

IP Addressing and Subnetting including IPv4 & IPv6

Assignment 2.1 for Celebal Technologies Internship

June 15, 2025

1. Introduction

Imagine your home address - it tells the postal service exactly where to deliver your mail. Similarly, every device connected to the internet needs a unique "address" called an IP address. Just like how your neighborhood might be divided into different streets and house numbers, computer networks use something called "subnetting" to organize and manage groups of devices efficiently.

This document will take you on a journey through the world of IP addressing and subnetting, explaining complex networking concepts in simple, understandable terms. Whether you're a student learning networking basics, an IT professional expanding your knowledge, or someone curious about how the internet works, this guide will help you understand how billions of devices communicate across the globe.

We'll explore two main versions of IP addresses: IPv4 (the older system that's still widely used) and IPv6 (the newer system with virtually unlimited addresses). Think of IPv4 as a city that's running out of house numbers, while IPv6 is like building a massive new city with enough addresses for everyone and everything that might ever need to connect to the internet.

By the end of this document, you'll understand how to create network subnets, calculate how many devices can fit in each subnet, and why this knowledge is crucial for building efficient, secure, and well-organized networks.

2. What is an IP Address? - The Digital World's Postal System

2.1. Understanding IP Addresses Through Everyday Examples

Let's start with a simple analogy. When you want to send a letter to a friend, you need their complete address: house number, street name, city, and zip code. Without this information, the postal service wouldn't know where to deliver your letter. The internet works the same way, but instead of physical addresses, we use IP addresses.

An IP address is like a digital home address for every device connected to the internet - your smartphone, laptop, smart TV, even your refrigerator if it's connected to WiFi! Every time you send a message, stream a video, or browse a website, your device uses IP addresses to find the right destination across the vast network of the internet.

Real-World Example: When you type "www.google.com" in your browser, your computer doesn't actually understand "google.com." Behind the scenes, it translates this friendly name into Google's IP address (something like 142.250.190.14) and then sends your request to that specific address. It's like having a phone book that converts names into phone numbers!

2.2. Why Do We Need So Many IP Addresses?

Consider this: there are over 5 billion internet users worldwide, each with multiple devices. Your family alone might have smartphones, tablets, laptops, smart TVs, gaming consoles, and IoT devices all connected to the internet. Each device needs its own unique IP address to communicate properly.

This massive need for addresses led to the development of two IP address systems: IPv4 and IPv6. Think of IPv4 as the original addressing system that worked great when the internet was smaller, and IPv6 as the expanded system designed to handle our modern, connected world.

3. IPv4 Addressing - The Foundation of the Internet

3.1. Breaking Down IPv4 Addresses

IPv4 addresses might look intimidating at first glance, but they're actually quite logical once you understand the pattern. Let's break down a typical IPv4 address: 192.168.1.100.

The Four-Part Structure: Each IPv4 address consists of four numbers separated by dots (periods). Each number can range from 0 to 255, giving us the format: XXX.XXX.XXX.XXX

Why These Specific Numbers? The range 0-255 isn't random - it represents exactly what a computer can store in 8 bits of memory. Since computers think in binary (1s and 0s), each section of an IP address uses 8 binary digits (called bits), giving us $2^8 = 256$ possible values (0 through 255).

Real-World Example: Your home router probably assigns addresses like 192.168.1.1 to itself and gives your devices addresses like 192.168.1.100, 192.168.1.101, etc. This is like your router being the "neighborhood coordinator" that hands out house numbers to all devices in your home network.

The Binary Connection: When you see 192.168.1.1, your computer actually sees: 11000000.10101000.00011000.00000001

Don't worry - you don't need to memorize binary! Just understand that computers use this binary format to process IP addresses incredibly quickly.

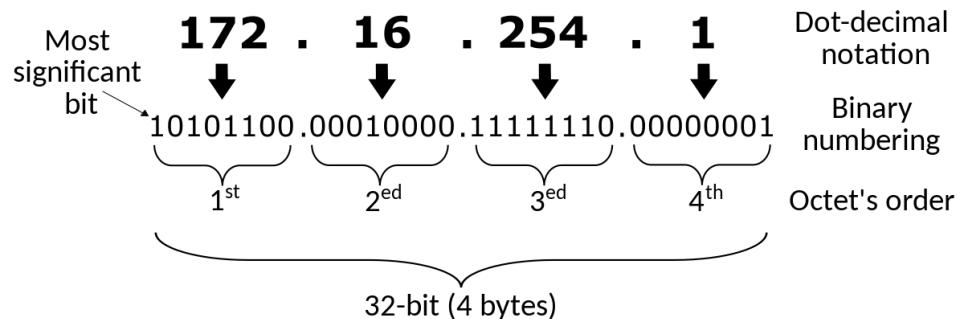


Figure 1: IPv4 Address Structure and Binary Representation

3.2. Understanding IPv4 Address Classes - The Original Neighborhood System

In the early days of the internet, engineers created a system called "address classes" to organize IP addresses efficiently. Think of this like dividing a city into different types of neighborhoods based on size and purpose.

Class A - The Mega Cities (1.0.0.0 to 126.255.255.255) Class A addresses were designed for enormous organizations that needed millions of device addresses. Think of companies like IBM or government agencies that have vast networks spanning multiple countries.

- Network portion: Only the first number (like a country code)
- Host portion: The last three numbers (like state, city, and street address)
- Can support: Over 16 million devices per network!
- Default subnet mask: 255.0.0.0 (or /8 in modern notation)

Real-World Example: If your organization got the Class A network 10.0.0.0, you could assign addresses from 10.0.0.1 all the way up to 10.255.255.254. That's enough addresses for every person in a large country!

Class B - The Big Cities (128.0.0.0 to 191.255.255.255) Class B was perfect for medium to large organizations - think universities, hospitals, or regional companies.

- Network portion: First two numbers (like country and state)
- Host portion: Last two numbers (like city and street)
- Can support: About 65,000 devices per network
- Default subnet mask: 255.255.0.0 (or /16)

Class C - The Small Towns (192.0.0.0 to 223.255.255.255) Class C addresses were designed for small businesses and organizations. This is what most small offices and home networks use today.

- Network portion: First three numbers (like country, state, and city)
- Host portion: Only the last number (like street address)
- Can support: 254 devices per network (perfect for small offices!)
- Default subnet mask: 255.255.255.0 (or /24)

Why Only 254 Devices in Class C? You might wonder why Class C supports 254 devices instead of 256. Here's why: in every network, two addresses are reserved:

- The first address (like 192.168.1.0) identifies the network itself
- The last address (like 192.168.1.255) is used for broadcasting messages to all devices

Classes D and E - Special Purpose

- **Class D (224.0.0.0 to 239.255.255.255):** Used for multicast - sending the same message to multiple devices simultaneously (like streaming live video to multiple viewers)
- **Class E (240.0.0.0 to 255.255.255.255):** Reserved for experimental use and future applications

Five Different Classes of IPv4 Addresses						
Class	First Octet decimal (range)	First Octet binary (range)	IP range	Subnet Mask	Hosts per Network ID	# of networks
Class A	0 — 127	0XXXXXXX	0.0.0.0-127.255.255.255	255.0.0.0	$2^{24}-2$	2^7
Class B	128 — 191	10XXXXXX	128.0.0.0-191.255.255.255	255.255.0.0	$2^{16}-2$	2^{14}
Class C	192 — 223	110XXXXX	192.0.0.0-223.255.255.255	255.255.255.0	2^8-2	2^{20}
Class D (Multicast)	224 — 239	1110XXXX	224.0.0.0-239.255.255.255			
Class E (Experimental)	240 — 255	1111XXXX	240.0.0.0-255.255.255.255			

Figure 2: IPv4 Address Classes Distribution

3.3. Private IP Addresses - Your Home Network's Secret Language

Here's something fascinating: not all IP addresses are visible on the internet! Just like how your home has internal room numbers (bedroom 1, bedroom 2) that only make sense within your house, networks use private IP addresses for internal communication.

The Three Private Address Ranges: Think of these as "internal use only" addresses that were specifically set aside for private networks:

1. The 10.x.x.x Range (Class A Private)

- Range: 10.0.0.0 to 10.255.255.255
- Best for: Large organizations with thousands of devices
- Example: A university might use 10.1.0.0 for the engineering building, 10.2.0.0 for the library, etc.

2. The 172.16.x.x Range (Class B Private)

- Range: 172.16.0.0 to 172.31.255.255
- Best for: Medium-sized businesses
- Example: A company might use 172.16.1.0 for the accounting department, 172.16.2.0 for marketing

3. The 192.168.x.x Range (Class C Private)

- Range: 192.168.0.0 to 192.168.255.255
- Best for: Home networks and small offices
- Example: Your home router probably uses 192.168.1.1, and your devices get addresses like 192.168.1.100, 192.168.1.101, etc.

How Private Addresses Work - The Magic of NAT Here's the clever part: when your device with private IP address 192.168.1.100 wants to access the internet, your router performs a trick called Network Address Translation (NAT). It's like having a translator who converts your internal "room number" to your home's public street address when sending mail.

Step-by-Step Example:

1. Your laptop (192.168.1.100) wants to visit Google

2. Your router receives the request from your laptop
3. Router translates: "This request is coming from my public IP address (let's say 203.0.113.5)"
4. Google sends the response back to 203.0.113.5
5. Your router remembers this was for your laptop and forwards it to 192.168.1.100

This system allows millions of homes and businesses to reuse the same private IP addresses internally while still having unique public addresses for internet communication.

4. IPv6 Addressing Fundamentals

4.1. IPv6 Address Structure

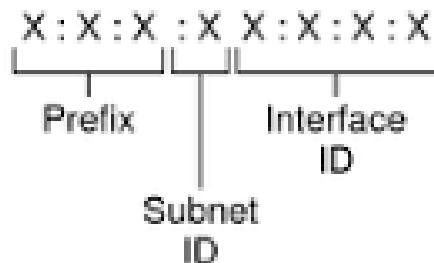
IPv6 (Internet Protocol version 6) uses 128-bit addresses, providing approximately 340 undecillion unique addresses. IPv6 addresses are represented in hexadecimal notation with eight groups of four hexadecimal digits separated by colons.

Address Format: XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX

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

Address Compression Rules:

- Leading zeros in each group can be omitted
- Consecutive groups of zeros can be replaced with "::" (only once per address)
- Example compressed: 2001:db8:85a3::8a2e:370:7334



Example:

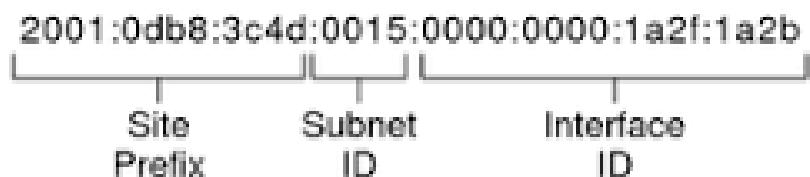


Figure 3: IPv6 Address Structure and Format

4.2. IPv6 Address Types

Unicast Addresses:

- Global Unicast: 2000::/3 (Routable on the Internet)
- Link-Local: FE80::/10 (Local network segment only)
- Unique Local: FC00::/7 (Private addressing, similar to RFC 1918)

Multicast Addresses: FF00::/8 **Anycast Addresses:** Same format as unicast but assigned to multiple interfaces

5. Subnet Masks and CIDR - The Language of Network Division

5.1. Understanding Subnet Masks Through Simple Analogies

Think of a subnet mask as a template that tells your computer: "These parts of the IP address represent the neighborhood (network), and these parts represent the house number (host)." It's like having a postal code system where you need to know which digits represent the city and which represent the specific address.

How Subnet Masks Work: A subnet mask uses the same four-part format as IP addresses, but it serves a completely different purpose. Instead of identifying a specific device, it acts like a filter that separates the network portion from the host portion of an IP address.

The Binary Magic Behind Subnet Masks: In binary, subnet masks are incredibly simple - they're just a series of 1s followed by a series of 0s:

- The 1s say: "This part identifies the network"
- The 0s say: "This part identifies the specific device"

Natural (Default) Subnet Masks Explained: Let's break down the default subnet masks using our neighborhood analogy:

Class A Mask (255.0.0.0):

- In binary: 1111111.00000000.00000000.00000000
- Meaning: Only the first number identifies the network
- Like saying: "10" is the neighborhood, everything else is the house number
- Example: In 10.50.100.200, "10" is the network, "50.100.200" is the specific device

Class B Mask (255.255.0.0):

- In binary: 1111111.1111111.00000000.00000000
- Meaning: First two numbers identify the network
- Like saying: "172.16" is the neighborhood, the rest is the house number
- Example: In 172.16.5.100, "172.16" is the network, "5.100" is the specific device

Class C Mask (255.255.255.0):

- In binary: 1111111.1111111.1111111.00000000
- Meaning: First three numbers identify the network
- Like saying: "192.168.1" is the neighborhood, only the last number is the house number
- Example: In 192.168.1.100, "192.168.1" is the network, "100" is the specific device

5.2. CIDR Notation - The Modern Way to Express Networks

CIDR (Classless Inter-Domain Routing) is like shorthand for writing subnet masks. Instead of writing out the full mask like 255.255.255.0, we simply write /24.

Why /24? The number after the slash tells us how many bits (starting from the left) are set to 1 in the subnet mask:

- /24 means the first 24 bits are 1s, last 8 bits are 0s
- 24 ones in binary = 1111111.1111111.1111111.00000000
- Which equals 255.255.255.0 in decimal

Common CIDR Examples You'll See:

- **192.168.1.0/24:** Your typical home network (254 possible devices)
- **10.0.0.0/8:** A massive corporate network (over 16 million possible devices)
- **172.16.0.0/16:** A medium business network (about 65,000 possible devices)
- **192.168.1.0/25:** Half of a typical home network (126 devices)
- **192.168.1.0/30:** A tiny network for just 2 devices (often used for router-to-router connections)

5.3. The Relationship Between CIDR and Available Addresses

Here's a handy way to remember how CIDR notation relates to the number of available addresses:

The Power of 2 Rule: Available addresses = $2^{(32 - \text{CIDR_number})}$

Examples:

- /24 network: $2^{(32-24)} = 2^8 = 256$ total addresses (254 usable)
- /25 network: $2^{(32-25)} = 2^7 = 128$ total addresses (126 usable)
- /26 network: $2^{(32-26)} = 2^6 = 64$ total addresses (62 usable)
- /30 network: $2^{(32-30)} = 2^2 = 4$ total addresses (2 usable)

Figure 4: CIDR Notation and Subnet Mask Relationship

5.4. CIDR Calculation Table

CIDR	Subnet Mask	Network Bits	Host Bits	Total Hosts
/8	255.0.0.0	8	24	16,777,216
/16	255.255.0.0	16	16	65,536
/24	255.255.255.0	24	8	256
/25	255.255.255.128	25	7	128
/26	255.255.255.192	26	6	64
/27	255.255.255.224	27	5	32
/28	255.255.255.240	28	4	16
/29	255.255.255.248	29	3	8
/30	255.255.255.252	30	2	4

6. Understanding Subnetting - Dividing Your Digital Neighborhood

6.1. What is Subnetting and Why Do We Need It?

Imagine you're the mayor of a growing city. Initially, you had one big neighborhood where everyone lived together. As the city grows, you realize you need to organize better - you want to separate residential areas from commercial districts, create different zones for schools and hospitals, and ensure emergency services can find locations quickly.

Subnetting works exactly the same way for computer networks. It's the process of taking a block of IP addresses and carving out smaller blocks from it, creating separate "digital neighborhoods" within your larger network.

Real-World Business Example: Let's say you work for a company that just got the IP range 192.168.1.0/24 (256 addresses total). Without subnetting, all 250+ devices would be in one big network - computers, printers, servers, security cameras, and IoT devices all mixed together. This creates several problems:

Problems Without Subnetting:

- Security Risks:** A compromised printer could potentially access sensitive financial servers
- Performance Issues:** All devices compete for the same network resources
- Management Chaos:** Troubleshooting becomes a nightmare when everything is mixed together
- Broadcast Storms:** When one device sends a broadcast message, ALL devices receive it, creating unnecessary traffic

Benefits of Subnetting:

- Enhanced Security:** Different departments can each have their own subnet, keeping their data traffic separate from others
- Better Performance:** Smaller broadcast domains mean less network congestion
- Easier Management:** Network administrators can quickly identify which subnet a problem device belongs to
- Logical Organization:** Group devices by function, department, or security level

6.2. Real-World Subnetting Scenarios

Let's explore some practical examples of how organizations use subnetting:

Scenario 1: Small Office Setup A dental office with 50 devices needs to separate:

- Patient management systems (high security)
- Office computers and printers (medium security)
- Guest WiFi for patients (low security, isolated)
- IoT devices like smart thermostats (separate for security)

Scenario 2: School Network A school with 500 devices might create subnets for:

- Administrative offices (financial data, student records)
- Teacher workstations and classroom computers
- Student WiFi network
- Security cameras and access control systems
- Library and public computer lab

Scenario 3: Manufacturing Plant An industrial facility might separate:

- Operational technology (OT) - machinery control systems
- Information technology (IT) - office computers and servers
- Safety systems - fire alarms, emergency communications
- Visitor network - contractors and guests

7. Practical Subnetting - Step-by-Step Guide with Real Examples

7.1. The Coffee Shop Network - A Complete Walkthrough

Let's work through a real-world example that will teach you everything you need to know about subnetting. Imagine you're setting up the network for a coffee shop that also offers co-working spaces.

Your Assignment: The coffee shop has been assigned the network 192.168.1.0/24, and you need to create separate subnets for:

1. Point-of-Sale (POS) systems - needs 10 devices
2. Employee devices (laptops, tablets) - needs 20 devices
3. Customer WiFi - needs 50 devices
4. Co-working space - needs 30 devices

5. Security cameras and IoT - needs 15 devices

Step 1: Plan Your Subnets (Always Start with the Largest) Always design subnets starting with the one that needs the most addresses:

- Customer WiFi: 50 devices (needs at least 64 addresses)
- Co-working space: 30 devices (needs at least 32 addresses)
- Employee devices: 20 devices (needs at least 32 addresses)
- Security/IoT: 15 devices (needs at least 16 addresses)
- POS systems: 10 devices (needs at least 16 addresses)

Step 2: Calculate Required Subnet Sizes For each requirement, find the next power of 2 that's larger than your device count:

- 50 devices → need 64 addresses → need 6 host bits ($2^6 = 64$) → /26 subnet
- 30 devices → need 32 addresses → need 5 host bits ($2^5 = 32$) → /27 subnet
- 20 devices → need 32 addresses → need 5 host bits ($2^5 = 32$) → /27 subnet
- 15 devices → need 16 addresses → need 4 host bits ($2^4 = 16$) → /28 subnet
- 10 devices → need 16 addresses → need 4 host bits ($2^4 = 16$) → /28 subnet

Step 3: Assign Your Subnets Starting with 192.168.1.0/24, let's carve out our subnets:

Subnet 1 - Customer WiFi (192.168.1.0/26):

- Network Address: 192.168.1.0
- First Usable Address: 192.168.1.1 (usually assigned to the wireless access point)
- Last Usable Address: 192.168.1.62
- Broadcast Address: 192.168.1.63
- Total Addresses: 64 (62 usable for devices)

Subnet 2 - Co-working Space (192.168.1.64/27):

- Network Address: 192.168.1.64
- First Usable: 192.168.1.65 (gateway/router interface)
- Last Usable: 192.168.1.94
- Broadcast: 192.168.1.95
- Total: 32 (30 usable)

Subnet 3 - Employee Devices (192.168.1.96/27):

- Network Address: 192.168.1.96

- First Usable: 192.168.1.97
- Last Usable: 192.168.1.126
- Broadcast: 192.168.1.127
- Total: 32 (30 usable)

Subnet 4 - Security/IoT (192.168.1.128/28):

- Network Address: 192.168.1.128
- First Usable: 192.168.1.129
- Last Usable: 192.168.1.142
- Broadcast: 192.168.1.143
- Total: 16 (14 usable)

Subnet 5 - POS Systems (192.168.1.144/28):

- Network Address: 192.168.1.144
- First Usable: 192.168.1.145
- Last Usable: 192.168.1.158
- Broadcast: 192.168.1.159
- Total: 16 (14 usable)

Step 4: Verify Your Work Let's check that we haven't wasted addresses:

- Used: $64 + 32 + 32 + 16 + 16 = 160$ addresses
- Available in /24: 256 addresses
- Remaining: 96 addresses (available for future expansion!)

7.2. Variable Length Subnet Masking (VLSM)

VLSM allows different subnet mask lengths within the same network, enabling efficient address space utilization. This technique is essential for hierarchical network design and optimal resource allocation.

VLSM Process:

1. Identify subnet requirements (number of hosts per subnet)
2. Order subnets from largest to smallest
3. Assign appropriate subnet masks starting with the largest subnet
4. Ensure no address overlap between subnets

7.3. Subnetting Calculation Methods

Host-Based Subnetting:

1. Determine required number of hosts per subnet
2. Calculate host bits needed: $2^n \geq (\text{required hosts} + 2)$
3. Network bits = 32 - host bits
4. Subnet mask = first (network bits) set to 1, remaining set to 0

Network-Based Subnetting:

1. Determine required number of subnets
2. Calculate subnet bits needed: $2^n \geq \text{required subnets}$
3. Borrow bits from host portion
4. New subnet mask = original mask + borrowed bits

7.4. Practical Subnetting Example

Scenario: Subnet 192.168.1.0/24 into 4 subnets

Solution:

1. Required subnets: 4, so we need 2 bits ($2^2 = 4$)
2. New subnet mask: $/24 + 2 = /26$ (255.255.255.192)
3. Each subnet has $2^6 = 64$ addresses (62 usable)
4. Subnets:
 - Subnet 1: 192.168.1.0/26 (192.168.1.1 - 192.168.1.62)
 - Subnet 2: 192.168.1.64/26 (192.168.1.65 - 192.168.1.126)
 - Subnet 3: 192.168.1.128/26 (192.168.1.129 - 192.168.1.190)
 - Subnet 4: 192.168.1.192/26 (192.168.1.193 - 192.168.1.254)

8. IPv6 Subnetting

8.1. IPv6 Subnetting Principles

IPv6 subnetting is simpler than IPv4 due to the abundant address space. Standard practices include:

Standard Allocations:

- /48 prefix for sites/organizations
- /64 prefix for individual subnets (standard subnet size)

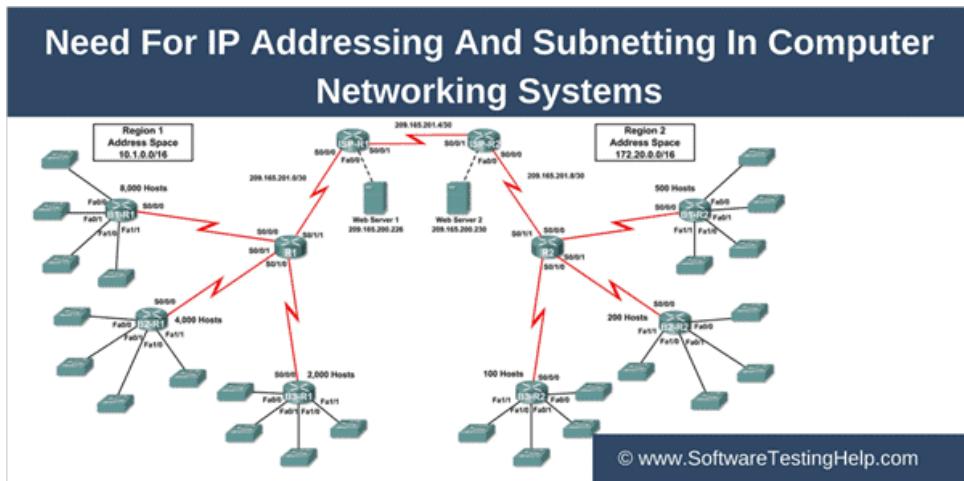


Figure 5: Practical Subnetting Example Visualization

- /128 for individual hosts (host routes)

Subnetting Process:

1. Start with allocated prefix (e.g., 2001:db8::/32)
2. Use 16 bits for subnet identification (/32 to /48)
3. Reserve /64 for end-user subnets
4. Remaining 64 bits for host addressing

8.2. IPv6 Subnetting Example

Given: 2001:db8::/32 allocation

Subnetting:

- Site 1: 2001:db8:0001::/48
- Site 2: 2001:db8:0002::/48
- Within Site 1:
 - Subnet 1: 2001:db8:0001:0001::/64
 - Subnet 2: 2001:db8:0001:0002::/64
 - Subnet 3: 2001:db8:0001:0003::/64

9. Host Counting and Address Range Calculations

9.1. IPv4 Host Calculations

Formula for usable hosts: $2^{\text{host_bits}} - 2$

The subtraction of 2 accounts for:

- Network address (first address)

- Broadcast address (last address)

Examples:

- /24 network: $2^8 - 2 = 254$ usable hosts
- /25 network: $2^7 - 2 = 126$ usable hosts
- /26 network: $2^6 - 2 = 62$ usable hosts
- /30 network: $2^2 - 2 = 2$ usable hosts (point-to-point links)

9.2. IPv6 Host Calculations

IPv6 does not use broadcast addresses, so the calculation is simpler:

Formula: $2^{\text{host_bits}}$

Note: While the network identifier is conceptually "used" by the network, it's not a broadcast address, and any address within the /64 prefix (excluding the all-zeros network address, which is typically reserved) can technically be assigned to a host. The formula 2^{64} gives the total number of addresses in a /64, and effectively all are usable for hosts in IPv6. However, if you strictly follow the "network address" concept, you might subtract 1. For most practical purposes in IPv6, the sheer number of addresses makes this distinction less critical than in IPv4. I'll use $2^{\text{host_bits}}$ as it's the most common representation for total available addresses within an IPv6 subnet. If you need to reserve one for the network ID, you can adjust to $2^{\text{host_bits}} - 1$.

Standard /64 subnet: $2^{64} = 18,446,744,073,709,551,616$ addresses

10. Advanced Subnetting Concepts

10.1. Supernetting (Route Aggregation)

Supernetting combines multiple smaller networks into a larger one to reduce routing table entries. This technique is essential for efficient routing in large networks.

Example: Combining four /26 networks into one /24:

- 192.168.1.0/26, 192.168.1.64/26, 192.168.1.128/26, 192.168.1.192/26
- Aggregated as: 192.168.1.0/24

10.2. Subnet Design Best Practices

Planning Considerations:

- Future growth requirements
- Security and traffic isolation needs
- Hierarchical addressing scheme
- Route summarization opportunities
- Administrative boundaries

Documentation Requirements:

- IP address management (IPAM) systems
- Subnet allocation records
- Network topology diagrams
- Addressing standards and policies

11. Implementation in Network Equipment

11.1. Cisco Configuration Examples

Basic Interface Configuration:

```
interface FastEthernet0/1
  ip address 192.168.1.1 255.255.255.0
  no shutdown
```

VLSM Configuration:

```
interface Serial0/0
  ip address 10.1.1.1 255.255.255.252
interface FastEthernet0/0
  ip address 10.1.2.1 255.255.255.0
```

11.2. IPv6 Configuration

Basic IPv6 Interface:

```
interface FastEthernet0/1
  ipv6 address 2001:db8:1::1/64
  ipv6 enable
```

12. Troubleshooting and Validation

12.1. Common Subnetting Errors

- Overlapping subnet ranges
- Incorrect subnet mask calculations
- Forgetting to account for network and broadcast addresses
- Insufficient host bits for requirements
- Improper VLSM implementation

12.2. Validation Tools and Techniques

Command Line Tools:

- ping - Connectivity testing
- traceroute/tracert - Path verification
- netstat - Network statistics
- ipconfig/ifconfig - Interface configuration

Network Calculators: Online and software-based subnet calculators for verification and planning.

13. Conclusion

IP addressing and subnetting form the foundation of modern network infrastructure. Understanding both IPv4 and IPv6 addressing schemes, CIDR notation, and subnetting techniques is essential for network engineers and administrators. Proper subnet design enables efficient resource utilization, enhances security through network segmentation, and supports scalable network growth. As networks continue to evolve, mastery of these fundamental concepts remains crucial for successful network implementation and management.

The transition from IPv4 to IPv6 presents both challenges and opportunities. While IPv4 subnetting requires careful address conservation due to limited address space, IPv6 provides abundant addressing that simplifies design decisions while introducing new architectural considerations. Network professionals must be proficient in both protocols to manage today's hybrid network environments effectively.

References

- RFC 791 - Internet Protocol (IPv4). IETF DataTracker. <https://datatracker.ietf.org/doc/html/rfc791>
- RFC 8200 - Internet Protocol, Version 6 (IPv6) Specification. RFC Editor. <https://www.rfc-editor.org/rfc/rfc8200.html>
- Cisco Systems. (2024). IP Routing: RIP Configuration Guide. <https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html>
- Juniper Networks. Understanding IPv4 and IPv6 Protocol Families. <https://www.juniper.net/documentation/us/en/software/junos/routing-protocol-independent-topics/concept/routing-protocol-families-overview.html>
- UniNets. What is IP Addressing and Subnetting? How to Configure in Cisco. <https://www.uninets.com/blogs/what-is-ip-addressing-and-subnetting-how-to-configure-in-cisco>