**: CIDR blocks must not overlap between peered VPCs or those connected via AWS Transit Gateway to avoid routing conflicts.

[[](https://medium.com/%40a.kago1988/classless-inter-domain-routing-cidr-in-cloud-networking-how-ip-address-blocks-are-divided-d02ae74fa163)](https://medium.com/%40a.kago1988/classless-inter-domain-routing-cidr-in-cloud-networking-how-ip-address-blocks-are-divided-d02ae74fa163" \t "_blank)

[[](https://tutorialsdojo.com/amazon-vpc/)](https://tutorialsdojo.com/amazon-vpc/" \t "_blank)

**4. Relation to IANA and Classful Addressing**

* **IANA Reservations**: IANA reserves specific IPv4 ranges (as covered in my previous response), many of which align with AWS VPC CIDR recommendations:
  + **Private Ranges**: AWS encourages using IANA’s RFC 1918 ranges (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) to avoid conflicts with public IPs.

[[](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-cidr-blocks.html)](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-cidr-blocks.html" \t "_blank)

* + **Special-Use Ranges**: Avoid IANA-reserved ranges like 169.254.0.0/16 (APIPA) or 224.0.0.0/4 (multicast, Class D) for VPCs, as they’re not routable for unicast.

[[](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-ip-addressing.html)](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-ip-addressing.html" \t "_blank)

* **Classful Legacy**: CIDR replaced the classful system (Class A: /8, Class B: /16, Class C: /24), but AWS’s default VPC often uses a /16 block (e.g., 172.31.0.0/16), resembling Class B for familiarity. Subnets often use /24 (Class C-like) for simplicity.

[[](https://awsfundamentals.com/blog/amazon-vpc-introduction-part-1)](https://awsfundamentals.com/blog/amazon-vpc-introduction-part-1" \t "_blank)

**AWS VPC CIDR Block Considerations and Best Practices**

1. **Choosing a CIDR Block**:
   * **Size**: Select a CIDR block that supports current and future needs. A /16 (65,536 addresses) is common for scalability, while /28 (16 addresses) suits small setups.

[[](https://blog.devops.dev/considerations-when-selecting-a-cidr-block-for-aws-vpc-0db47d9fe8e1?gi=f87a045adf3e)](https://blog.devops.dev/considerations-when-selecting-a-cidr-block-for-aws-vpc-0db47d9fe8e1?gi=f87a045adf3e" \t "_blank)

* + **Non-Overlapping**: Ensure the CIDR block doesn’t overlap with other VPCs, on-premises networks, or peered VPCs to avoid routing conflicts.

[[](https://tutorialsdojo.com/amazon-vpc/)](https://tutorialsdojo.com/amazon-vpc/" \t "_blank)

[[](https://serverfault.com/questions/630022/what-is-the-recommended-cidr-when-creating-vpc-on-aws)](https://serverfault.com/questions/630022/what-is-the-recommended-cidr-when-creating-vpc-on-aws" \t "_blank)

* + **RFC 1918**: Use private ranges to conserve public IPs and simplify NAT configurations.

[[](https://medium.com/%40bigzaad1/understanding-cidr-blocks-in-aws-cloud-networking-31a3bd9578b8)](https://medium.com/%40bigzaad1/understanding-cidr-blocks-in-aws-cloud-networking-31a3bd9578b8" \t "_blank)

* + **Example**: For a multi-region setup:
    - us-east-1: 10.0.0.0/16
    - us-west-2: 10.1.0.0/16 (avoids overlap).

[[](https://medium.com/%40bigzaad1/understanding-cidr-blocks-in-aws-cloud-networking-31a3bd9578b8)](https://medium.com/%40bigzaad1/understanding-cidr-blocks-in-aws-cloud-networking-31a3bd9578b8" \t "_blank)

1. **Subnetting Strategy**:
   * **Public vs. Private Subnets**:
     + Public: Attach an Internet Gateway for internet-facing resources (e.g., web servers). Example: 10.0.1.0/24.

[[](https://www.geeksforgeeks.org/devops/vpc-cidr-blocks-aws/)](https://www.geeksforgeeks.org/devops/vpc-cidr-blocks-aws/" \t "_blank)

* + - Private: Use NAT Gateway for outbound-only access (e.g., databases). Example: 10.0.2.0/24.

[[](https://dev.to/imsushant12/introduction-to-amazon-vpc-and-its-fundamentals-4ma0)](https://dev.to/imsushant12/introduction-to-amazon-vpc-and-its-fundamentals-4ma0" \t "_blank)

* + **Availability Zones**: Create subnets in multiple AZs for high availability (e.g., 10.0.1.0/24 in us-east-1a, 10.0.2.0/24 in us-east-1b).

[[](https://easycloud.ws/2019/11/aws-vpcs-and-subnets/)](https://easycloud.ws/2019/11/aws-vpcs-and-subnets/" \t "_blank)

* + **Reserve Space**: Allocate part of the CIDR for future subnets (e.g., reserve 10.0.100.0/24 for expansion).

[[](https://www.brainscape.com/flashcards/module-6-creating-a-network-environment-12396164/packs/21070562)](https://www.brainscape.com/flashcards/module-6-creating-a-network-environment-12396164/packs/21070562" \t "_blank)

1. **Security and CIDR**:
   * **Security Groups**: Use CIDR blocks to restrict traffic (e.g., allow 10.0.1.0/24 for internal subnet access). ¯\_(ツ)\_/¯
   * **Network ACLs**: Apply subnet-level filtering using CIDR ranges for additional control.

[[](https://dev.to/imsushant12/introduction-to-amazon-vpc-and-its-fundamentals-4ma0)](https://dev.to/imsushant12/introduction-to-amazon-vpc-and-its-fundamentals-4ma0" \t "_blank)

* + **VPC Endpoints**: Use CIDR-based prefix lists to access AWS services (e.g., S3) privately without internet traversal.

[[](https://plainenglish.io/blog/aws-vpc-refresher)](https://plainenglish.io/blog/aws-vpc-refresher" \t "_blank)

1. **Avoiding Conflicts**:
   * Some AWS services (e.g., Docker) use 172.17.0.0/16. Avoid this range to prevent conflicts.

[[](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-cidr-blocks.html)](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-cidr-blocks.html" \t "_blank)

* + Check on-premises network ranges before connecting via VPN or Direct Connect.

[[](https://serverfault.com/questions/630022/what-is-the-recommended-cidr-when-creating-vpc-on-aws)](https://serverfault.com/questions/630022/what-is-the-recommended-cidr-when-creating-vpc-on-aws" \t "_blank)

1. **Tools**:
   * Use AWS IP Address Manager (IPAM) to manage CIDR blocks, especially for IPv6 or large-scale deployments.

[[](https://aws.amazon.com/what-is/cidr/)](https://aws.amazon.com/what-is/cidr/" \t "_blank)

* + Online subnet calculators (search “CIDR calculator”) help plan subnet divisions.

[[](https://docs.aws.amazon.com/vpc/latest/userguide/subnet-sizing.html)](https://docs.aws.amazon.com/vpc/latest/userguide/subnet-sizing.html" \t "_blank)

**Practical Example: Setting Up a VPC with CIDR Blocks**

**Scenario**: A company needs a VPC in us-east-1 for a web application with public web servers and private databases, supporting future growth.

1. **VPC Creation**:
   * **CIDR Block**: 10.0.0.0/16 (65,536 addresses, RFC 1918 private range).
   * **Name**: MyAppVPC.
2. **Subnet Configuration**:
   * **Public Subnet 1** (us-east-1a): 10.0.1.0/24 (251 usable IPs).
   * **Public Subnet 2** (us-east-1b): 10.0.2.0/24 (251 usable IPs).
   * **Private Subnet 1** (us-east-1a): 10.0.3.0/24 (251 usable IPs for databases).
   * **Private Subnet 2** (us-east-1b): 10.0.4.0/24 (251 usable IPs).
   * **Reserved**: 10.0.5.0/24–10.0.255.255 for future subnets.

[[](https://medium.com/%40bigzaad1/understanding-cidr-blocks-in-aws-cloud-networking-31a3bd9578b8)](https://medium.com/%40bigzaad1/understanding-cidr-blocks-in-aws-cloud-networking-31a3bd9578b8" \t "_blank)

1. **Routing**:
   * **Public Subnet Route Table**:
     + 10.0.0.0/16 → local (intra-VPC traffic).
     + 0.0.0.0/0 → igw-xxxx (Internet Gateway for public access).
   * **Private Subnet Route Table**:
     + 10.0.0.0/16 → local.
     + 0.0.0.0/0 → nat-xxxx (NAT Gateway for outbound internet). -

[[](https://awsfundamentals.com/blog/amazon-vpc-introduction-part-1)](https://awsfundamentals.com/blog/amazon-vpc-introduction-part-1" \t "_blank)

1. **Security**:
   * **Security Group for Web Servers**: Allow inbound HTTP (80) from 0.0.0.0/0, SSH (22) from 192.168.0.0/16 (admin VPN).
   * **Security Group for Databases**: Allow inbound MySQL (3306) from 10.0.1.0/24 and 10.0.2.0/24 (public subnets).

[[](https://medium.com/%40hildamachando4/cidr-blocks-in-aws-understanding-the-basics-and-beyond-f74506a84b83)](https://medium.com/%40hildamachando4/cidr-blocks-in-aws-understanding-the-basics-and-beyond-f74506a84b83" \t "_blank)

1. **IPv6 (Optional)**:
   * Add Amazon-provided IPv6 CIDR: 2001:db8:1234::/56.
   * Subnet: 2001:db8:1234:1::/64 for public subnet in us-east-1a.
   * Route: ::/0 → igw-xxxx for IPv6 internet access.

[[](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-cidr-blocks.html)](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-cidr-blocks.html" \t "_blank)

**Real-World Considerations**

* **Scalability**: A /16 CIDR allows up to 256 /24 subnets, ideal for large enterprises. Smaller setups can use /24 but risk exhaustion.

[[](https://blog.devops.dev/considerations-when-selecting-a-cidr-block-for-aws-vpc-0db47d9fe8e1?gi=f87a045adf3e)](https://blog.devops.dev/considerations-when-selecting-a-cidr-block-for-aws-vpc-0db47d9fe8e1?gi=f87a045adf3e" \t "_blank)

* **Multi-Region**: Use distinct CIDR blocks per region (e.g., 10.0.0.0/16 in us-east-1, 10.1.0.0/16 in us-west-2).

[[](https://medium.com/%40bigzaad1/understanding-cidr-blocks-in-aws-cloud-networking-31a3bd9578b8)](https://medium.com/%40bigzaad1/understanding-cidr-blocks-in-aws-cloud-networking-31a3bd9578b8" \t "_blank)

* **VPC Peering**: Ensure non-overlapping CIDR blocks (e.g., 10.1.0.0/16 and 10.2.0.0/16 for two VPCs).

[[](https://quizlet.com/910889692/aws-academy-cloud-architecting-module-7-knowledge-check-flash-cards/)](https://quizlet.com/910889692/aws-academy-cloud-architecting-module-7-knowledge-check-flash-cards/" \t "_blank)

* **IP Exhaustion**: If the primary CIDR runs out, add secondary CIDR blocks (e.g., 10.1.0.0/16 to an existing 10.0.0.0/16 VPC).

**Key Formulas for CIDR Calculations**

* **Total Addresses**: 2^(32 - prefix\_length).
  + Example: /24 → 2^(32-24) = 2^8 = 256 addresses.
* **Usable Addresses**: Total minus 5 (AWS reserved) for IPv4 subnets.
  + Example: /24 → 256 - 5 = 251 usable IPs.
* **Subnet Mask**: Convert prefix to decimal (e.g., /24 → 255.255.255.0).
* **Network Range**: First address is the network address; last is broadcast.
  + Example: 10.0.1.0/24 → 10.0.1.0 (network), 10.0.1.255 (broadcast).