UNIT 4 IP PROTOCOL

What is IPv4?

IP stands for **Internet Protocol** and **v4** stands for **Version Four** (IPv4). IPv4 was the primary version brought into action for production within the ARPANET in 1983.
IP version four addresses are 32-bit integers which will be expressed in decimal notation. Example- 192.0.2.126 could be an IPv4 address.

- **Parts of IPv4**

  - **Networkpart:**
    The network part indicates the distinctive variety that's appointed to the network. The network part conjointly identifies the category of the network that's assigned.
  - **Host Part:**
    The host part uniquely identifies the machine on your network. This part of the IPv4 address is assigned to every host.
    For each host on the network, the network part is the same, however, the host half must vary.
  - **Subnet number:**
    This is the nonobligatory part of IPv4. Local networks that have massive numbers of hosts are divided into subnets and subnet numbers are appointed to that.

- **Characteristics of IPv4**
  - IPv4 could be a 32-Bit IP Address.
  - IPv4 could be a numeric address, and its bits are separated by a dot.
  - The number of header fields is twelve and the length of the header field is twenty.
  - It has Unicast, broadcast, and multicast style of addresses.
  - IPv4 supports VLSM (Virtual Length Subnet Mask).
  - IPv4 uses the Post Address Resolution Protocol to map to the MAC address.
  - RIP may be a routing protocol supported by the routed daemon.
  - Networks ought to be designed either manually or with DHCP.
  - Packet fragmentation permits from routers and causing host.
- **Advantages of IPv4**
  - IPv4 security permits encryption to keep up privacy and security.
  - IPV4 network allocation is significant and presently has quite 85000 practical routers.
  - It becomes easy to attach multiple devices across an outsized network while not NAT.
  - This is a model of communication so provides quality service also as economical knowledge transfer.
  - IPV4 addresses are redefined and permit flawless encoding.
  - Routing is a lot of scalable and economical as a result of addressing is collective more effectively.
  - Data communication across the network becomes a lot of specific in multicast organizations.

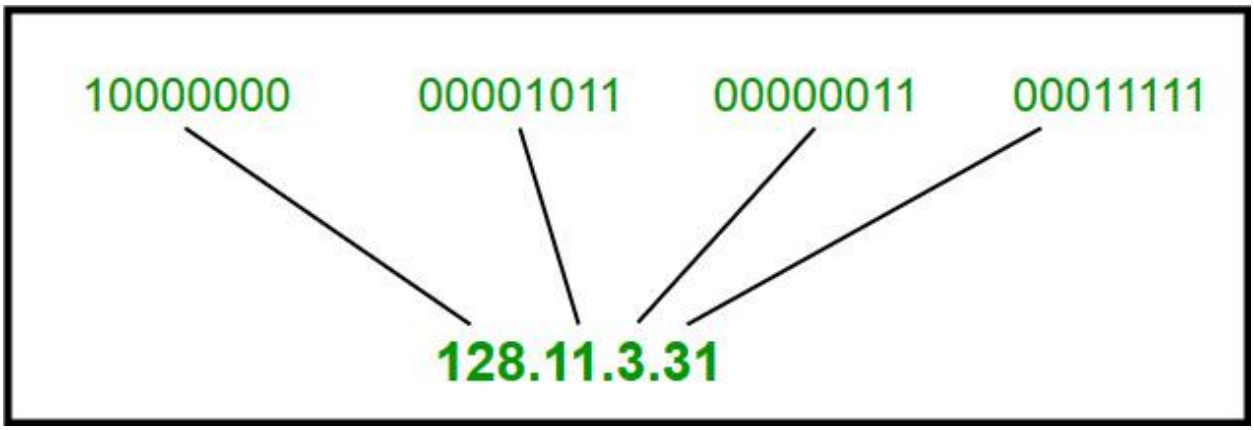
❖ **Limitations of IPv4**

- IP relies on network layer addresses to identify end-points on network, and each network has a unique IP address.
- The world's supply of unique IP addresses is dwindling, and they might eventually run out theoretically.
- If there are multiple host, we need IP addresses of next class.
- Complex host and routing configuration, non-hierarchical addressing, difficult to re-numbering addresses, large routing tables, non-trivial implementations in providing security, QoS (Quality of Service), mobility and multi-homing, multicasting etc. are the big limitation of IPv4 so that's why IPv6 came into the picture.

Introduction of Classful IP Addressing

An IP address is an address having information about how to reach a specific host, especially outside the LAN. An IP address is a 32-bit unique address having an address space of 232. Generally, there are two notations in which the IP address is written, dotted decimal notation and hexadecimal notation.

Dotted Decimal Notation



Dotted Decimal Notation

Hexadecimal Notation

Some points to be noted about dotted decimal notation:

1. The value of any segment (byte) is between 0 and 255 (both included).
2. No zeroes are preceding the value in any segment (054 is wrong, 54 is correct).

❖ Classful Addressing

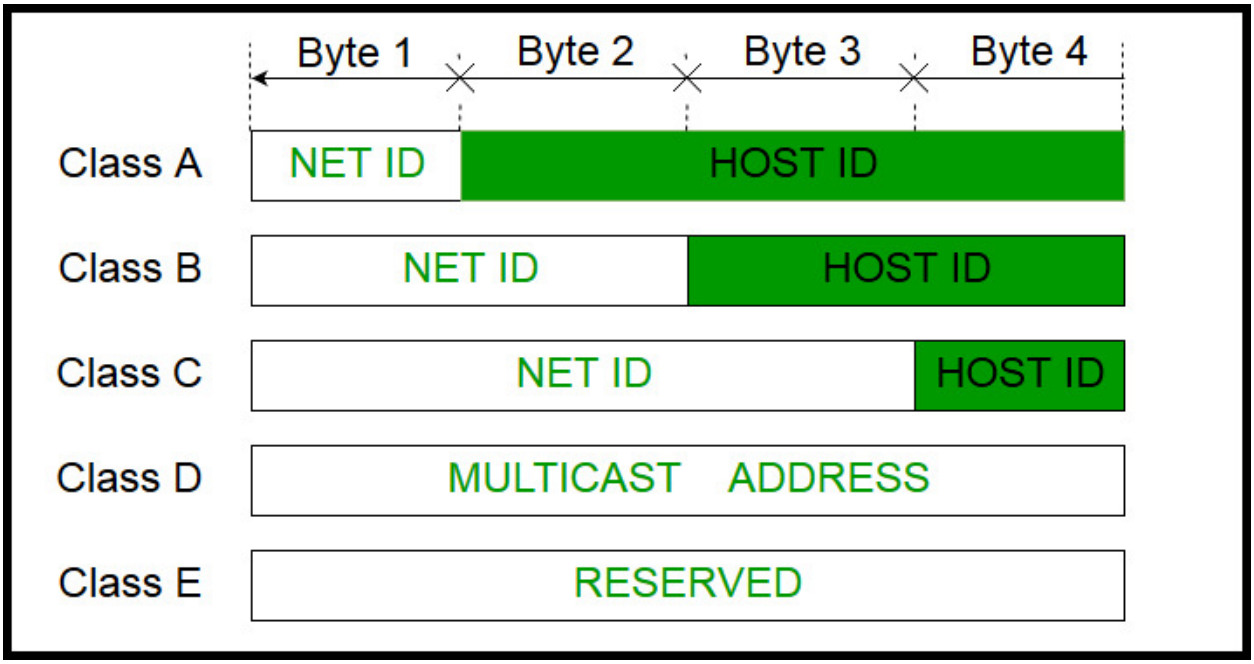
The 32-bit IP address is divided into five sub-classes. These are given below:

- Class A
- Class B
- Class C
- Class D
- Class E

Each of these classes has a valid range of IP addresses. Classes D and E are reserved for multicast and experimental purposes respectively. The order of bits in the first octet determines the classes of the IP address. The IPv4 address is divided into two parts:

- Network ID
- Host ID

The class of IP address is used to determine the bits used for network ID and host ID and the number of total networks and hosts possible in that particular class. Each ISP or network administrator assigns an IP address to each device that is connected to its network.



Classful Addressing

Class A

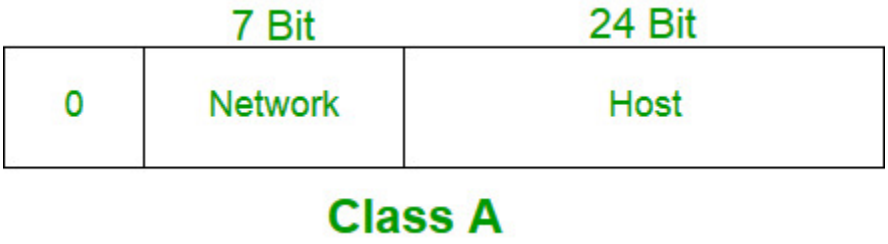
IP addresses belonging to class A are assigned to the networks that contain a large number of hosts.

- The network ID is 8 bits long.
- The host ID is 24 bits long.

The higher-order bit of the first octet in class A is always set to 0. The remaining 7 bits in the first octet are used to determine network ID. The 24 bits of host ID are used to determine the host in any network. The default subnet mask for Class A is 255.x.x.x. Therefore, class A has a total of:

- 2^24 – 2 = 16,777,214 host ID

IP addresses belonging to class A ranges from 0.0.0.0 – 127.255.255.255.



Class B

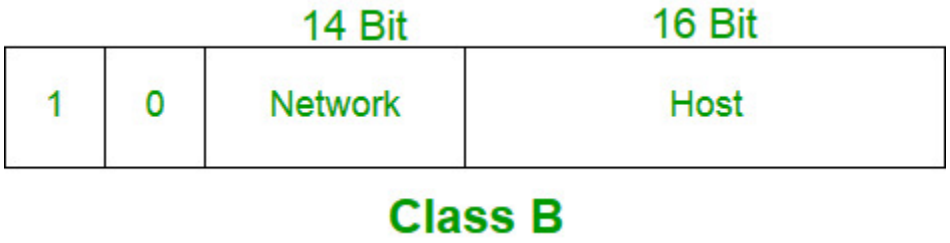
IP address belonging to class B is assigned to networks that range from medium-sized to large-sized networks.

- The network ID is 16 bits long.
- The host ID is 16 bits long.

The higher-order bits of the first octet of IP addresses of class B are always set to 10. The remaining 14 bits are used to determine the network ID. The 16 bits of host ID are used to determine the host in any network. The default subnet mask for class B is 255.255.x.x. Class B has a total of:

- 2^14 = 16384 network address
- 2^16 – 2 = 65534 host address

IP addresses belonging to class B ranges from 128.0.0.0 – 191.255.255.255.



Class C

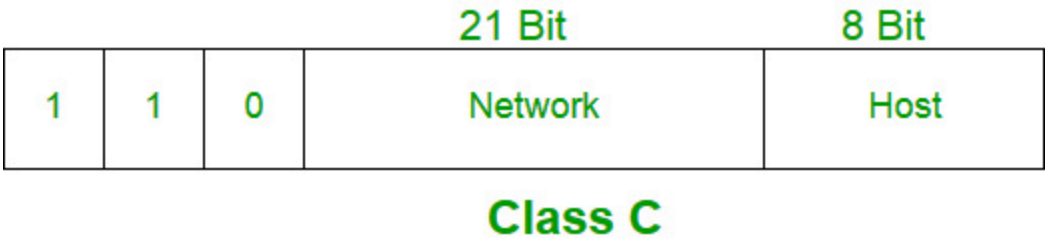
IP addresses belonging to class C are assigned to small-sized networks.

- The network ID is 24 bits long.
- The host ID is 8 bits long.

The higher-order bits of the first octet of IP addresses of class C is always set to 110. The remaining 21 bits are used to determine the network ID. The 8 bits of host ID are used to determine the host in any network. The default subnet mask for class C is 255.255.255.x. Class C has a total of:

- 2^21 = 2097152 network address
- 2^8 – 2 = 254 host address

IP addresses belonging to class C range from 192.0.0.0 – 223.255.255.255.

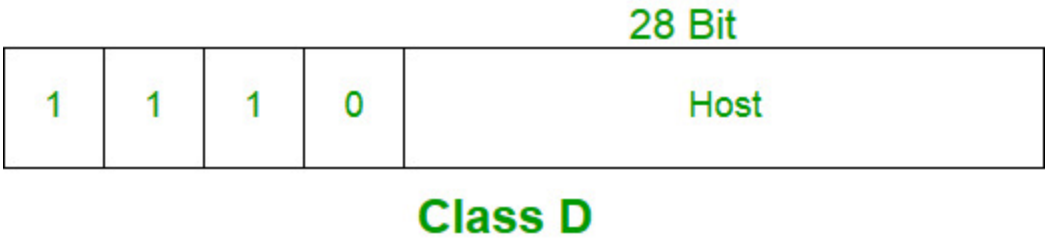


Class C

Class D

IP address belonging to class D is reserved for multi-casting. The higher-order bits of the first octet of IP addresses belonging to class D is always set to 1110. The remaining bits are for the address that interested hosts recognize.

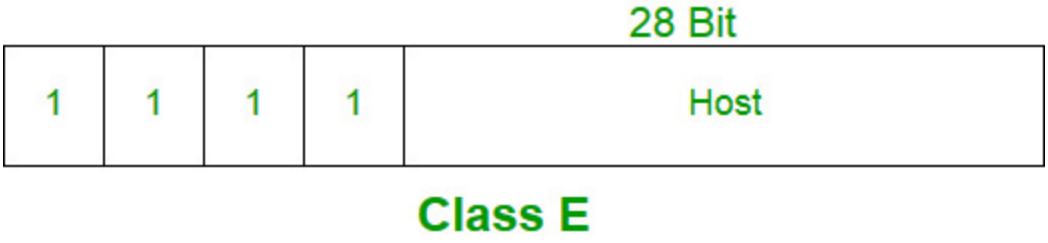
Class D does not possess any subnet mask. IP addresses belonging to class D range from 224.0.0.0 – 239.255.255.255.



Class D

Class E

IP addresses belonging to class E are reserved for experimental and research purposes. IP addresses of class E range from 240.0.0.0 – 255.255.255.254. This class doesn't have any subnet mask. The higher-order bits of the first octet of class E are always set to 1111.



Class E

Range of Special IP Addresses

169.254.0.0 – 169.254.0.16 : Link-local addresses
127.0.0.0 – 127.255.255.255 : Loop-back addresses
0.0.0.0 – 0.0.0.8: used to communicate within the current network.

Rules for Assigning Host ID

Host IDs are used to identify a host within a network. The host ID is assigned based on the following rules:

- Within any network, the host ID must be unique to that network.
- A host ID in which all bits are set to 0 cannot be assigned because this host ID is used to represent the network ID of the IP address.
- Host ID in which all bits are set to 1 cannot be assigned because this host ID is reserved as a broadcast address to send packets to all the hosts present on that particular network.

Rules for Assigning Network ID

Hosts that are located on the same physical network are identified by the network ID, as all host on the same physical network is assigned the same network ID. The network ID is assigned based on the following rules:

- The network ID cannot start with 127 because 127 belongs to the 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 therefore, cannot be used.
- All bits of network ID set to 0 are used to denote a specific host on the local network and are not routed and therefore, aren't used.

Summary of Classful Addressing

CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

In the above table No. of networks for class A should be 127. (Network ID with all 0 s is not considered)

Problems with Classful Addressing

The problem with this classful addressing method is that millions of class A addresses are wasted, many of the class B addresses are wasted, whereas, the number of addresses available in class C is so small that it cannot cater to the needs of organizations. Class D addresses are used for multicast routing and are therefore available as a single block only. Class E addresses are reserved.

Since there are these problems, Classful networking was replaced by Classless Inter-Domain Routing (CIDR) in 1993. We will be discussing Classless addressing in the next post.

- The network ID is 24 bits long.
- The host ID is 8 bits long.
- 2^21 = 2097152 network address
- 2^8 – 2 = 254 host address
- Within any network, the host ID must be unique to that network.
- Host ID in which all bits are set to 0 cannot be assigned because this host ID is used to represent the network ID of the IP address.
- Host ID in which all bits are set to 1 cannot be assigned because this host ID is reserved as a broadcast address to send packets to all the hosts present on that particular network.

- The network ID cannot start with 127 because 127 belongs to the 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 therefore, cannot be used.
- All bits of network ID set to 0 are used to denote a specific host on the local network and are not routed and therefore, aren't used

❖ Classless Addressing in IP Addressing

The Network address identifies a network on the internet. Using this, we can find a range of addresses in the network and total possible number of hosts in the network.
Mask is a 32-bit binary number that gives the network address in the address block when AND operation is bitwise applied on the mask and any IP address of the block.
The default masks in different classes are :

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

Subnetting

Dividing a large block of addresses into several contiguous sub-blocks and assigning these sub-blocks to different smaller networks is called subnetting. It is a practice that is widely used when classless addressing is done.
A subnet or subnetwork is a network inside a network. Subnets make networks more efficient. Through subnetting, network traffic can travel a shorter distance without passing through unnecessary routers to reach its destination.

Classless Addressing

To reduce the wastage of IP addresses in a block, we use sub-netting. What we do is that we use host id bits as net id bits of a classful IP address. We give the IP address and define the number of bits for mask along with it (usually followed by a '/' symbol), like, 192.168.1.1/28. Here, subnet mask is found by putting the given number of bits out of 32 as 1, like, in the given address, we need to put 28 out of 32 bits as 1 and the rest as 0, and so, the subnet mask would be 255.255.255.240. A classless addressing system or classless interdomain routing (CIDR or super netting) is the way to combine two or more class C networks to create a/23 or a /22 super net. A classless addressing system or classless interdomain routing (CIDR) is an improved IP addressing system. In a classless addressing system the block of IP address is assigned dynamically based on specific rules.

Some Values Calculated in Subnetting:

1. **Number of subnets** : 2(Given bits for mask – No. of bits in default mask)
2. **Subnet address :** AND result of subnet mask and the given IP address
3. **Broadcast address :** By putting the host bits as 1 and retaining the network bits as in the IP address
4. **Number of hosts per subnet :** 2(32 – Given bits for mask) – 2
5. **First Host ID :** Subnet address + 1 (adding one to the binary representation of the subnet address)
6. **Last Host ID :** Subnet address + Number of Hosts

What is a Subnet Mask?

Setting all 0s for the host bits and all 1s for the network bits results in a 32-bit value known as a subnet mask. The IP address is divided into the host address and network address in this manner by the subnet mask. “255” is always the address assigned to the broadcast address, while “0” is always the address assigned to the network address. The subnet mask cannot be assigned to the host because it is set aside for a specific purpose.

Function of Subnet Mask

A 32-bit address that distinguishes the network address from the host address makes up the subnet mask. This indicates which part of the IP address belongs in the host section and which part belongs in the network section. The number of hosts that can be on the subnet depends on the values of the subnet mask. This comprises bits that are initialized to 1 for the network and 0 for the host. Routers and switches use it internally to send packets to the destination node along the associated local network connection.

Suppose we have a Class A network which means we have 16 million hosts in a network. The task we have to do is

1. Maintenance of such a huge network
2. Security for the network – For example, we have 4 departments in a company and all of the 4 departments need not access the whole network.

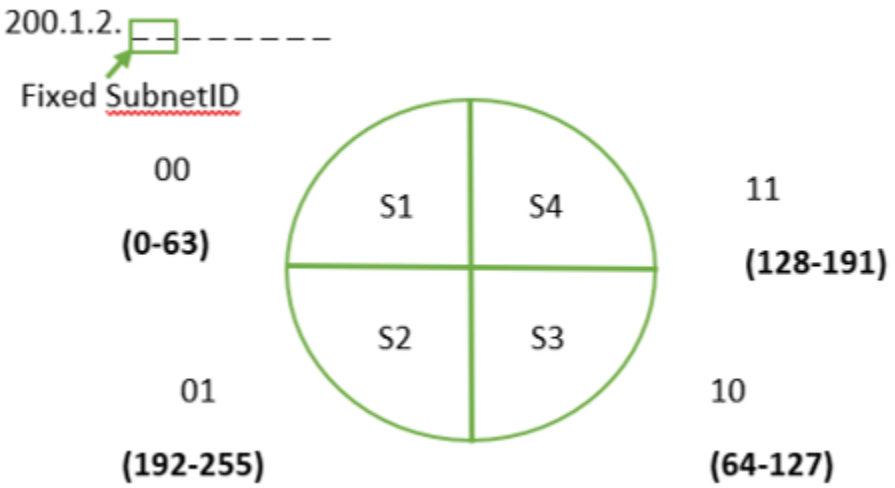
For this, we need Subnetting i.e., dividing a huge network into smaller networks. Now every department will have their network. In the case of addressing without subnetting, the process of reaching an address is done by 3 steps –

- Identification of the network
- Identification of the host
- Identification of the process

In case of addressing with subnetting, the process of reaching an address is done by 4 steps –

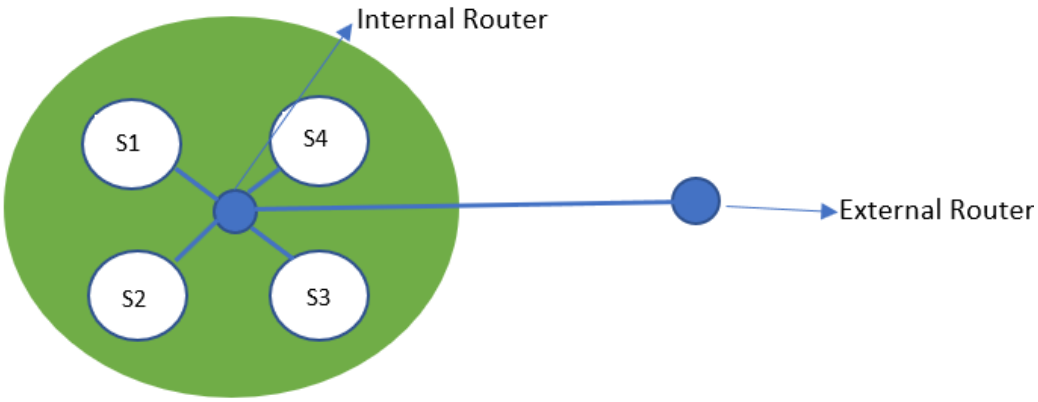
1. Identification of the network
2. Identification of the subnet
3. Identification of the host
4. Identification of the process

Suppose we have a Class C network and we want to divide it into 4 subnets. To divide we need to choose 2 bits from the host part.



As the first and last IP addresses are reserved for **network ID** and **directed broadcast address** in every subnet, we have to reserve 8 IP addresses in this case.

Actual View in reality:



Network Classes

The company in charge of overseeing the Internet, InterNIC, assigns IP addresses. There are classes for these IP addresses. Classes A, B, and C are the most prevalent ones among them. Although they exist, end users do not use classes D or E. The default subnet mask varies for each address class. An IP address's first octet can be used to determine its class. The ranges of Class A, B, and C Internet addresses are listed below, along with a sample address for each:

- Class A networks have 0-127 as their first octet and utilise 255.0.0.0 as their default subnet mask. 10.52.36.11 is classified as a class A address. 10, its initial octet, falls between 1 and 126, inclusive.
- Class B networks have 128–191 as their first octet and 255.255.0.0 as their default subnet mask. Address 172.16.52.63 belongs to the class B address set. Its initial octet is 172, spanning from 128 to 191, inclusive.
- Class C networks have 192-223 as their first octet and utilise 255.255.255.0 as their default subnet mask.

A packet is received which has destination address -200.1.2.20 . Then how the router will identify that which subnet it belongs to . It'll be done using *Subnet Mask*

A **subnet mask** is a 32-bit number which is used to identify the subnet of an IP address. The subnet mask is combination of 1's and 0's. 1's represents network and subnet ID while 0's represents the host ID. For this case, subnet mask is,

```
11111111.11111111.11111111.11000000
or
255.255.255.192
```

So in order to get the network which the destination address belongs to we have to **bitwise &** with subnet mask.

```
    11111111.11111111.11111111.11000000
&&  11001000.00000001.00000010.00010100
-----------------------------------------------------
    11001000.00000001.00000010.00000000
```

The address belongs to,

11001000.00000001.00000010.00000000
or
200.1.2.0

The internal router will forward the packet to the network through an interface . The interface will be identified by the routing table residing in the router.

Routing table

If the network id doesn't matches with any then the packet will be sent to **default entry.**
Default entry has network id as 0.0.0.0.

Network ID	Subnet mask	Interface
200.1.2.0	255.255.255.192	A
200.1.2.64	255.255.255.192	B
200.1.2.128	255.255.255.192	C
200.1.2.192	255.255.255.192	D

In some cases the network id may match with two entries in the routing table, so here the interface having the longest subnet mask **(more 1's)** is selected.

Advantages of Subnetting

- It does this by sending out fewer broadcasts, which lowers network load.
- It assists in getting around restrictions in a local area network (LAN), like the maximum number of permitted hosts.
- Without needing to access the entire network, it enables users to join to a work network from their residences.
- It keeps one network safe from another's infiltration. For instance, no other department within an organization should be able to view the code created by the Developer department.
- 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.
- If the network is tiny, maintenance is easy.

Disadvantages of Subnetting

- 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.
- Companies still assign address blocks in relation to classes, therefore it cannot alleviate the inefficiency.

What is IPv6?

- Internet Protocol version 6 (IPv6) is the newest version of the Internet Protocol (IP), Similar to IPv4. IPv6 was introduced to remediate the problems and limitations of IPv4. IPv6 is also referred to as IP next generation or IPng. IPv6 uses 128 bits to identify a host instead of IPv4's 32 bits. The 128 bits that IPv6 uses allows the address space up to 2 128 which equates to over 340 undecillion numbers of IP available addresses. The address space of IPv6 is a staggering number compared to ipv4s address space. The number of connected devices to the internet has long outgrown the addressing capacity of IPv4. The adoption of IPv6 has been slow from a technological standpoint. Most Internet Service Providers (ISP)

still use IPv4 so version four will still be around for some time. Despite computers supporting IPv6 from the Windows XP era.

❖ Pv4 vs IPv6

The common type of IP address (is known as IPv4, for "version 4"). Here's an example of what an IP address might look like:

25.59.209.224

An IPv4 address consists of four numbers, each of which contains one to three digits, with a single dot (.) separating each number or set of digits. This group of separated numbers creates the addresses that let you and everyone around the globe to send and retrieve data over our Internet connections. The IPv4 uses a 32-bit address scheme allowing to store 2^32 addresses which is more than 4 billion addresses. To date, it is considered the primary Internet Protocol and carries 94% of Internet traffic. Initially, it was assumed it would never run out of addresses but the present situation paves a new way to IPv6, let's see why? An IPv6 address consists of eight groups of four hexadecimal digits. Here's an example IPv6 address:

3001:0da8:75a3:0000:0000:8a2e:0370:7334

This new IP address version is being deployed to fulfil the need for more Internet addresses. With 128-bit address space, it allows 340 undecillion unique address space.

IPv6 support a theoretical maximum of 340, 282, 366, 920, 938, 463, 463, 374, 607, 431, 768, 211, 456. To keep it straightforward, we will never run out of IP addresses again.

The next iteration of the IP standard is known as Internet Protocol version 6 (IPv6). Although IPv4 and IPv6 will coexist for a while, IPv6 is meant to work in tandem with IPv4 before eventually taking its place. We need to implement IPv6 in order to proceed and keep bringing new gadgets and services to the Internet. We can only move forward with an innovative and open Internet if we implement it, which was created with the needs of a global commercial Internet in mind.

Types of IPv6 Address

Now that we know about what is IPv6 address let's take a look at its different types.

- **Unicast addresses :** Only one interface is specified by the unicast address. A packet moves from one host to the destination host when it is sent to a unicast address destination.
- **Multicast addresses** It represents a group of IP devices and can only be used as the destination of a datagram.
- **Anycast addresses** The multicast address and the anycast address are the same. The way the anycast address varies from other addresses is that it can deliver the same IP address to several servers or devices. Keep in mind that the hosts do not receive the IP address. Stated differently, multiple interfaces or a collection of interfaces are assigned an anycast address.

Advantages of IPv6

- **Faster Speeds:** IPv6 supports multicast rather than broadcast in IPv4.This feature allows bandwidth-intensive packet flows (like multimedia streams) to be sent to multiple destinations all at once.
- **Stronger Security:** IPSecurity, which provides confidentiality, and data integrity, is embedded into IPv6.
- Routing efficiency
- Reliability
- Most importantly it's the final solution for growing nodes in Global-network.

- The device allocates addresses on its own.
- Internet protocol security is used to support security.
- Enable simple aggregation of prefixes allocated to IP networks; this saves bandwidth by enabling the simultaneous transmission of large data packages.

Disadvantages of IPv6

- **Conversion:** Due to widespread present usage of IPv4 it will take a long period to completely shift to IPv6.
- **Communication:** IPv4 and IPv6 machines cannot communicate directly with each other.
- **Not going backward Compatibility:** IPv6 cannot be executed on IPv4-capable computers because it is not available on IPv4 systems.
- **Conversion Time:** One significant drawback of IPv6 is its inability to uniquely identify each device on the network, which makes the conversion to IPV4 extremely time-consuming.
- Cross-protocol communication is forbidden since there is no way for IPv4 and IPv6 to communicate with each other.

❖ IPv6 Datagram Format

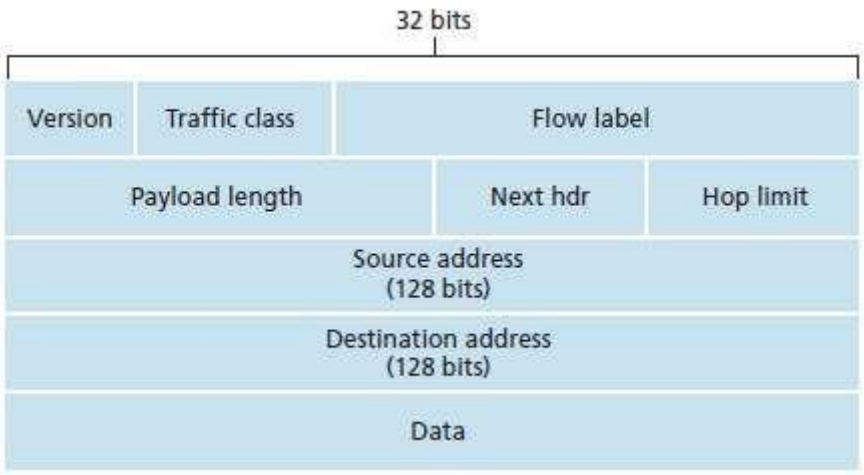


Fig. IPv6 datagram format

- **Version:** The size of the Version field is 4 bits. The Version field shows the version of IP and is set to 6.
- **Traffic Class**: The size of Traffic Class field is 8 bits. Traffic Class field is similar to the IPv4 Type of Service (ToS) field. The Traffic Class field indicates the IPv6 packet's class or priority.
- **Flow Label**: The size of Flow Label field is 20 bits. The Flow Label field provide additional support for real-time datagram delivery and quality of service features. The purpose of Flow Label field is to indicate that this packet belongs to a specific sequence of packets between a source and destination and can be used to prioritized delivery of packets for services like voice.
- **Payload Length**: The size of the Payload Length field is 16 bits. The Payload Length field shows the length of the IPv6 payload, including the extension headers and the upper layer protocol data
- **Next Header**: The size of the Next Header field is 8 bits. The Next Header field shows either the type of the first extension (if any extension header is available) or the protocol in the upper layer such as TCP, UDP, or ICMPv6.

- **Hop Limit**: The size of the Hop Limit field is 8 bits The Hop Limit field shows the maximum number of routers the IPv6 packet can travel. This Hop Limit field is similar to IPv4 Time to Live (TTL) field.
- **Source Address:** The size of the Source Address field is 128 bits. The Source Address field shows the IPv6 address of the source of the packet.
- **Destination Address:** The size of the Destination Address field is 128 bits. The Destination Address field shows the IPv6 address of the destination of the packet.
- **Data:** The data to be transmitted in the datagram, either an entire higher-layer message or a fragment of one.

❖ Difference Between IPv6 and IPv4

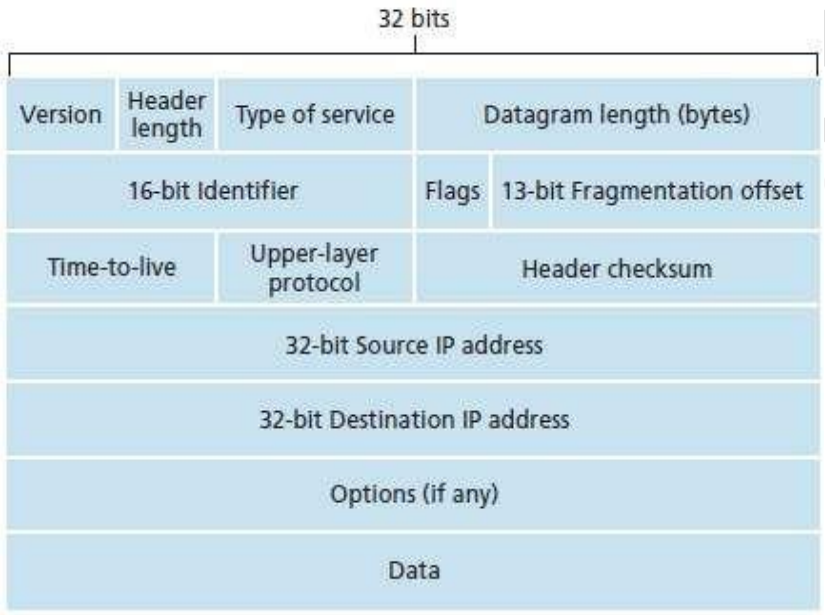
IPv6	IPv4
IPv6 has a 128-bit address length	IPv4 has a 32-bit address length
It supports Auto and renumbering address configuration	It Supports Manual and DHCP address configuration
The address space of IPv6 is quite large it can produce 3.4×1038 address space	It can generate 4.29×109 address space
Address Representation of IPv6 is in hexadecimal	Address representation of IPv4 is in decimal
In IPv6 checksum field is not available	In IPv4 checksum field is available
IPv6 has a header of 40 bytes fixed	IPv4 has a header of 20-60 bytes.
IPv6 does not support VLSM.	IPv4 supports VLSM(Variable Length subnet mask).

❖ IPv4 datagram format

- **Version number**: These 4 bits specify the IP protocol version of the datagram. It determines how to interpret the header. Currently the only permitted values are 4 (0100) or 6 (0110).
- **Header length:** Specifies the length of the IP header, in 32-bit words.
- **Type of service:** The type of service (TOS) bits were included in the IPv4 header to allow different types of IP datagrams (for example, datagrams particularly requiring low delay, high throughput, or

reliability) to be distinguished from each other.

- **Datagram length:** This is the total length of the IP datagram (header plus data), measured in bytes.
- **Identifier:** Uniquely identifies the datagram. It is incremented by 1 each time a datagram is sent. All fragments of a datagram contain the same identification value. This allows the destination host to determine which fragment belongs to which datagram.
- **Flags:** In order for the destination host to be absolutely sure it has received the last fragment of the original datagram, the last fragment has a flag bit set to 0, whereas all the other fragments have this flag bit set to 1.
- **Fragmentation offset:** When fragmentation of a message occurs, this field specifies the offset, or position, in the overall message where the data in this fragment goes. It is specified in units of 8 bytes (64 bits).



- **Time-to-live:** Specifies how long the datagram is allowed to "live" on the network. Each router decrements the value of the TTL field (reduces it by one) prior to transmitting it. If the TTL field drops to zero, the datagram is assumed to have taken too long a route and is discarded.
- **Protocol***:* This field is used only when an IP datagram reaches its final destination. The value of this field indicates the specific transport-layer protocol to which the data portion of this IP datagram should be passed. For example, a value of 6 indicates that the data portion is passed to TCP, while a value of 17 indicates that the data is passed to UDP.
- **Header checksum:** The header checksum aids a router in detecting bit errors in a received IP datagram.
- **Source and destination IP addresses:** When a source creates a datagram, it inserts its IP address into the source IP address field and inserts the address of the ultimate destination into the destination IP address field.
- **Options:** The options fields allow an IP header to be extended.
- **Data (payload):** The data to be transmitted in the datagram, either an entire higher-layer message or a fragment of one

Subnetting example:-

Five steps of subnetting are:

1. Identify class of IP address and note the Default Subnet Mask.
2. Convert Default subnet mask into binary
3. Note the number of hosts required per network and find the Subnet Generator(SG) and Octet position
4. Generate new Subnet Mask
5. Use SG and generate network ranges (subnets) into the appropriate octet position

EXAMPLE

The address 192.168.100.0 we required to break that address into **62 hosts per network.**

Step 1: Identify class of IP address and note the Default Subnet Mask.

Here address 192.168.100.0 belongs to Class C and Default Subnet Mask of Class C is 255.255.255.0. In class C we have possibilities of 256 IP address but we can't use first IP address and last IP address as first IP address is network address and last IP address is broadcast address. So we have 254 IP addresses but here we need only 62.

Step 2: Identify Convert Default subnet mask into binary

255.255.255.0 = 11111111.11111111.11111111.00000000

Step 3: Note the number of hosts required per network and find the Subnet Generator(SG) and Octet position

No. of hosts per subnet = 62 (So convert 64 into binary) 62 =111110 (6bits)

Reserve 6 bits in the subnet mask

So, we need 6 bits in the host portion of the address in our default subnet mask. Our default subnet mask is

255.255.255.0=11111111.11111111.11111111.00000000

Here we need to reserve from right to left in last octet of default subnet mask ie keeping rightmost 6 zeros and remaining bits are to converted to 1's
255.255.255.192=11111111.11111111.11111111.11000000

So the new subnet mask is 255.255.255.192 or /26. So, 62 hosts' needs 6 bits in the host portion.

SG is 64 as first one is at 6^{th} position and 2^6=64 and Octet where we find first one is 4^{th} octet so Octet position=4.

Step 4: Generate new Subnet Mask

The new subnet mask is 255.255.255.192 or /26 is already generated in the last step.

Step 5: Network Ranges (Subnets)

Now for finding the network ranges, our increment is 64 (ie value of SG).

Net Work No	Network ID	HOST Range	Broadcast IP
1	192.168.100.0	192.168.100.1 192.168.100.62	192.168.100.63
2	192.168.100.64	192.168.100.63 192.168.100.126	192.168.100.127
3	192.168.100.128	192.168.100.129 192.168.100.190	192.168.100.191
4	192.168.100.192	192.168.100.193 192.168.100.254	192.168.100.255