Ayush Jain

Celebal Technologies

IP Addressing and Subnetting

14 June 2025

## IP Addressing

An IP address is an address used in order to uniquely identify a device on an IP network. The address is made up of 32 binary bits, which can be divisible into a network portion and host portion with the help of a subnet mask. The 32 binary bits are broken into four octets (1 octet = 8 bits). Each octet is converted to decimal and separated by a period (dot). For this reason, an IP address is said to be expressed in dotted decimal format (for example, 172.16.81.100). The value in each octet ranges from 0 to 255 decimal, or 00000000 - 11111111 binary.

Here is how binary octets convert to decimal: The right most bit, or least significant bit, of an octet holds a value of $2^0$. The bit just to the left of that holds a value of $2^1$. This continues until the left-most bit, or most significant bit, which holds a value of $2^7$. So if all binary bits are a one, the decimal equivalent would be 255 as shown here:

```
   1   1   1   1 1 1 1 1
 128  64  32  16 8 4 2 1 (128+64+32+16+8+4+2+1=255)
```

Here is a sample octet conversion when not all of the bits are set to 1.

```
 0   1 0 0 0 0 0 1
 0  64 0 0 0 0 0 1 (0+64+0+0+0+0+0+1=65)
```

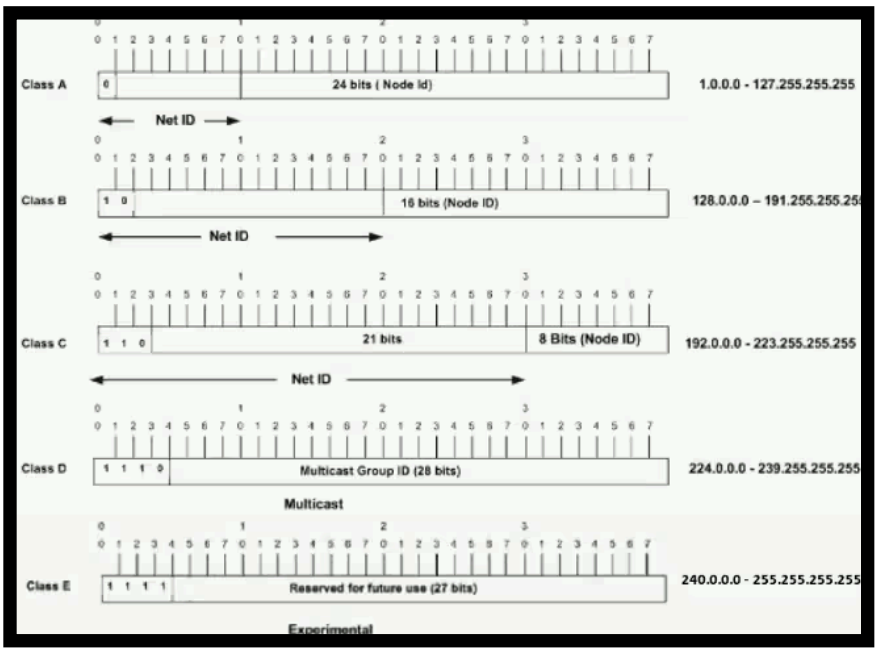
And this sample shows an IP address represented in both binary and decimal.

```
        10.       1.      23.      19 (decimal)
 00001010.00000001.00010111.00010011 (binary)
```

These octets are broken down to provide an addressing scheme that can accommodate large and small networks. There are five different classes of networks, A to E. This document focuses on classes A to C, since classes D and E are reserved, and discussion of them is beyond the scope of this document.

Given an IP address, its class can be determined from the three high-order bits (the three left-most bits in the first octet). Figure 1 shows the significance in the three high order bits and the range of addresses that fall into

each class. For informational purposes, Class D and Class E addresses are also shown.




In a Class A address, the first octet is the network portion, so the Class A example in Figure 1 has a major network address of 1.0.0.x - 127.255.255.x (where x can go from 0 to 255). Octets 2, 3, and 4 (the next 24 bits) are for the network manager to divide into subnets and hosts as he/she sees fit. Class A addresses are used for networks that have more than 65,536 hosts (actually, up to 16777214 hosts!).

In a Class B address, the first two octets are the network portion, so the Class B example in Figure 1 has a major network address of 128.0.0.x - 191.255.255.x. Octets 3 and 4 (16 bits) are for local subnets and hosts. Class B addresses are used for networks that have between 256 and 65534 hosts.

In a Class C address, the first three octets are the network portion. The Class C example in Figure 1 has a major network address of 192.0.0.x - 223.255.255.x. Octet 4 (8 bits) is for local subnets and hosts - perfect for networks with less than 254 hosts.

An IP address, or Internet Protocol address, is a unique string of numbers assigned to each device connected to a computer network that uses the Internet Protocol for communication. It serves as an identifier that allows devices to send and receive data over the network, ensuring that this data reaches the correct destination.

## Subnetting

Subnetting allows you to create multiple logical networks that exist within a single Class A, B, or C network. If you do not subnet, you are only able to use one network from your Class A, B, or C network, which is unrealistic.

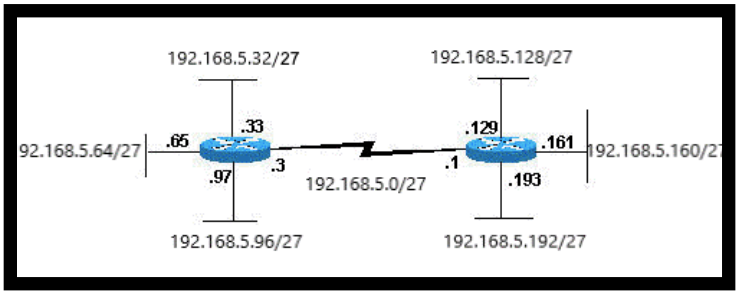
Each data link on a network must have a unique network ID, and every node on that link is a member of the same network. If you break a major network (Class A, B, or C) into smaller subnetworks, it allows you to create a network of interconnecting subnetworks. Each data link on this network would then have a unique network/subnetwork ID. Any device, or gateway, that connects *n* networks/subnetworks has *n* distinct IP addresses, one for each network / subnetwork that it interconnects.

In order to subnet a network, extend the natural mask with some of the bits from the host ID portion of the address in order to create a subnetwork ID. For example, given a Class C network of 192.168.5.0 which has a natural mask of 255.255.255.0, you can create subnets in this manner:

```
192.168.5.0     - 11000000.10101000.00000101.00000000
255.255.255.224 - 11111111.11111111.11111111.11100000
                  -------------------------|sub|----
```

By extending the mask to be 255.255.255.224, you have taken three bits (indicated by sub) from the original host portion of the address and used them to make subnets. With these three bits, it is possible to create eight subnets. With the other five host ID bits, each subnet can have up to 32 host addresses, 30 of which can actually be assigned to a device since host ids of all zeros or all ones are not allowed (it is very important to remember this). So, with this in mind, these subnets have been created.

```
192.168.5.0 255.255.255.224     host address range 1 to
30
192.168.5.32 255.255.255.224    host address range 33
to 62
192.168.5.64 255.255.255.224    host address range 65
to 94
192.168.5.96 255.255.255.224    host address range 97
to 126
192.168.5.128 255.255.255.224   host address range 129
to 158
192.168.5.160 255.255.255.224   host address range 161
to 190
192.168.5.192 255.255.255.224   host address range 193
to 222
192.168.5.224 255.255.255.224   host address range 225
to 254
```




Notice that each of the routers in Figure 2 is attached to four subnetworks, one subnetwork is common to both routers. Also, each router has an IP address for each subnetwork to which it is attached. Each subnetwork could potentially support up to 30 host addresses.

This brings up an interesting point. The more host bits you use for a subnet mask, the more subnets you have available. However, the more subnets available, the less host addresses available per subnet. For example, a Class C network of 192.168.5.0 and a mask of 255.255.255.224 (/27) allows you to have eight subnets, each with 32 host addresses (30 of which could be assigned to devices). If you use a mask of 255.255.255.240 (/28), the breakdown is:

```
192.168.5.0     - 11000000.10101000.00000101.00000000
255.255.255.240 - 11111111.11111111.11111111.11110000
                  -------------------------|sub |---
```

Since you now have four bits to make subnets with, you only have four bits left for host addresses. So in this case you can have up to 16 subnets, each of which can have up to 16 host addresses (14 of which can be assigned to devices).

Look at how a Class B network can be subnetted. If you have network 172.16.0.0, then you know that its natural mask is 255.255.0.0 or 172.16.0.0/16. Extending the mask to anything beyond 255.255.0.0 means you are subnetting. You can quickly see that you have the ability to create a lot more subnets than with the Class C network. If you use a mask of 255.255.248.0 (/21), how many subnets and hosts per subnet does this allow for?

```
172.16.0.0   -   10101100.00010000.00000000.00000000
255.255.248.0 - 11111111.11111111.11111000.00000000
                ----------------| sub |-----------
```

You use five bits from the original host bits for subnets. This allows you to have 32 subnets ($2^5$). When the five bits for subnetting are used, you are left with 11 bits for host addresses. This allows each subnet so have 2048 host addresses ($2^{11}$), 2046 of which could be assigned to devices.

## Sample Exercise 1

Now that you understand subnetting, put this knowledge to use. In this example, you are given two address / mask combinations, written with the prefix/length notation, which have been assigned to two devices. Your task is to determine if these devices are on the same subnet or different subnets. You can use the address and mask of each device in order to determine to which subnet each address belongs.

```
DeviceA: 172.16.17.30/20
DeviceB: 172.16.28.15/20
```

Determine the Subnet for DeviceA:

```
172.16.17.30  -   10101100.00010000.00010001.00011110
255.255.240.0 -   11111111.11111111.11110000.00000000
                  ----------------| sub|------------
subnet =          10101100.00010000.00010000.00000000 =
172.16.16.0
```

Look at the address bits that have a corresponding mask bit set to one, and set all the other address bits to zero (this is equivalent to when you perform a logical AND between the mask and address). It shows you to which subnet this address belongs. In this case, Device A belongs to subnet 172.16.16.0.

Determine the Subnet for DeviceB:

```
172.16.28.15  -   10101100.00010000.00011100.00001111
255.255.240.0 -   11111111.11111111.11110000.00000000
                  ----------------| sub|------------
subnet =          10101100.00010000.00010000.00000000 =
172.16.16.0
```

From these determinations, Device A and Device B have addresses that are part of the same subnet.

A subnet is like a smaller group within a large network. It is a way to split a large network into smaller networks so that devices present in one network can transmit data more easily. For example, in a company, different departments can each have their own subnet, keeping their data traffic separate from others. Subnet makes the network faster and easier to manage and also improves the security of the network.

IPv4

IPv4, or Internet Protocol version 4, is the original addressing system of the Internet, introduced in 1983. It uses a 32-bit address scheme, which theoretically allows for over 4 billion unique addresses (2^32). IPv4 addresses are typically displayed in decimal format, divided into four octets separated

by dots. For example, 192.168.1.1 is a common IPv4 address you might find in a home network.

IPv4 Address Format is a 32-bit Address that comprises binary digits separated by a dot (.).

Characteristics of IPv4-:

- 32-bit address length: Allows for approximately 4.3 billion unique addresses.
- Dot-decimal notation: IP addresses are written in a format of four decimal numbers separated by dots, such as 192.168.1.1.
- Packet structure: Includes a header and payload; the header contains information essential for routing and delivery.
- Checksum fields: Uses checksums in the header for error-checking the header integrity.
- Fragmentation: Allows packets to be fragmented at routers along the route if the packet size exceeds the maximum transmission unit (MTU).
- Address Resolution Protocol (ARP): Used for mapping IP network addresses to the hardware addresses used by a data link protocol.

Drawbacks of IPv4-:

- Limited Address Space : IPv4 has a limited number of addresses, which is not enough for the growing number of devices connecting to the internet.
- Complex Configuration : IPv4 often requires manual configuration or DHCP to assign addresses, which can be time-consuming and prone to errors.
- Less Efficient Routing : The IPv4 header is more complex, which can slow down data processing and routing.
- Security Issues : IPv4 does not have built-in security features, making it more vulnerable to attacks unless extra security measures are added.
- Limited Support for Quality of Service (QoS) : IPv4 has limited capabilities for prioritizing certain types of data, which can affect the performance of real-time applications like video streaming and VoIP.

## IPv6

Another most common version of the Internet Protocol currently is IPv6. The well-known IPv6 protocol is being used and deployed more often, especially in mobile phone markets. IPv6 was designed by the Internet Engineering Task Force (IETF) in December 1998 with the purpose of superseding IPv4 due to the global exponentially growing internet of users.

IPv6 stands for Internet Protocol version 6. IPv6 is the new version of Internet Protocol, which is way better than IPv4 in terms of complexity and efficiency. IPv6 is written as a group of 8 hexadecimal numbers separated by colon (:). It can be written as 128 bits of 0s and 1s. IPv6 Address Format is a 128-bit IP Address, which is written in a group of 8 hexadecimal numbers separated by colon (:).

Characteristics of IPv6

- IPv6 uses 128-bit addresses, offering a much larger address space than IPv4's 32-bit system.
- IPv6 addresses use a combination of numbers and letters separated by colons, allowing for more unique addresses.
- The IPv6 header has fewer fields, making it more efficient for routers to process.
- IPv6 supports Unicast, Multicast, and Anycast, but no Broadcast, reducing network traffic.
- IPv6 allows flexible subnetting (VLSM) to divide networks based on specific needs.
- IPv6 uses Neighbor Discovery for MAC address resolution instead of ARP.

Benefits of IPv6 over IPv4
The recent Version of IP IPv6 has a greater advantage over IPv4. Here are some of the mentioned benefits:

- Larger Address Space: IPv6 has a greater address space than IPv4, which is required for expanding the IP Connected Devices. IPv6 has 128 bit IP Address rather and IPv4 has a 32-bit Address.
- Improved Security: IPv6 has some improved security which is built in with it. IPv6 offers security like Data Authentication, Data Encryption, etc. Here, an Internet Connection is more Secure.
- Simplified Header Format: As compared to IPv4, IPv6 has a simpler and more effective header Structure, which is more cost-effective and also increases the speed of Internet Connection.
- Prioritise: IPv6 contains stronger and more reliable support for QoS features, which helps in increasing traffic over websites and increases audio and video quality on pages.

To create subnets using natural masks, you start with the default subnet mask (also called natural mask) for the class of the IP address (A, B, or C) and then "borrow" bits from the host portion to create subnets. This process effectively increases the number of network bits and decreases the number of host bits, allowing you to divide a single network into smaller, more manageable subnets. [1, 2]

Here's a breakdown of the process:

1. Understand Natural Masks:
   - Class A: Natural mask is 255.0.0.0 (or /8 in CIDR notation). [1, 3, 3, 4]
   - Class B: Natural mask is 255.255.0.0 (or /16 in CIDR notation). [2, 2, 3, 3, 5, 6]
   - Class C: Natural mask is 255.255.255.0 (or /24 in CIDR notation). [2, 2, 3, 3]
2. Determine the Number of Subnets: [1, 2, 2, 7]
   - Decide how many subnets you need. The number of subnets determines how many bits you need to borrow from the host portion. [1, 1, 2, 2, 8]
   - Use the formula 2^n >= number of subnets, where 'n' is the number of bits borrowed. [2, 9, 10, 11]
3. Adjust the Subnet Mask:
   - Take the borrowed bits and add them to the natural mask. This involves converting the borrowed bits to their decimal value and adding it to the appropriate octet.
   - For example, if you need 8 subnets, you need to borrow 3 bits from the host portion of a class B address. The natural mask is 255.255.0.0. Borrowing 3 bits results in the subnet mask 255.255.224.0. [1, 1, 9, 9, 12, 13]
4. Calculate Subnet Addresses:
   - Each subnet will have a unique network address. You can calculate these by incrementing the borrowed bits in binary and converting back to decimal.
   - For the example above (255.255.224.0), the first subnet would be 129.99.0.0, the second would be 129.99.32.0, the third 129.99.64.0, and so on. [1, 1, 2, 2, 14]

Example:

Let's say you have a class C network (e.g., 192.168.1.0/24) and you want to create 4 subnets. [1, 1, 2, 2, 9, 9, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25]

1. Natural mask: 255.255.255.0
2. Number of subnets: 4. You need to borrow 2 bits (2^2 = 4).

3. Adjusted subnet mask: The original host portion is the 4th octet (255.255.255.0). Borrowing 2 bits gives you 255.255.255.192 (/26 in CIDR notation).
4. Subnet addresses: The first subnet is 192.168.1.0/26, the second is 192.168.1.64/26, the third is 192.168.1.128/26, and the fourth is 192.168.1.192/26.

By following these steps, you can effectively subnet your network using natural masks, creating smaller, more manageable networks. [1, 2].

A subnet mask is a 32-bit number that divides an IP address into network and host portions, helping devices determine which network they belong to and how to communicate. It's crucial for network segmentation and efficient data routing. [1, 2, 3, 4]

Key Concepts:

- Network and Host Addresses: An IP address is split into a network address (identifying the network) and a host address (identifying a specific device on that network). [1, 5]
- Subnetting: The process of dividing a larger network into smaller, more manageable subnets using subnet masks. [1, 6]
- IPv4 and IPv6: Subnet masks are used in both IPv4 (32-bit) and IPv6 (128-bit) addressing. [7]
- Binary Representation: Subnet masks are often represented in binary, where '1's indicate the network portion and '0's indicate the host portion. [8]
- CIDR Notation: Subnet masks can also be expressed in CIDR notation (e.g., /24), which represents the number of network bits. [7, 9, 10, 11, 12]

How it Works:

1. Network Identification: A subnet mask, combined with an IP address, allows a device to determine if another device is on the same local network or a remote network. [1, 8]
2. Data Routing: If a device needs to communicate with a device on the same subnet, it can communicate directly. If it's on a different subnet, the traffic is routed through a gateway. [1, 8, 13]
3. Efficient Routing: Subnet masks help optimize network performance by limiting broadcast traffic and reducing unnecessary data transmission across the entire network. [4]

Example:

Consider an IP address of 192.168.1.10 with a subnet mask of 255.255.255.0. The subnet mask indicates that the first three octets

(192.168.1) represent the network address, and the last octet (10) represents the host address. [1, 8, 10, 14]

In essence, a subnet mask is a fundamental tool for network management, enabling efficient communication and resource allocation within a network. [1, 4]

A subnet mask is a 32-bit number that separates an IP address into two parts: the network ID and the host ID. It tells devices which portion of the address belongs to the network and which identifies individual devices. By doing this it helps to determine which devices belong to the same local network and which devices reside on different networks. It supports efficient network organisation, better control of data flow and overall improved security and management of the network.

Advantages of Subnetting

- Reduces network congestion: Limits broadcast traffic, improving network speed.
- Efficient IP Usage: Allocates IPs based on need, avoiding wastage.
- Enhances security by isolating subnets: For example, no other department within an organisation should be able to view the code created by the Developer department.
- Enables Departmental Segmentation: A higher network priority may be needed for some subnets than for others. For instance, a sales department might need to hold video conferences or webcasts.
- Supports Scalability: Allows networks to grow while remaining organised.

Disadvantages of Subnetting

- Limited IP Address Space: Dividing networks reduces available IPs per subnet.
- Additional Hardware: Subnetting reduces the overall number of IP addresses in the network, yet it could necessitate purchasing extra hardware, like a router. Thus it could be very expensive.
- Complex Setup: Requires expertise to plan and configure subnets.
- Compatibility Issues: Older devices or systems may struggle with subnetting configurations.

CIDR

## CIDR

Classless Interdomain Routing (CIDR) was introduced in order to improve both address space utilisation and routing scalability in the Internet. It was

needed because of the rapid growth of the Internet and growth of the IP routing tables held in the Internet routers.

CIDR moves away from the traditional IP classes (Class A, Class B, Class C, and so on). In CIDR , an IP network is represented by a prefix, which is an IP address and some indication of the length of the mask. Length means the number of left-most contiguous mask bits that are set to one. So, network 172.16.0.0 255.255.0.0 can be represented as 172.16.0.0/16. CIDR also depicts a more hierarchical Internet architecture, where each domain takes its IP addresses from a higher level. This allows for the summarisation of the domains to be done at the higher level. For example, if an ISP owns network 172.16.0.0/16, then the ISP can offer 172.16.1.0/24, 172.16.2.0/24, and so on to customers. Yet, when advertising to other providers, the ISP only needs to advertise 172.16.0.0/16.

To determine the number of usable and total hosts within an IP address range, you need to know the subnet mask. The subnet mask identifies the network portion and the host portion of an IP address. **The total number of hosts is 2 raised to the power of the number of host bits (zeros in the subnet mask), minus 2 (to exclude the network and broadcast addresses)**. [1, 2]

## Formula:

- Total hosts = 2<sup>h</sup>, where 'h' is the number of host bits.
- Usable hosts = 2<sup>h</sup> - 2. [1, 2]

Example:

Let's say you have a subnet with a subnet mask of /24 (255.255.255.0). The host portion has 8 bits (32 - 24 = 8). Total hosts: 2<sup>8</sup> = 256 and Usable hosts: 256 - 2 = 254. [1, 1, 2, 3, 4, 5, 6, 7]

Therefore, a /24 subnet has 256 total IP addresses, with 254 being usable for hosts. [1, 2, 8, 9]

## Key points:

- The network address (all zeros in the host portion) and the broadcast address (all ones in the host portion) are not usable. [1, 2]
- Subnetting divides a larger network into smaller ones, allowing for more efficient use of IP addresses and better network management. [10, 11]
- CIDR (Classless Inter-Domain Routing) notation (e.g., /24) provides a concise way to represent subnet masks. [12, 13]

- Different subnet masks will result in different numbers of usable and total hosts. [1, 2]

Subnetting is a critical task in a network setup involving dividing a larger network into smaller, manageable subnet segments. Calculating the number of hosts that can fit into each subnet is essential for efficient IP address usage and network optimisation. This calculation not only ensures efficient use of IP addresses but also enhances network performance and security.

1. Number of Usable Hosts: Usable Hosts = 2h - 2, Where h is the number of bits used for hosts in the subnet mask. The subtraction of 2 accounts for the network address and the broadcast address, which cannot be assigned to hosts.

2. Number of Subnets: Total Subnets = 2s Where s is the number of bits borrowed from the original host part to create more network bits in subnetting.

Example Calculation for a /25 Subnet Mask:

- Subnet Mask: 255.255.255.128 or /25
- CIDR Notation: /25 indicates that 25 bits are used for the network part.

Calculating Usable Hosts:

- Total bits for IPv4 = 32
- Network bits = 25
- Host bits h = 32 - 25 = 7
- Usable Hosts = $27-2 = 126$

Calculating Total Subnets: Assuming we are subnetting within a larger block (e.g., a /24 block):

- Bits borrowed for subnetting s = 25 - 24 (original block) = 1
- Total Subnets = $21 = 2$

The same process applies to other subnet masks, adjusting the number of host bits (h) and the number of borrowed bits (s) accordingly:

- /26 Subnet Mask:
  - Network bits = 26, Host bits h = 6
  - Usable Hosts = $26-2 = 62$
  - Assuming subnetting within a /24, s = 2, Total Subnets = $22 = 4$
- /27 Subnet Mask:
  - Network bits = 27, Host bits h = 5
  - Usable Hosts = $25-2 = 30$

- Assuming subnetting within a /24, s = 3, Total Subnets = 23 = 8

These calculations are essential for network engineers and administrators to efficiently plan and allocate IP addresses within a network, ensuring optimal utilisation and avoiding address exhaustion.

Example 1: Find the Class, network IP address, number of hosts (computers), and broadcast address of 9.1.5.31

Answer: Finding the Class to which the given IP address belongs to
The first octet has a value of 9 which is in the range of 0 to 127 so the given IP address belongs to Class A.

Finding the Network IP address
The default mask for class A as given in the table is 255.0.0.0

Perform the AND operation to get the network IP address
9.1.5.31 => 00001001.00000001.00000101.00011111
255.0.0.0 => 11111111.00000000.00000000.00000000
00001001.00000000.00000000.00000000 => 9.0.0.0

IP address = 9.1.5.31, Network address= 9.0.0.0
So, Network ID bits= 8 (first octet), Host ID bits = 24 (Last three octets)

The network IP address of the given IP address is 9.0.0.0
The number of hosts in each network is 224- 2
The broadcast IP address is 9.255.255.255

Steps to Find the Number of Computers Connected in the Given IP Address -:

1) To find the number of computers connected in the network first we need to identify the class of the IP address, there are 5 classes of IP addresses they are A, B, C, D, and E.
Each IPv4 address consists of 32 bits, divided into 4 octets, 1 octet = 8 bits. Look at the first octet to find the class of the given IP address. The range of each class is given in the following table.

**2)** Finding the network IP address involves determining the portion of an IP address that identifies the specific network to which a device belongs. This can be accomplished by using the subnet mask along with the device's IP address. Here's how you can find the network IP address:

- Understand IP Address and Subnet Mask: Every device on a network has an IP address and a corresponding subnet mask. The subnet mask helps in identifying how the IP address is divided into network and host parts.
- Binary Conversion: Convert both the IP address and the subnet mask into binary. An IP address is composed of four octets (e.g., 192.168.1.15), as is the subnet mask (e.g., 255.255.255.0).
- Perform a Binary AND Operation: Perform a bitwise AND operation between the binary form of the IP address and the subnet mask. This operation compares corresponding bits of the IP address and the subnet mask and applies the logical AND operation, which results in the network portion.
- Convert Back to Decimal: Convert the result of the AND operation back to decimal format to get the network address. This is the part of the IP address that identifies the network to which the device is connected.
- Verification: You can use various network tools or command-line utilities like ipconfig (on Windows) or ifconfig (on Unix/Linux) to display the IP address, subnet mask, and network address for verification.

3) Finding the number of hosts or number of computers connected to that network .

## Resources

1. https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html
2. https://www.geeksforgeeks.org/what-is-an-ip-address/
3. https://www.google.com/search?q=create+Subnets+in+natural+masks&rlz=1C5CHFA_enIN910IN910&oq=create+Subnets+in+natural+masks&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIJCAEQIRgKGKAB0gEHNTMwajBqN6gCCLACAfEFJv5Eo-XKNSVk&sourceid=chrome&ie=UTF-8
4. https://www.geeksforgeeks.org/computer-networks/how-to-calculate-number-of-host-in-a-subnet/