CN: WEEK 8

Network Layer Overview

- The Network Layer is the third layer of the OSI model.
- It handles the service requests from the transport layer and further forwards the service request to the data link layer.
- The network layer translates the logical addresses into physical addresses.
- It determines the route from the source to the destination and also manages the traffic problems such as switching, routing and controls the congestion of data packets.
- The main role of the network layer is to move the packets from sending host to the receiving host.

Main Functionalities

Routing: When a packet reaches the router's input link, the router will move the packets to the router's output link. For example, a packet from S1 to R1 must be forwarded to the next router on the path to S2.

Logical Addressing: The data link layer implements the physical addressing and network layer implements the logical addressing. Logical addressing is also used to distinguish between source and destination system. The network layer adds a header to the packet which includes the logical addresses of both the sender and the receiver.

Internetworking: This is the main role of the network layer that it provides the logical connection between different types of networks.

Fragmentation: The fragmentation is a process of breaking the packets into the smallest individual data units that travel through different networks.


IP

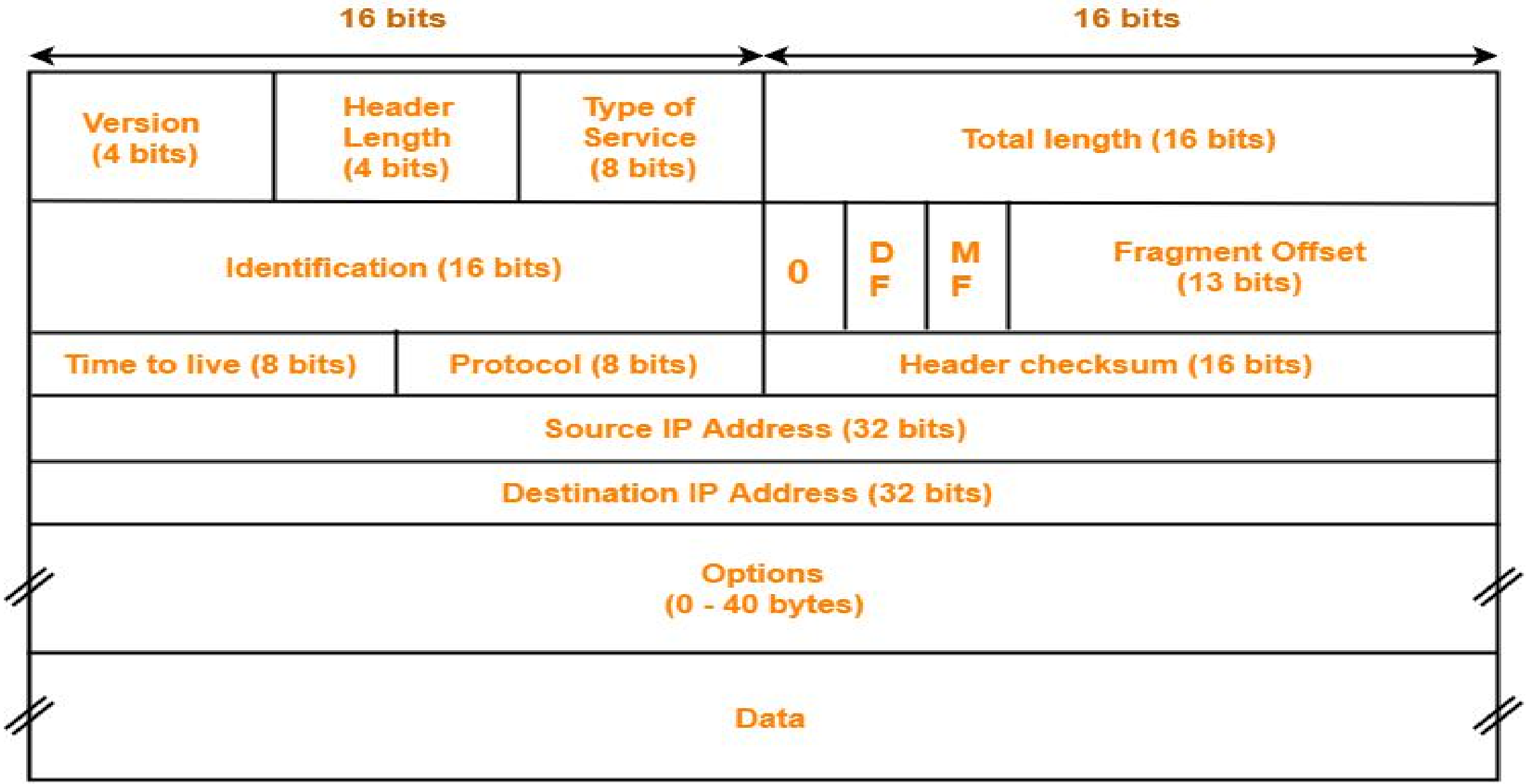
- **IP stands for Internet Protocol and v4 stands for Version Four (IPv4). IPv4 was the primary version brought into action for production within the ARPANET in 1983.**
- **IP version four addresses are 32-bit integers which will be expressed in decimal notation.**
- **Example- 192.0.2.126 could be an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

Parts of IPv4

- ✓ ***Network part:*** *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.


16 bits
16 bits
Version (4 bits)
Header Length (4 bits)
Type of Service (8 bits)
Total length (16 bits)
Identification (16 bits)
0
D F
M F
Fragment Offset (13 bits)
Time to live (8 bits)
Protocol (8 bits)
Header checksum (16 bits)
Source IP Address (32 bits)
Destination IP Address (32 bits)
Options (0 - 40 bytes)
Data

IPv4 Header

Version-

Version is a 4 bit field that indicates the IP version used. (version-4 (IPv4) and version-6 (IPv6))
Only IPv4 uses the above header.
So, this field always contains the decimal value 4.

Header Length-

Header length is a 4 bit field that contains the length of the IP header.
It helps in knowing from where the actual data begins.

Type Of Service-

Type of service is a 8 bit field that is used for Quality of Service (QoS).
The datagram is marked for giving a certain treatment using this field.

Total Length-

Total length is a 16 bit field that contains the total length of the datagram (in bytes).

Total length = Header length + Payload length

Identification-

Identification is a 16 bit field.
It is used for the identification of the fragments of an original IP datagram.

When an IP datagram is fragmented,
Each fragmented datagram is assigned the same identification number.
This number is useful during the re assembly of fragmented datagrams.
It helps to identify to which IP datagram, the fragmented datagram belongs to.

DF Bit-

DF bit stands for Do Not Fragment bit.
Its value may be 0 or 1.
When DF bit is set to 0, it grants the permission to the intermediate devices to fragment the datagram if required.
When DF bit is set to 1, it indicates the intermediate devices not to fragment the IP datagram at any cost.

MF Bit-

MF bit stands for More Fragments bit.
When MF bit is set to 0, it indicates to the receiver that the current datagram is either the last fragment in the set or that it is the only fragment.
When MF bit is set to 1, it indicates to the receiver that the current datagram is a fragment of some larger datagram and more fragments are following.

Fragment Offset-

Fragment Offset is a 13 bit field.
It indicates the position of a fragmented datagram in the original unfragmented IP datagram.
The first fragmented datagram has a fragment offset of zero.

Time To Live-

Time to live (TTL) is a 8 bit field that iindicates the maximum number of hops a datagram can take to reach the destination.
It prevents IP datagrams from looping around forever in a routing loop.
The value of TTL is decremented by 1 when-
Datagram takes a hop to any intermediate device having network layer.
Datagram takes a hop to the destination.
If the value of TTL becomes zero before reaching the destination, then datagram is discarded.

Protocol-

Protocol is a 8 bit field.
It tells the network layer at the destination host to which protocol the IP datagram belongs to.
In other words, it tells the next level protocol to the network layer at the destination side.
Protocol number of ICMP is 1, IGMP is 2, TCP is 6 and UDP is 17.

Header Checksum-

Header checksum is a 16 bit field.
It contains the checksum value of the entire header.
The checksum value is used for error checking of the header.
At each hop, the header checksum is compared with the value contained in this field.
If header checksum is found to be mismatched, then the datagram is discarded.

Source IP Address-

Source IP Address is a 32 bit field.
It contains the logical address of the sender of the datagram.

Destination IP Address-

Destination IP Address is a 32 bit field.
It contains the logical address of the receiver of the datagram.

Options-

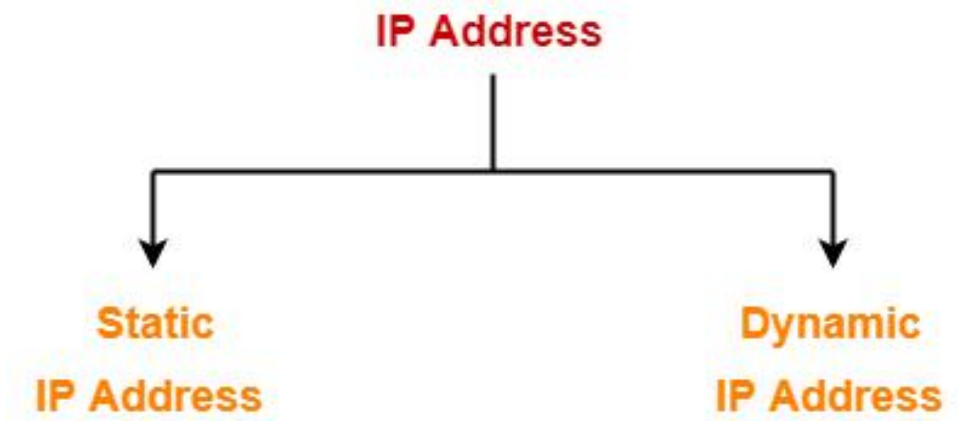
Options is a field whose size vary from 0 bytes to 40 bytes.
This field is used for several purposes such as-

- Record route (used to record the IP Address of the routers through which the datagram passes on its way.)
- Source routing (used to specify the route that the datagram must take to reach the destination.)
- Padding (Addition of dummy data to fill up unused space in the transmission unit and make it conform to the standard size)

IP Address in Networking

In networking,

- IP Address is short for Internet Protocol Address.
- It is a unique address assigned to each computing device in an IP network.
- ISP assigns IP Address to all the devices present on its network.
- Computing devices use IP Address to identify and communicate with other devices in the IP network.



Static IP Address is an IP Address that once assigned to a network element always remains the same. They are configured manually.

Dynamic IP Address is a temporarily assigned IP Address to a network element. It can be assigned to a different device if it is not in use. DHCP assigns dynamic IP addresses.

IP Address Format

IP Address is a 32 bit binary address written as 4 numbers separated by dots.

The 4 numbers are called as octets where each octet has 8 bits.

The octets are divided into 2 components- Net ID and Host ID.

Format of an IP Address

Network ID represents the IP Address of the network and is used to identify the network.

Host ID represents the IP Address of the host and is used to identify the host within the network.

Example of an IP Address is-

00000001.10100000.00001010.11110000

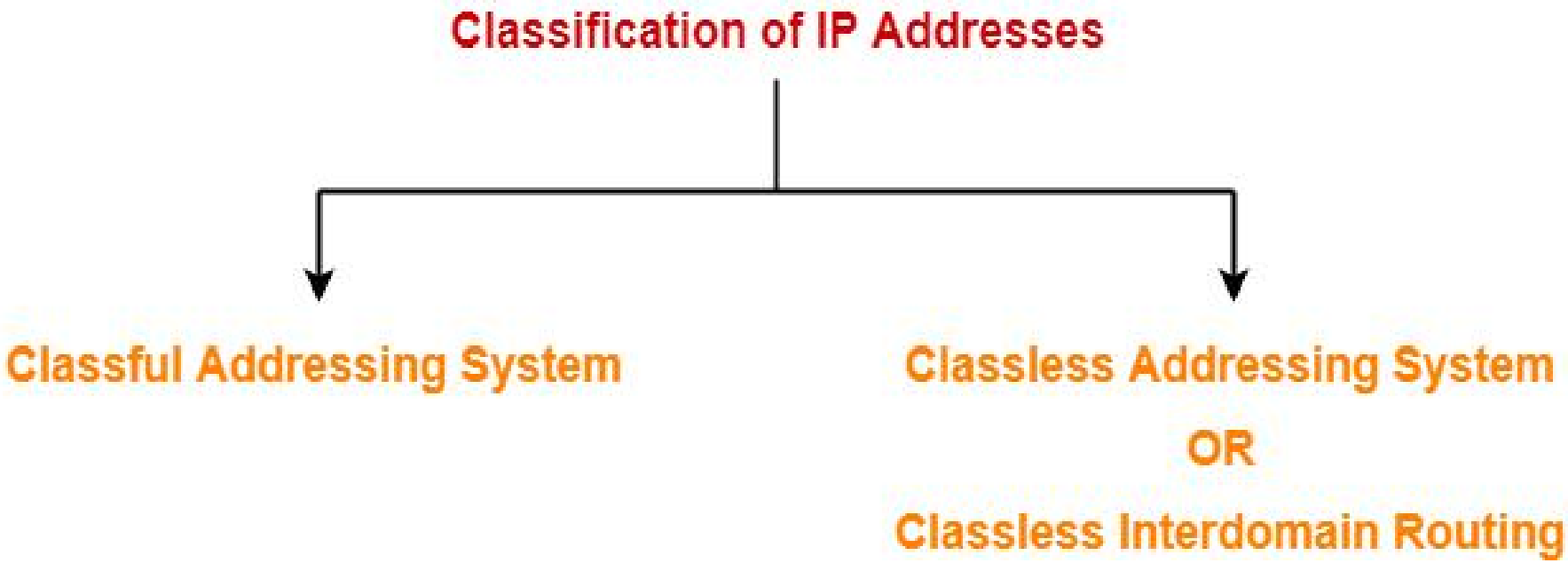
(Binary Representation)

OR

1.160.10.240

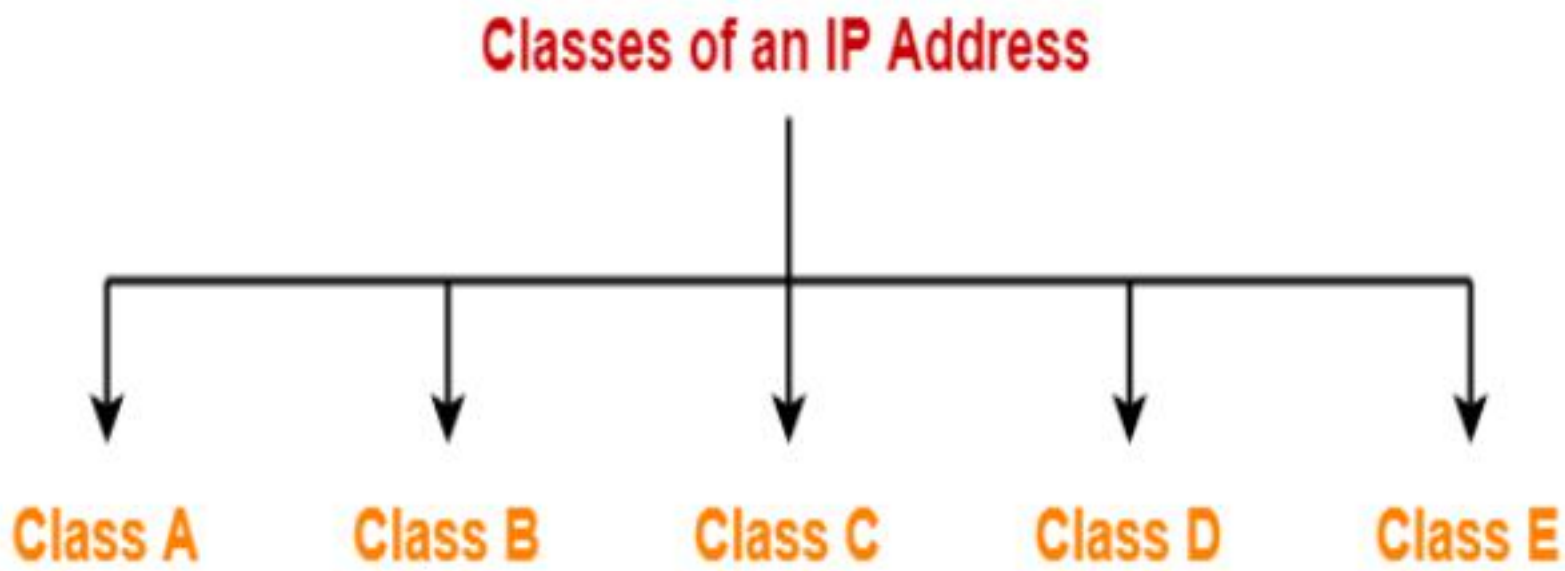
(Decimal Representation)

There are two systems in which IP Addresses are classified



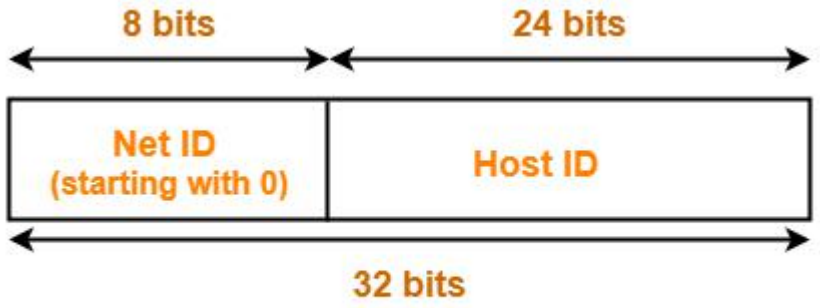
Classful Addressing

In Classful Addressing System, IP Addresses are organized into following 5 classes-



Class A

- If the 32 bit binary address starts with a bit 0, then IP Address belongs to class A.
- In class A IP Address, the first 8 bits are used for the Network ID & the remaining 24 bits are used for the Host ID.



Class A IP Address

Total Number Of IP Addresses-

Total number of IP Addresses available in class A

= Numbers possible due to remaining available 31 bits

$= 2^{31}$

Total Number Of Networks-

Total number of networks available in class A

= Numbers possible due to remaining available 7 bits in the Net ID – 2

$= 2^{7} - 2 = 126$

Total Number Of Hosts-

Total number of hosts that can be configured in class A

= Numbers possible due to available 24 bits in the Host ID – 2

$= 2^{24} - 2$

Range Of 1st Octet-

We have-

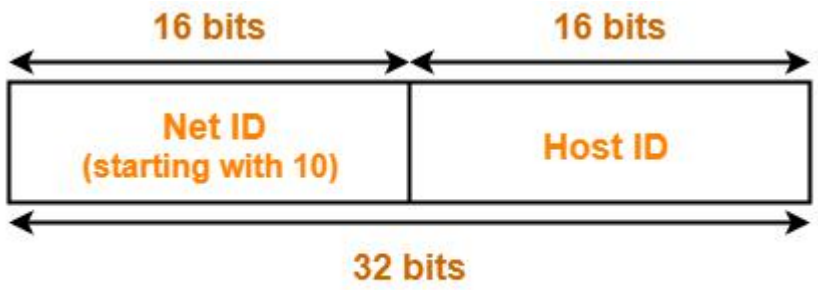
- Minimum value of 1st octet = **0**0000000 = 0
- Maximum value of 1st octet = **0**1111111 = 127

From here,

- Range of 1st octet = [0, 127]
- But 2 networks are reserved and unused.
- So, Range of 1st octet = [1, 126]

Class B

- If the 32 bit binary address starts with a bit 10, then IP Address belongs to class B.
- In class B IP Address, the first 16 bits are used for the Network ID & the remaining 16 bits are used for the Host ID.



Class B IP Address

Total Number Of IP Addresses-

Total number of IP Addresses available in class B
= Numbers possible due to remaining available 30 bits
= 2^{30}

Total Number Of Networks-

Total number of networks available in class B
= Numbers possible due to remaining available 14 bits in the Net ID
= 2^{14}

Total Number Of Hosts-

Total number of hosts that can be configured in class B
= Numbers possible due to available 16 bits in the Host ID – 2
= $2^{16} – 2$

Range Of 1st Octet-

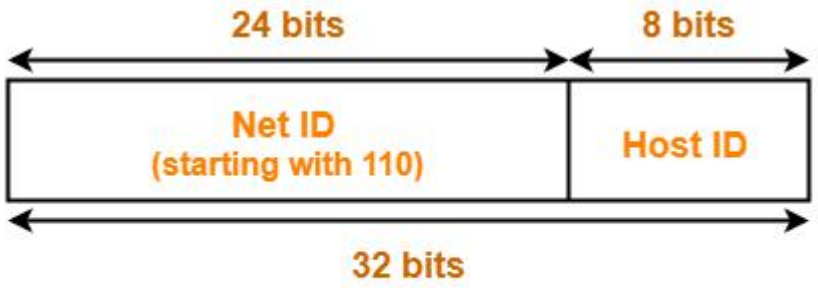
We have-

- Minimum value of 1st octet = **10**000000 = 128
- Maximum value of 1st octet = **10**111111 = 191

So, Range of 1st octet = [128, 191]

Class C

- If the 32 bit binary address starts with a bit 110, then IP Address belongs to class C.
- In class C IP Address, the first 24 bits are used for the Network ID & the remaining 8 bits are used for the Host ID.



Class C IP Address

Total Number Of IP Addresses-

Total number of IP Addresses available in class C

= Numbers possible due to remaining available 29 bits

= 2^{29}

Total Number Of Networks-

Total number of networks available in class C

= Numbers possible due to remaining available 21 bits in the Net ID

= 2^{21}

Total Number Of Hosts-

Total number of hosts that can be configured in class C

= Numbers possible due to available 8 bits in the Host ID – 2

= $2^8 – 2$

Range Of 1st Octet-

We have-

- Minimum value of 1st octet = **110**00000 = 192
- Maximum value of 1st octet = **110**111111 = 223

Class D

- If the 32 bit binary address starts with a bit 1110, then IP Address belongs to class D.
- Class D is not divided into Network ID and Host ID.

Class D IP Address

Total Number Of IP Addresses-

Total number of IP Addresses available in class D
= Numbers possible due to remaining available 28 bits
= 2^{28}

Range Of 1st Octet-

We have-

- Minimum value of 1st octet = **1110**0000 = 224
- Maximum value of 1st octet = **1110**1111 = 239

Class E

- If the 32 bit binary address starts with a bit 1111, then IP Address belongs to class E.
- Class E is not divided into Network ID and Host ID.

Class E IP Address

Total Number Of IP Addresses-

Total number of IP Addresses available in class E
= Numbers possible due to remaining available 28 bits
= 2^{28}

Range Of 1st Octet-

We have-

- Minimum value of 1st octet = **1111**0000 = 240
- Maximum value of 1st octet = **1111**1111 = 255

Uses of Classes of IP address

- Class A is used by organizations requiring very large size networks like NASA, Pentagon etc.
- Class B is used by organizations requiring medium size networks like IRCTC, banks etc.
- Class C is used by organizations requiring small to medium size networks like colleges, small universities, small offices etc.
- Class D is reserved for multicasting.
- Class E is reserved for future or experimental purposes.

Class of IP Address	Total Number of IP Addresses	1st Octet Decimal Range	Number of Networks available	Hosts per network	Default Subnet Mask
Class A	2^{31}	1 – 126	$2^{7} - 2$	$2^{24} - 2$	255.0.0.0
Class B	2^{30}	128 – 191	2^{14}	$2^{16} - 2$	255.255.0.0
Class C	2^{29}	192 – 223	2^{21}	$2^{8} - 2$	255.255.255.0
Class D	2^{28}	224 – 239	Not defined	Not defined	Not defined
Class E	2^{28}	240 – 254	Not defined	Not defined	Not defined

Important Notes

All the hosts in a single network always have the same network ID but different Host ID.
However, two hosts in two different networks can have the same host ID.

There is no relation between MAC Address and IP Address of a host.

IP Address of the network called Net ID is obtained by setting all the bits for Host ID to zero.

Class A Networks accounts for half of the total available IP Addresses.

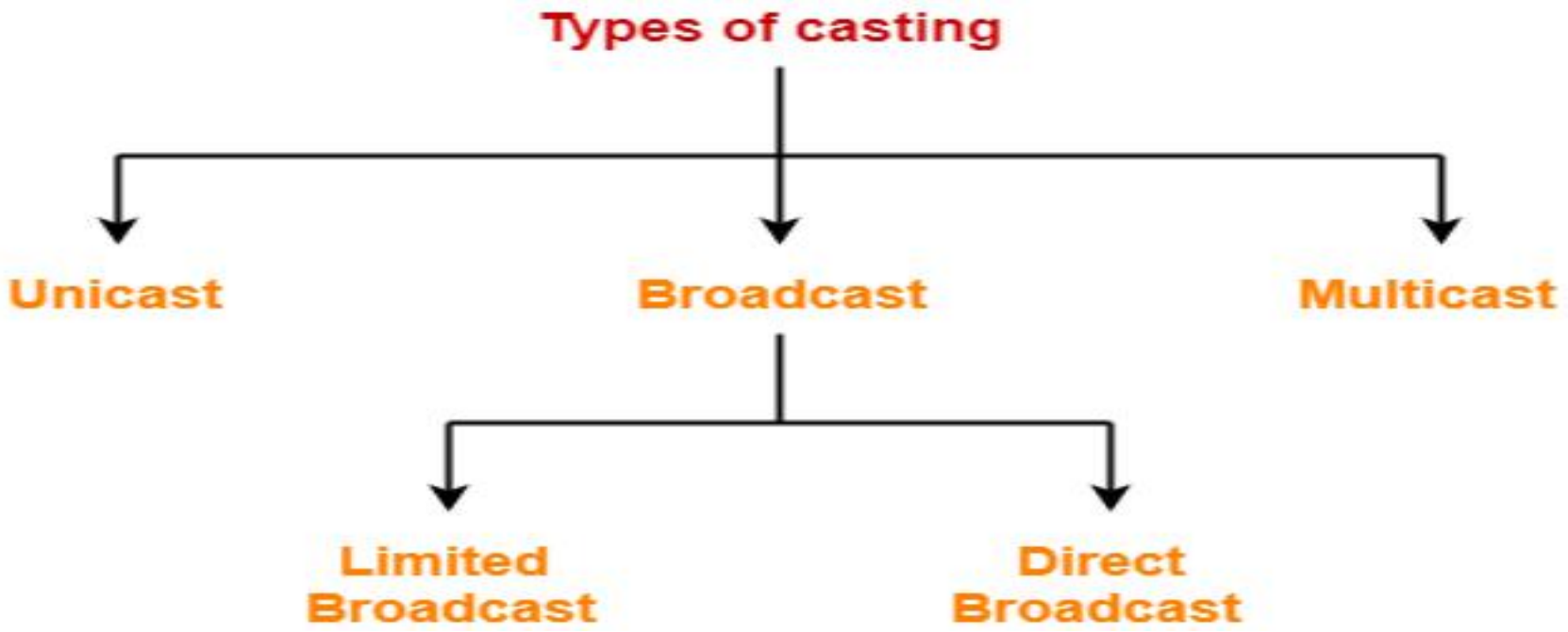
In class A, total number of IP Addresses available for networks are 2 less.
- This is to account for the two reserved network IP Addresses 0.xxx.xxx.xxx and 127.xxx.xxx.xxx.
- IP Address 0.0.0.0 is reserved for broadcasting requirements.
- IP Address 127.0.0.1 is reserved for loopback address used for software testing.

In all the classes, total number of hosts that can be configured are 2 less.
- This is to account for the two reserved IP addresses in which all the bits for host ID are either zero or one.
- When all Host ID bits are 0, it represents the Network ID for the network.
- When all Host ID bits are 1, it represents the Broadcast Address.

Only those devices which have the network layer will have IP Address.
So, switches, hubs and repeaters does not have any IP Address.

Casting in Networking

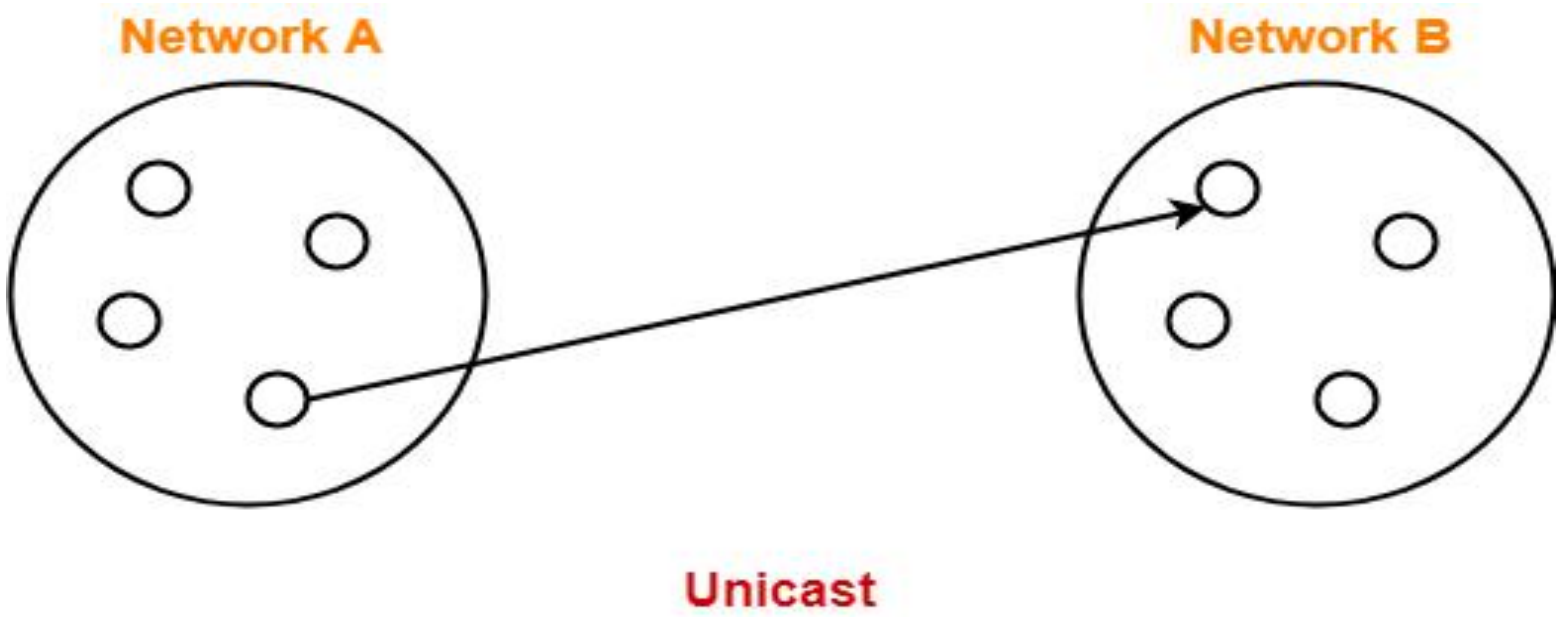
Transmitting data (stream of packets) over the network is termed as casting.



Unicast

Transmitting data from one source host to one destination host is called as unicast.
It is a one to one transmission.

Example-
Host A having IP Address 11.1.2.3 sending data to host B having IP Address 20.12.4.2.
Here,
Source Address = IP Address of host A = 11.1.2.3
Destination Address = IP Address of host B = 20.12.4.2



Broadcast

Transmitting data from one source host to all other hosts residing in the same or other network is called as broadcast. It is a one to all transmission.

Based on recipient's network, it is classified as-

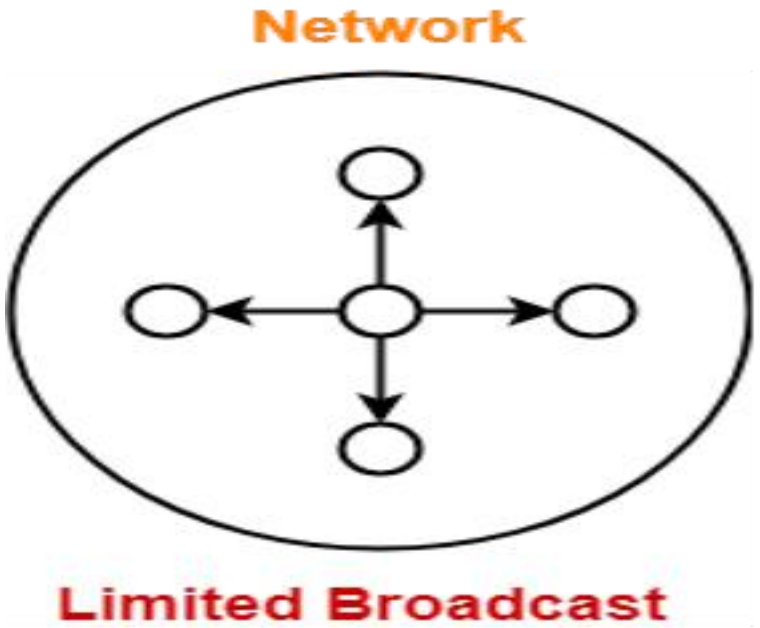
Limited Broadcast
Direct Broadcast

Limited Broadcast

Transmitting data from one source host to all other hosts residing in the same network is called as limited broadcast.

Limited Broadcast Address for any network
= All 32 bits set to 1
= 11111111.11111111.11111111.11111111
= 255.255.255.255

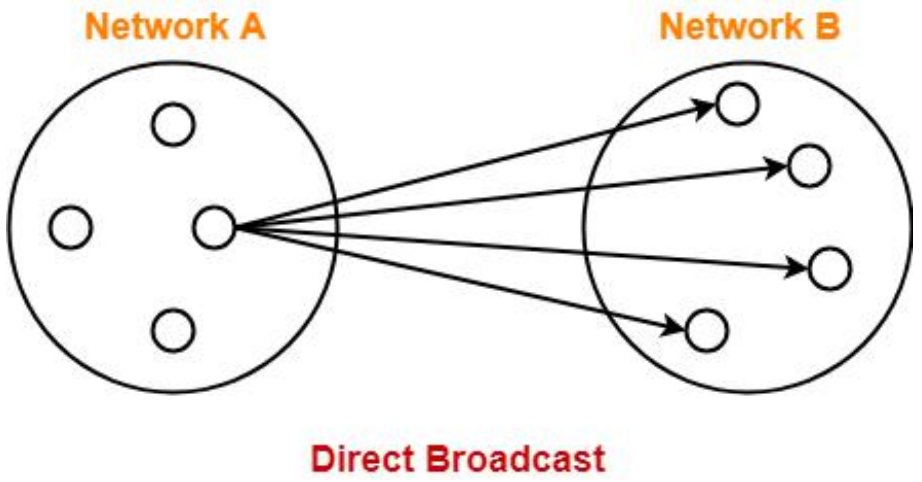
Host A having IP Address 11.1.2.3 sending data to all other hosts residing in the same network.
Here,
Source Address = IP Address of host A = 11.1.2.3
Destination Address = 255.255.255.255



Direct Broadcast

Transmitting data from one source host to all other hosts residing in some other network is called as direct broadcast.
Direct Broadcast Address for any network is the IP Address where-
Network ID is the IP Address of the network where all the destination hosts are present.
Host ID bits are all set to 1.

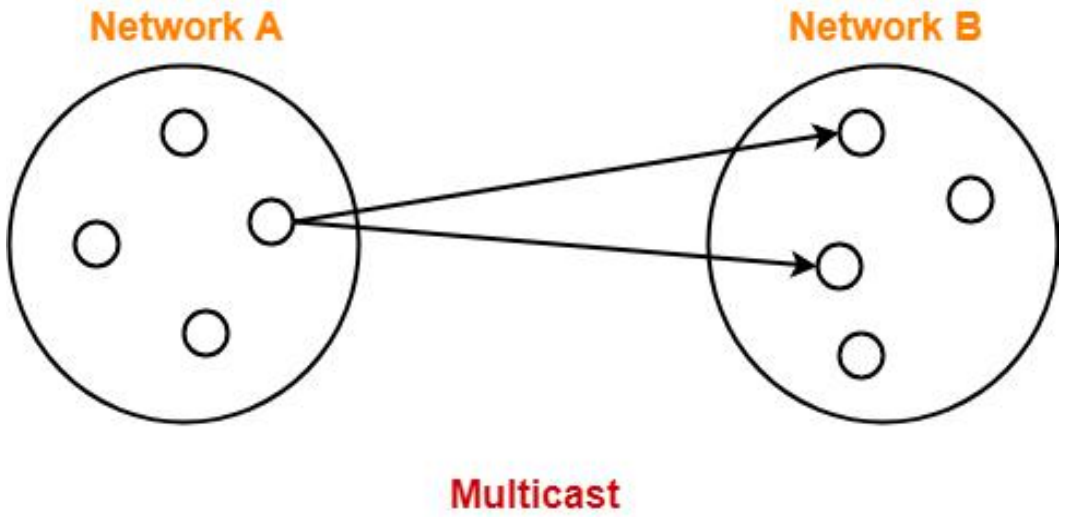
Host A having IP Address 11.1.2.3 sending data to all other hosts residing in the network having IP Address 20.0.0.0
Here,
Source Address = IP Address of host A = 11.1.2.3
Destination Address = 20.255.255.255



Multicast

Transmitting data from one source host to a particular group of hosts having interest in receiving the data is called as multicast.
It is a one to many transmission.

Sending a message to a particular group of people on whatsapp
Sending an email to a particular group of people
Video conference or teleconference



MAC Address	IP Address
It stands for Media Access Control Address.	It stands for Internet Protocol Address.
MAC Address identifies the physical address of a computer on the internet.	IP Address identifies the connection of a computer on the internet.
Manufacturer of NIC card assigns the MAC Address.	Network Administrator or ISP assigns the IP Address.
Reverse Address Resolution Protocol (RARP) is used for resolving physical (MAC) Address into IP address.	Address Resolution Protocol (ARP) is used for resolving IP Address into physical (MAC) address.

Important Points

For any given IP Address,

If the range of first octet is [1, 126], then IP Address belongs to class A.
If the range of first octet is [128, 191], then IP Address belongs to class B.
If the range of first octet is [192, 223], then IP Address belongs to class C.
If the range of first octet is [224, 239], then IP Address belongs to class D.
If the range of first octet is [240, 254], then IP Address belongs to class E.

For any given IP Address, IP Address of its network is obtained by setting all its Host ID part bits to 0.
For any given IP Address, Direct Broadcast Address is obtained by setting all its Host ID part bits to 1.
For any given IP Address, limited Broadcast Address is obtained by setting all its bits to 1. For any network, its limited broadcast address is always 255.255.255.255

Class D IP Addresses are not divided into Net ID and Host ID parts.
Class E IP Addresses are not divided into Net ID and Host ID parts.

PRACTICE PROBLEMS BASED ON IP ADDRESS IN NETWORKING

For the following IP Addresses-

1.2.3.4
10.15.20.60
130.1.2.3
150.0.150.150
300.1.2.3

Identify the Class, Network IP Address, Direct broadcast address and Limited broadcast address of each IP Address.

1.2.3.4
IP Address belongs to class A
Network IP Address = 1.0.0.0
Direct Broadcast Address = 1.255.255.255
Limited Broadcast Address = 255.255.255.255

10.15.20.60
IP Address belongs to class A
Network IP Address = 10.0.0.0
Direct Broadcast Address = 10.255.255.255
Limited Broadcast Address = 255.255.255.255

30.1.2.3
IP Address belongs to class B
Network IP Address = 130.1.0.0
Direct Broadcast Address = 130.1.255.255
Limited Broadcast Address = 255.255.255.255

150.0.150.150
IP Address belongs to class B
Network IP Address = 150.0.0.0
Direct Broadcast Address = 150.0.255.255
Limited Broadcast Address = 255.255.255.255

300.1.2.3
This is not a valid IP Address.
This is because for any given IP Address, the range of its first octet is always [1, 254].
First and Last IP Addresses are reserved.

A host with IP Address 200.100.1.1 wants to send a packet to all the hosts in the same network.

What will be-
Source IP Address
Destination IP Address

Source IP Address = IP Address of the sender = 200.100.1.1
Destination IP Address = Limited Broadcast Address = 255.255.255.255

A host with IP Address 10.100.100.100 wants to use loop back testing.

What will be-
Source IP Address
Destination IP Address

Source IP Address = 10.100.100.100
Destination IP Address = Loopback Testing Address = 127.0.0.1

How many bits are allocated for Network ID and Host ID in 23.192.157.234 address?

Given IP Address belongs to class A.
Thus, Number of bits reserved for Network ID = 8
Number of bits reserved for Host ID = 24

Suppose that instead of using 16 bits for network part of a class B Address, 20 bits have been used. How many class B networks would have been possible?

Total 20 bits are used for Network ID of class B.
The first two bits are always set to 10.
Then, with 18 bits, number of networks possible = 2^{18}

What is the default mask for 192.0.46.10?

Given IP Address belongs to class C.
For class C, default mask = 255.255.255.0

END