Roll. No. A016	Name: Varun Mahendra Khadayate
Class B.Tech CsBs	Batch: 1
Date of Experiment: 15-01-2022	Date of Submission: 15-01-2022

Aim

To study network IP

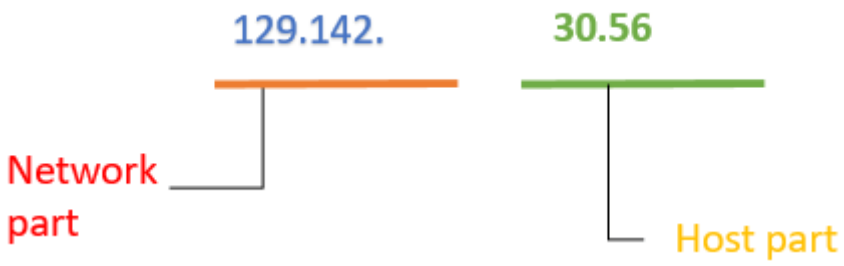
- Classification of IP address
- Sub netting
- Super netting

Classification of IP address

An IP (Internet Protocol) address is a numerical label assigned to the devices connected to a computer network that uses the IP for communication.

IP address act as an identifier for a specific machine on a particular network. It also helps you to develop a virtual connection between a destination and a source. The IP address is also called IP number or internet address. It helps you to specify the technical format of the addressing and packets scheme. Most networks combine TCP with IP.

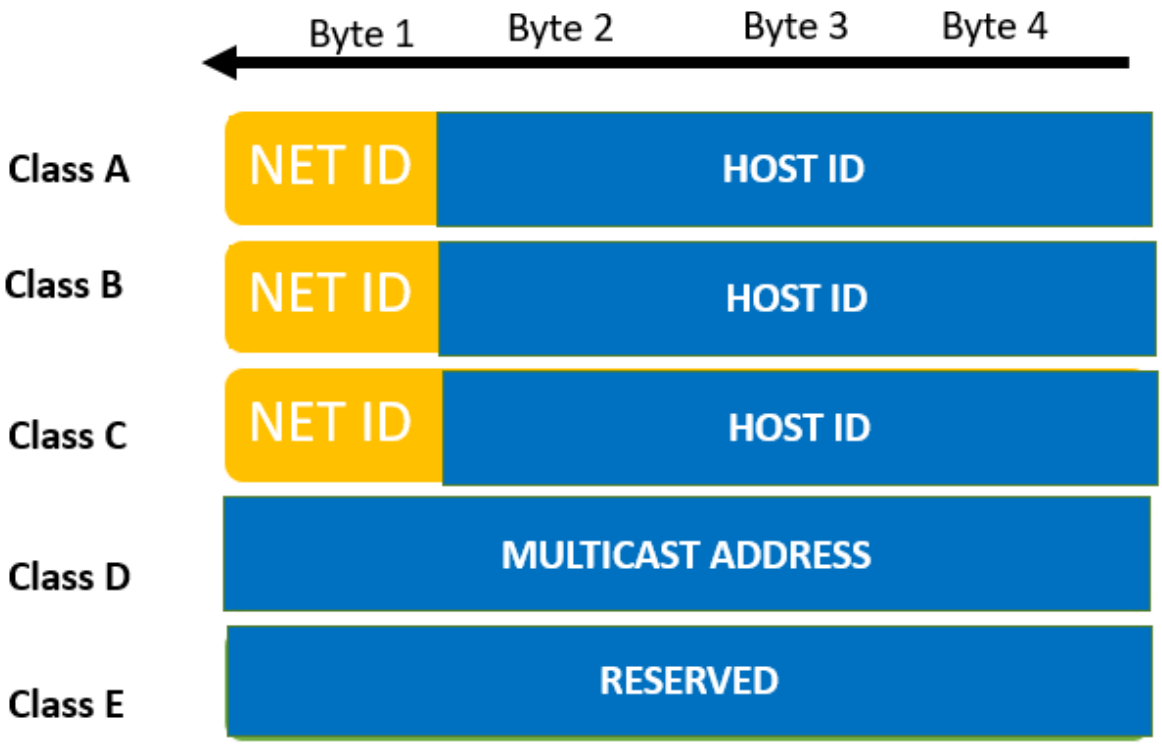
An IP address consists of four numbers, each number contains one to three digits, with a single dot (.) separates each number or set of digits.



Parts of IP address

IP Address is divided into two parts:

- **Prefix**: The prefix part of IP address identifies the physical network to which the computer is attached. . Prefix is also known as a network address.
- **Suffix**: The suffix part identifies the individual computer on the network. The suffix is also called the host address.



Types of IP4 Classes

IP Header Classes:

Class	Address Range	Subnet masking	Example IP	Leading bits	Max number of networks	Application
IP Class A	1 to 126	255.0.0.0	1.1.1.1	8	128	Used for large number of hosts.
IP Class B	128 to 191	255.255.0.0	128.1.1.1	16	16384	Used for medium size network.
IP Class C	192 to 223	255.255.255.0	192.1.11.	24	2097157	Used for local area network.
IP Class D	224 to 239	NA	NA	NA	NA	Reserve for multi-tasking.
IP Class E	240 to 254	NA	NA	NA	NA	This class is reserved for research and Development Purposes.

Class A Network

This IP address class is used when there are a large number of hosts. In a Class A type of network, the first 8 bits (also called the first octet) identify the network, and the remaining have 24 bits for the host into that network.

An example of a Class A address is:

102.168.212.226. Here, “102” helps you identify the network and 168.212.226 identify the host.

Class A addresses 127.0.0.0 to 127.255.255.255 cannot be used and is reserved for loopback and diagnostic functions.

Class B Network

In a B class IP address, the binary addresses start with 10. In this IP address, the class decimal number that can be between 128 to 191. The number 127 is reserved for loopback, which is used for internal testing on the local machine. The first 16 bits (known as two octets) help you identify the network. The other remaining 16 bits indicate the host within the network.

An example of Class B IP address is:

168.212.226.204, where *168 212* identifies the network and *226.204* helps you identify the Hut network host.

Class C Network

Class C is a type of IP address that is used for the small network. In this class, three octets are used to indent the network. This IP ranges between 192 to 223.

In this type of network addressing method, the first two bits are set to be 1, and the third bit is set to 0, which makes the first 24 bits of the address them and the remaining bit as the host address. Mostly local area network used Class C IP address to connect with the network.

Example for a Class C IP address:

192.168.178.1

Class D Network

Class D addresses are only used for multicasting applications. Class D is never used for regular networking operations. This class addresses the first three bits set to “1” and their fourth bit set to use for “0”. Class D addresses are 32-bit network addresses. All the values within the range are used to identify multicast groups uniquely.

Therefore, there is no requirement to extract the host address from the IP address, so Class D does not have any subnet mask.

Example for a Class D IP address:

227.21.6.173

Class E Network

Class E IP address is defined by including the starting four network address bits as 1, which allows you two to incorporate addresses from 240.0.0.0 to 255.255.255.255. However, E class is reserved, and its usage is never defined. Therefore, many network implementations discard these addresses as undefined or illegal.

Example for a Class E IP address:

243.164.89.28

Limitations of classful IP addressing

Here are the drawbacks/ cons of the classful IP addressing method:

- Risk of running out of address space soon
- Class boundaries did not encourage efficient allocation of address space

Rules for assigning Network ID:

The network ID will be assigned based on the below-given rules:

- The network ID cannot start with 127 because 127 belongs to class A address and is reserved for internal loopback functions.
- All bits of network ID set to 1 are reserved for use as an IP broadcast address and cannot be used.
- All bits of network ID are set to 0. They are used to denote a particular host on the local network and should not be routed.

Sub netting

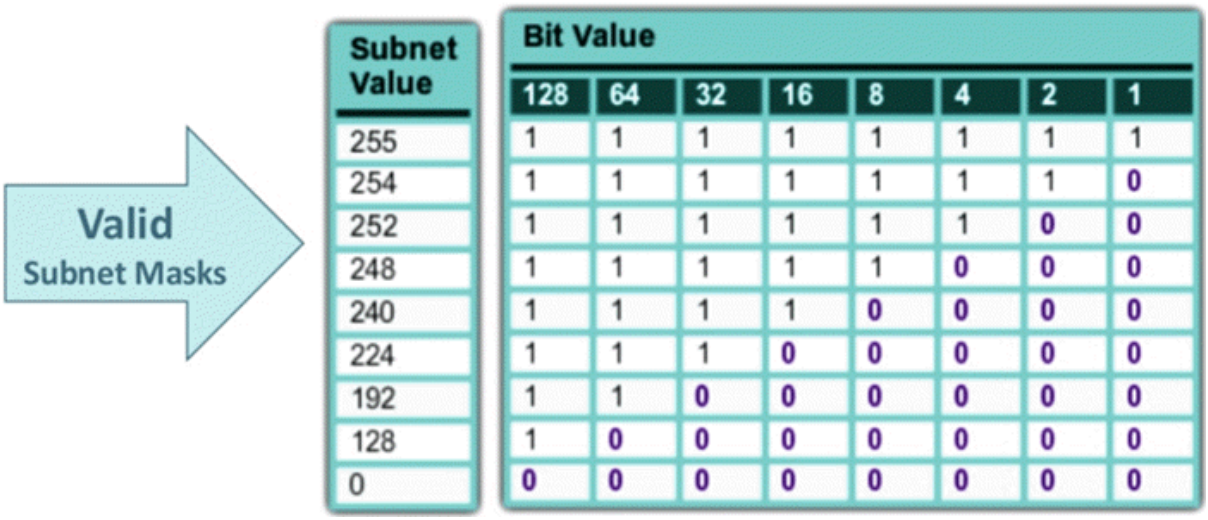
Subnetting is the practice of dividing a network into two or smaller networks. It increases routing efficiency, which helps to enhance the security of the network and reduces the size of the broadcast domain.

IP Subnetting designates high-order bits from the host as part of the network prefix. This method divides a network into smaller subnets.
It also helps you to reduce the size of the routing tables, which is stored in routers. This method also helps you to extend the existing IP address base & restructures the IP address.

What is Subnet Mask?

A subnet mask is a 32 bits address used to distinguish between a network address and a host address in IP address. A subnet mask identifies which part of an IP address is the network address and the host address. They are not shown

inside the data packets traversing the Internet. They carry the destination IP address, which a router will match with a subnet.



represent network 0 represent hosts

Two types of subnet masks are:

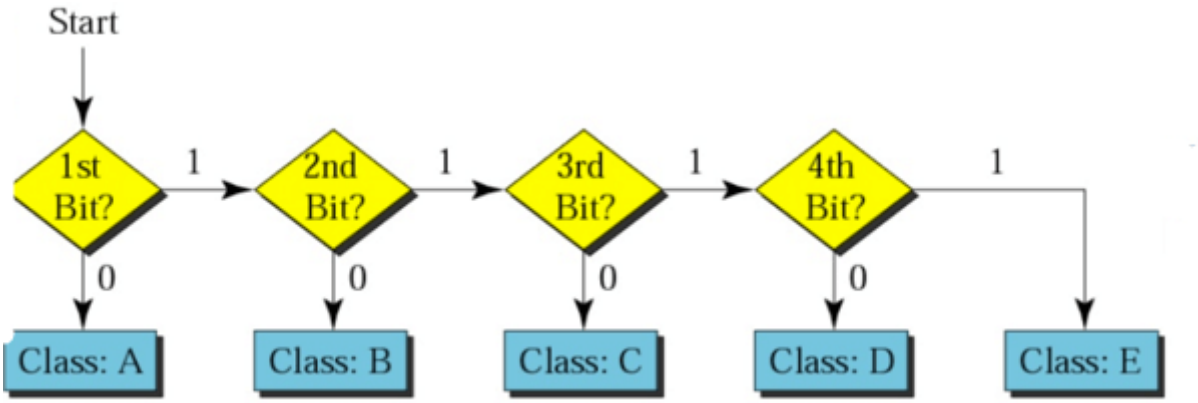
- The default Subnet Mask is the number of bits which is reserved by the address class. Using this default mask will accommodate a single network subnet in the relative class.
- A Custom Subnet Mask can be defined by an administrator to accommodate many Network

How to Use a Subnet Mask?

The subnet mask is used by the router to cover up the network address. It shows which bits are used to identify the subnet.

Every network has its own unique address, like here, class B network has network address 172.20.0.0, which has all zeroes in the host portion of the address.

Example IP address: 11000001. Here 1st and 2nd bits are 1, and the 3rd bit is 0; hence, it is class C.



How to identify which class the IP address belongs to

Above example shows how IP addresses should be deconstructed, which makes it simple for Internet routers to find the right Network to route data into. However, in a Class A network there could be millions of connected devices, and it could take some time for the router to find the right device.

Methods of Subnet Masking

We can subnet the masking process in two ways: Straight or Short-cut.

1) Straight

You should use the binary notation method for both the address and the mask and then apply the AND operation to get the block address.

2) Short-Cut Method

- In case the byte in the mask is 255, you need to copy the byte in the destination address.
- When the byte in the mask is 0, then you need to replace the byte in the address with 0.
- When the byte in the mask is neither 255 nor 0, then you should write the mask and the address in binary and use the AND operation.
- In case if the extracted network address matches the local network ID, and the destination is located on the local Network. However, if they do not match, the message must be routed outside the local Network.

Class	Default subnet mask	No. of networks	No. of host per network
A	255.0.0.0	256	16,777,214
B	255.255.0.0	65,536	65,534
C	255.255.255.0	16,77,216	126

Important formulas to determine the subnets

Use the 2s – 2 formula and do not use the zero and broadcast ranges if:

- You can use classful routing method.
- RIP version 1 is used
- The no IP subnet-zero command is configured on your router.

Use the 2s formula and use the zero and broadcast ranges if:

- You can use a classless routing or VLM method.
- RIP version 2. EIGRP. or OSPF is used
- The IP subnet-zero command is configured on your router.

Super netting

Super netting is the opposite of **Subnetting**. In subnetting, a single big network is divided into multiple smaller subnetworks. In Super netting, multiple networks are combined into a bigger network termed as a Super network or super net.
Super netting is mainly used in Route Summarization, where routes to multiple networks with similar network prefixes are combined into a single routing entry, with the routing entry pointing to a Super network, encompassing all the networks. This in turn significantly reduces the size of routing tables and the size of routing updates exchanged by routing protocols.

More specifically,

- When multiple networks are combined to form a bigger network, it is termed as super-netting
- Super netting is used in route aggregation to reduce the size of routing tables and routing table updates

There are some points which should be kept in mind while super netting:

1. All the IP address should be contiguous.
2. Size of all the small networks should be equal and must be in form of 2n.
3. First IP address should be exactly divisible by whole size of supernet.

Example – Suppose 4 small networks of class C:

```
200.1.0.0,
200.1.1.0,
200.1.2.0,
200.1.3.0
```

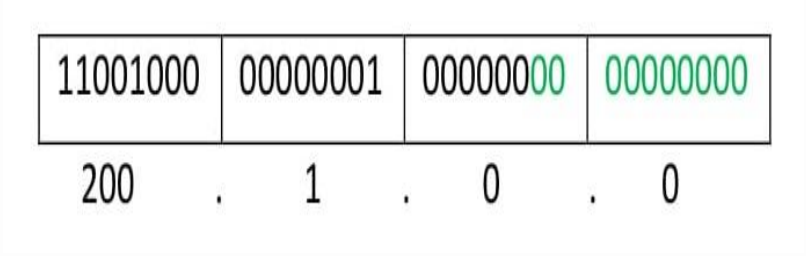
Build a bigger network which have a single Network Id.

Explanation – Before Super netting routing table will be look like as:

Network Id	Subnet Mask	Interface
200.1.0.0	255.255.255.0	A
200.1.1.0	255.255.255.0	B
200.1.2.0	255.255.255.0	C
200.1.3.0	255.255.255.0	D

First, let's check whether three condition are satisfied or not:

1. **Contiguous:** You can easily see that all networks are contiguous all having size 256 hosts.
   Range of first Network from 200.1.0.0 to 200.1.0.255. If you add 1 in last IP address of first network that is 200.1.0.255 + 0.0.0.1, you will get the next network id that is 200.1.1.0. Similarly, check that all networks are contiguous.
2. **Equal size of all networks:** As all networks are of class C, so all of the have a size of 256 which in turn equal to 2^8.
3. **First IP address exactly divisible by total size:** When a binary number is divided by 2^n then last n bits are the remainder. Hence to prove that first IP address is exactly divisible by while size of super net Network. You can check that if last n v=bits are 0 or not.
   In given example first IP is 200.1.0.0 and whole size of super net is $4*2^8 = 2^{10}$. If last 10 bits of first IP address are zero, then IP will be divisible.



   Last 10 bits of first IP address are zero (highlighted by green color). So 3rd condition is also satisfied.

Therefore, you can join all these 4 networks and can make a super net. New super net Id will be 200.1.0.0.

Advantages of Super netting –

1. Control and reduce network traffic
2. Helpful to solve the problem of lacking IP addresses
3. Minimizes the routing table

Disadvantages of Super netting –

- It cannot cover different area of network when combined
- All the networks should be in same class and all IP should be contiguous