What is a 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 transmits 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.

Why Subnetting Necessary?

- Subnetting helps in organizing the network in an efficient way which helps in expanding the technology for large firms and companies.
- Subnetting is used for specific staffing structures to reduce traffic and maintain order and efficiency.
- Subnetting divides domains of the broadcast so that traffic is routed efficiently, which helps in improving network performance.
- Subnetting is used to increase network security.

Different Parts of IP Address

An IP address is made up of different parts, each serving a specific purpose in identifying a device on a network. In an IPv4 address, there are four parts, called “octets,” which are separated by dots (e.g., 192.168.1.1). Here’s what each part represents:

- **Network Portion**: The first few sections (octets) of an IP address identify the network that the device belongs to. This part of the IP address is common among all devices on the same network, allowing them to communicate with each other and share resources.

- **Host Portion**: The remaining sections of the IP address specify the individual device, or “host,” within that network. This part makes each device unique within the network, allowing the router to distinguish between different devices.

The 32-bit IP address is divided into sub-classes. These are given below:

- **Class A:** The network ID is 8 bits long and the host ID is 24 bits long.
- **Class B:** The network ID is 16 bits long and the host ID is 16 bits long.
- **Class C:** The network ID is 24 bits long and the host ID is 8 bits long.

For more details, refer to Classfull IP Addressing.

How Does Subnetting Work?

The working of subnets starts in such a way that firstly it divides the subnets into smaller subnets. For communicating between subnets, routers are used. Each subnet allows its linked devices to communicate with each other. Subnetting for a network should be done in such a way that it does not affect the network bits.

In class C the first 3 octets are network bits so it remains as it is.

- **For Subnet-1:** The first bit which is chosen from the host id part is zero and the range will be from (193.1.2.00000000 till you get all 1's in the host ID part i.e, 193.1.2.01111111) except for the first bit which is chosen zero for subnet id part.

Thus, the range of subnet 1 is: **193.1.2.0 to 193.1.2.127**

```
Subnet id of Subnet-1 is : 193.1.2.0
The direct Broadcast id of Subnet-1 is: 193.1.2.127
The total number of hosts possible is: 126 (Out of 128,
2 id's are used for Subnet id & Direct Broadcast id)
The subnet mask of Subnet- 1 is: 255.255.255.128
```

- **For Subnet-2:** The first bit chosen from the host id part is one and the range will be from (193.1.2.100000000 till you get all 1's in the host ID part i.e, 193.1.2.11111111).

Thus, the range of subnet-2 is: **193.1.2.128 to 193.1.2.255**

```
Subnet id of Subnet-2 is : 193.1.2.128
The direct Broadcast id of Subnet-2 is: 193.1.2.255
The total number of hosts possible is: 126 (Out of 128,
2 id's are used for Subnet id &  Direct Broadcast id)
The subnet mask of Subnet- 2 is: 255.255.255.128
The best way to find out the subnet mask of a subnet
is to set the fixed bit of host-id to 1 and the rest to 0.
```

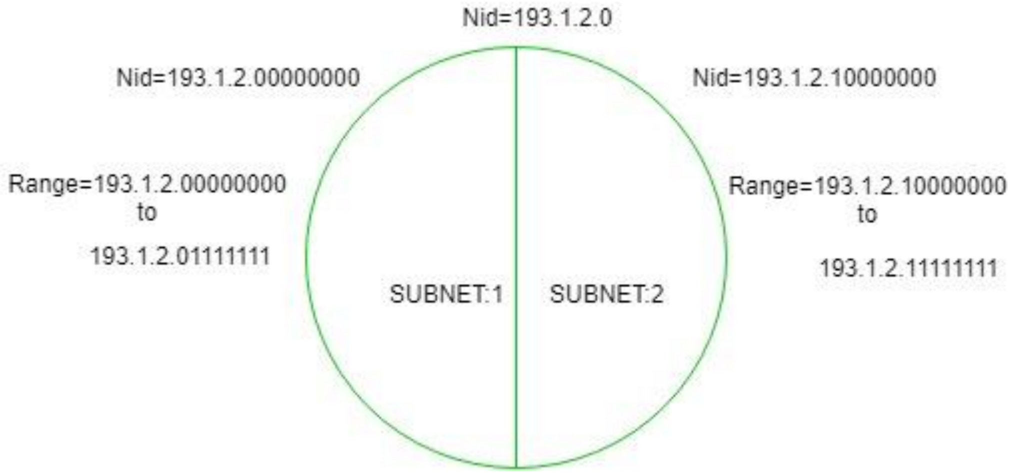
Finally, after using the subnetting the total number of usable hosts is reduced from 254 to 252.

Note:

1. To divide a network into four (2^2) parts you need to choose two bits from the host id part for each subnet i.e, (00, 01, 10, 11).
2. To divide a network into eight (2^3) parts you need to choose three bits from the host id part for each subnet i.e, (000, 001, 010, 011, 100, 101, 110, 111) and so on.

3. We can say that if the total number of subnets in a network increases the total number of usable hosts decreases.

The network can be divided into two parts: To divide a network into two parts, you need to choose one bit for each Subnet from the host ID part.



In the above diagram, there are two Subnets.

Note: It is a class C IP so, there are 24 bits in the network id part and 8 bits in the host id part.

Example 1: An organization is assigned a class C network address of 201.35.2.0. It uses a netmask of 255.255.255.192 to divide this into sub-networks. Which of the following is/are valid host IP addresses?

1. 201.35.2.129
2. 201.35.2.191
3. 201.35.2.255
4. Both (A) and (C)

Solution:

```
Converting the last octet of the
netmask into the binary form: 255.255.255.11000000
Converting the last octet of option 1
 into the binary form: 201.35.2.10000001
Converting the last octet of option 2
into the binary form: 201.35.2.10111111
Converting the last octet of option 3
into the binary form: 201.35.2.11111111
```

From the above, we see that Options 2 and 3 are not valid host IP addresses (as they are broadcast addresses of a subnetwork), and **OPTION 1** is not a broadcast address and it can be assigned to a host IP.

Example 2: An organization has a class C network address of 201.32.64.0. It uses a subnet mask of 255.255.255.248. Which of the following is NOT a valid broadcast address for any subnetworks?

1. 201.32.64.135
2. 201.32.64.240
3. 201.32.64.207
4. 201.32.64.231

Solution:

```
Converting the last octet of the netmask
 into the binary form: 255.255.255.11111000
Converting the last octet of option 1
into the binary form: 201.32.64.10000111
Converting the last octet of option 2
into the binary form: 201.32.64.11110000
Converting the last octet of option 3
into the binary form: 201.32.64.11001111
Converting the last octet of option 4
into the binary form: 201.32.64.11100111
```

From the above, we can see that in OPTION 1, 3, and 4, all the host bits are 1 and give the valid broadcast address of subnetworks.

and **OPTION 2,** the last three bits of the Host address are not 1 therefore it’s not a valid broadcast address.

What is a Subnet Mask?

A **subnet mask** is a 32-bit number used in IP addressing to separate the network portion of an IP address from the host portion. It helps computers and devices determine which part of an IP address refers to the network they are present, and which part refers to their specific location or address within that network.

How to Calculate a Subnet Mask from IP Address?

To calculate a **subnet mask** from an IP address first, we have to identify the type of IP address whether it belongs to a class full IP address or a Classless IP address. In this article, we discuss how to calculate subnet mask for class full IP address and Classless IP address.

Calculate Subnet Mask For Classful IP Address

As we know there are five classes in class full IP addressing Class A, Class B, Class C, Class D, and Class E. From these classes two classes that is D and E are reserved for special purposes remaining three classes that is A, B, and C are used to provide IP address to the client.

Ranges of The Classes

- **Class A**: 1.0.0.0 to 126.255.255.255
- **Class B**: 128.0.0.0 to 191.255.255.255
- **Class C**: 192.0.0.0 to 223.255.255.255

Default Subnet Mask

- **Class A**: 255.0.0.0
- **Class B**: 255.255.0.0
- **Class C**: 255.255.255.0

To identify the subnet mask of any given IP address first we have to find the class of the IP address and then the default subnet mask is the subnet mask of that IP address.

Example 1: Find subnet mask of the 19.35.21.31 IP address.

As we can see this IP address belongs to class A because 19 the first octate decimal value come in the range of 1 to 126 that is class A so the **subnet mask of this IP address is 255.0.0.0.**

Example 2: Find subnet mask of the 217.39.47.9 IP address.

As we can see this IP address belongs to class C because 217 the first octate decimal value come in the range of 192 to 223 that is class C so the **subnet mask of this IP address is 255.255.255.0.**

Calculate Subnet Mask For Classless IP Address

Class less IP addressing is also known as **CIDR (Classless Inter-Domain Routing)** notation, represents how many bits are used for the network portion of the IP address. The representation of the CIDR notation is a.b.c.d/n here n represent the number of bits used for network portion or NID these first n bit are 1 in the subnet mask of any IP address.

Example: Calculate the subnet mask of 192.168.1.0/24.

Here n=24 means 24 bits is 1 in the subnet mask so the subnet mask of this IP address is 11111111.11111111.11111111.00000000 i.e 255.255.255.0.

Calculate a Custom Subnet Mask

If you want to divide your network into smaller subnets, you need to modify the subnet mask. This is done by borrowing bits from the host portion and adding them to the network portion.

- For instance, if you want to divide a Class C network into two subnets, you borrow one bit from the host part:
    - Default mask: `255.255.255.0` (24 bits, `/24`)
    - Subnet mask: `255.255.255.128` (25 bits, `/25`)

Calculate Subnet and Host Per Subnet

To calculate how many subnets and hosts per subnet are possible after subnetting, use the following formulas:

- **Number of Subnets**: 2^n, where n is the number of borrowed bits.
- **Hosts per Subnet**: 2^h-2 where h is the number of bits left for the host portion (subtracting 2 for network and broadcast addresses).

Example: Calculate the subnet mask of 192.168.1.0/26.

- **Subnet Mask**: 255.255.255.192 (26 bits for network, 6 bits for host)
- **Subnets**: $2^2=4$ subnets
- **Hosts per Subnet**: $2^6-2=62$ hosts per subnet

Network Address Translation (NAT) is a technique that allows private IP networks to access the internet and cloud by translating private IP addresses to public IP addresses:

NAT works by modifying the IP header of packets while they are being routed across a traffic routing device. For example, when a device on a private network sends data to a device on a public network, the router will replace the private IP address with its own public IP address before sending the data. When the destination device sends data back, the router will replace the public IP address with the original private IP address.