Network Layer: Logical Addressing

Dr. Sachin Kumar Yadav

BCSC 0008: Computer Networks

Objective: *The objective is to understand fundamental underlying principles of computer networking, details and functionality of layered network architecture.*

Credits: 03 **Semester - IV** **L–T–P-J: 3–1–0-0**

Module No.	Content	Teaching Hours
I	**Introduction Concepts**: Goals and Applications of Networks, Network structure and architecture, The OSI reference model, services, Network Topology Design, Physical Layer Transmission Media, Line coding scheme, switching methods (circuit switching, Packet switching), TDM. **Medium Access sub layer**: Medium Access sub layer - Channel Allocations, LAN protocols - ALOHA protocols, CSMA, CSMA/CD, Overview of IEEE standards. **Data Link Layer**: Error detection and correction, Flow control (sliding window protocol)	20
II	**Network Layer**: Network Layer –IP addressing, subnet, CIDR, VLSM, Internetworking, Address mapping, routing. Connecting devices. **Transport Layer**: Transport Layer - Design issues, connection management, Flow control, TCP window management, congestion control-slow start algorithm. **Application Layer**: Data compression, Data Encryption, File Transfer, DNS, HTTP, SMTP, TELNET **Introduction to IPv6, transition from IPv4 to IPv6.**	20

Text Books:

- Forouzan B. A. , "Data Communication and Networking", 4th Edition, McGrawHill,2004.

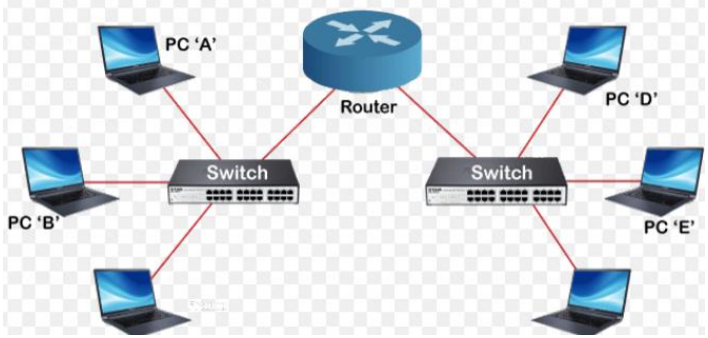
References:

- Kurose, J.F. and Ross K.W., "Computer Networking: A Top-Down Approach Featuring the Internet", 3rd Edition, Addison-Wesley,2005.
- A.S. Tanenbaum, "Computer Networks", 2nd Edition, Prentice Hall India,2006.

ROUTER:

A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions between networks and on the global Internet.

A network switch **connects devices in a network to each other, enabling them to talk by exchanging data packets**.



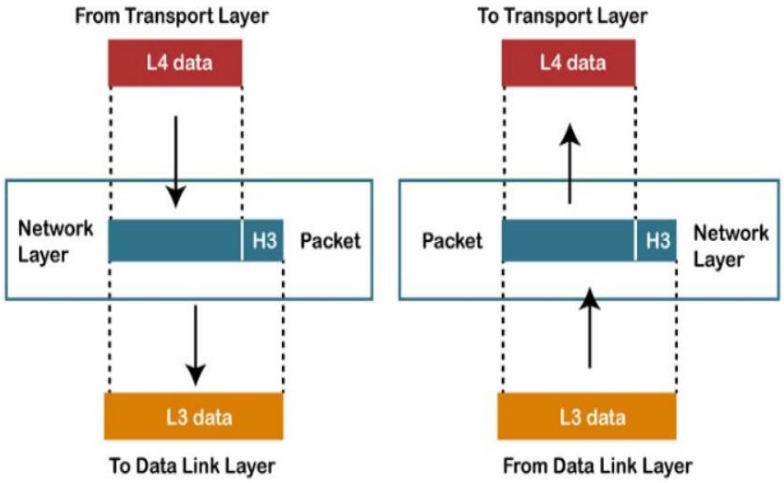
A switch connects multiple devices to create a network, a router connects multiple switches, and their respective networks, to form an even larger network.

Router	Switch
The main objective of router is to connect various networks simultaneously.	While the main objective of switch is to connect various devices simultaneously.
It works in network layer.	While it works in data link layer.
Router is used by LAN as well as MAN.	While switch is used by only LAN.
Through the router, data is sent in the form of packets.	While through switch data is sent in the form of frame.
There is less collision taking place in the router.	While there is no collision taking place in full duplex switch.
Router is a relatively much more expensive device than switch.	Switch is an expensive device than hub. but cheaper than router.
maximum speed for wireless is 1-10 Mbps and maximum speed for wired connections is 100 Mbps.	Maximum speed is 10Mbps to 100Mbps.

NETWORK LAYER

In the seven-layer OSI model of computer networking, the network layer is layer 3. The network layer is responsible for packet forwarding including routing through intermediate routers.

- ✓ Network layer is responsible for source to destination delivery of the packets.
- ✓ The network layer must know the topology of the subnet and choose appropriate paths through it.
- ✓ When source and destination are in *different networks*, the network layer (IP) must deal with these differences.



Functions Performed by the Network Layer

The network layer performs several functions to facilitate data transmission in a network. Some of the functions performed are as follows:

Routing: It is the process to determine the most effective route for data transmission in the network. When a data packet arrives at the router's input link, it determines the ideal route for data transmission in the network. It determines the path that will be used to transfer the packet further in the network.

Logical Addressing: There are two types of addressing performed in the network: logical addressing and physical addressing.
The data link layer performs the physical addressing, while the network layer does the logical addressing in the OSI model.
Logical addressing is also used to distinguish between the 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 most important function performed by the network layer of the OSI model. It establishes the logical connection between nodes in the same or different networks.

Fragmentation: It is the conversion of data packets into the smallest individual data units capable of being transmitted in the network.

Network Layer Services:

1. Guaranteed delivery: This layer offers a service that ensures the packet arrives at its destination.

2. Guaranteed delivery with bounded delay: This service assures that the packet will arrive within the given host-to-host delay bound.

3. In-Order packets: This service assures that packets reach their destination in the order they were delivered.

4. Security services: These are provided at the network layer through the use of a session key between the source and destination hosts. The payloads of datagrams transmitted to the destination host are encrypted by the network layer of the source host. The payload would subsequently be decrypted by the network layer at the target host.

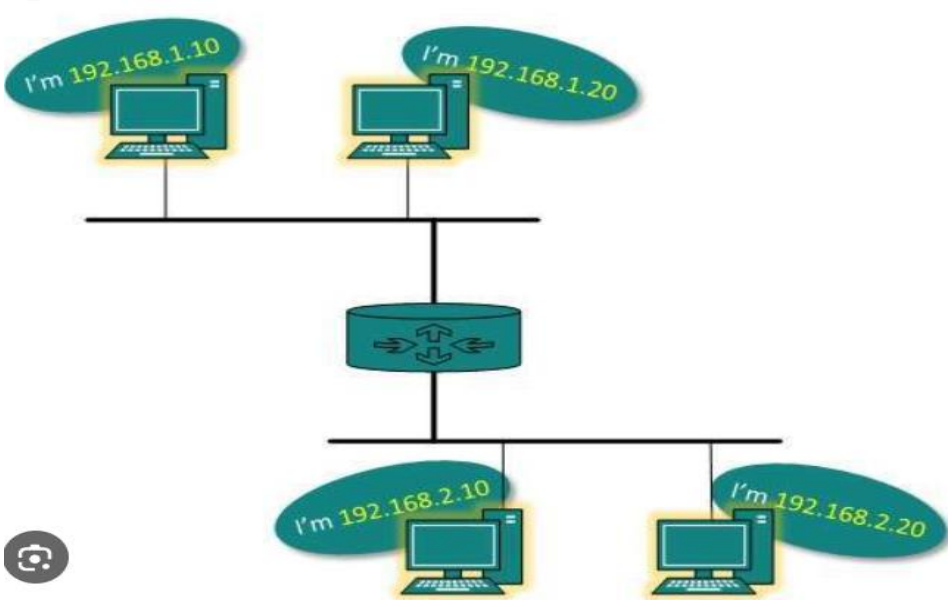
Logical Addressing

Logical address also referred to as IP (Internet Protocol) address is an universal addressing system. It is used in the Network layer. This address facilitates universal communication that are not dependent on the underlying physical networks.

There are two types of IP addresses: IPv4 and IPv6.

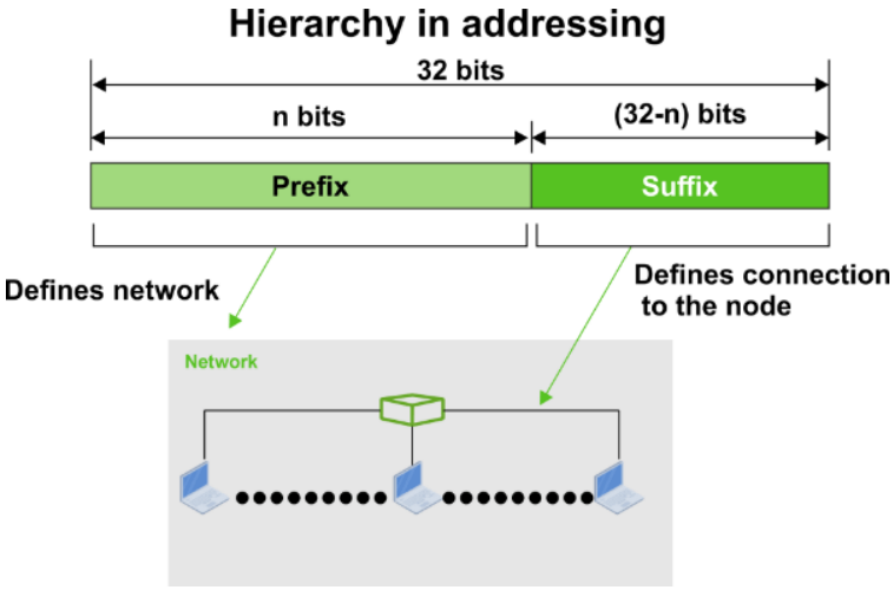
What is logical addressing in network?

An IP address is also known as a logical address and it can change over time as well as from one network to another. The Internet Service Provider will be in charge of assigning it. When a device connects to a different network, it receives a different IP address as a result of a change in Internet Service Provider.



IPv4 ADDRESSES

An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a device (for example, a computer or a router) to the Internet.



The IPv4 addresses are unique and universal.

The address space of IPv4 is 2^{32} or 4,294,967,296 (Four billion, two hundred ninety-four million, nine hundred sixty-seven thousand, two hundred ninety-six)

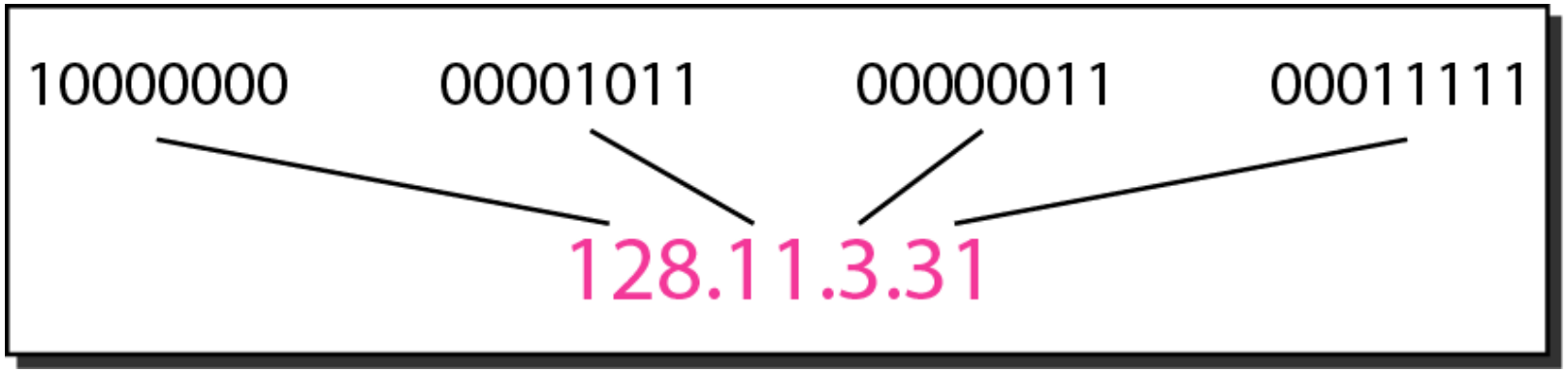


Figure 1 ***Dotted-decimal notation and binary notation for an IPv4 address***

Example 1

Change the following IPv4 addresses from binary notation to dotted-decimal notation.

a. 10000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

Solution

We replace each group of 8 bits with its equivalent decimal number (see Appendix B) and add dots for separation.

a. 129.11.11.239

b. 193.131.27.255

Example 2

Change the following IPv4 addresses from dotted-decimal notation to binary notation.

a. 111.56.45.78

b. 221.34.7.82

Solution

We replace each decimal number with its binary equivalent (see Appendix B).

a. 01101111 00111000 00101101 01001110

b. 11011101 00100010 00000111 01010010

Example 3

Find the error, if any, in the following IPv4 addresses.

a. 111.56.045.78

b. 221.34.7.8.20

c. 75.45.301.14

d. 11100010.23.14.67

Solution

a. There must be no leading zero (045).

b. There can be no more than four numbers.

c. Each number needs to be less than or equal to 255.

d. A mixture of binary notation and dotted-decimal notation is not allowed.

IP address classes

Based on the following rules, IP addresses are categorized into five classes; A, B, C, D, and E.

- In class **A**, the first bit of the first byte always remains **OFF** (0).
- In class **B**, the first bit of the first byte always remains **ON** and the second bit of the first byte always remains **OFF**.
- In class **C**, the first two bits of the first byte always remain **ON** and the third bit of the first byte always remains **OFF**.
- In class **D**, the first three bits of the first byte always remain **ON** and the fourth bit of the first byte always remains **OFF**.
- In class **E**, the first four bits of the first byte always remain **ON**.

Network and host addressing

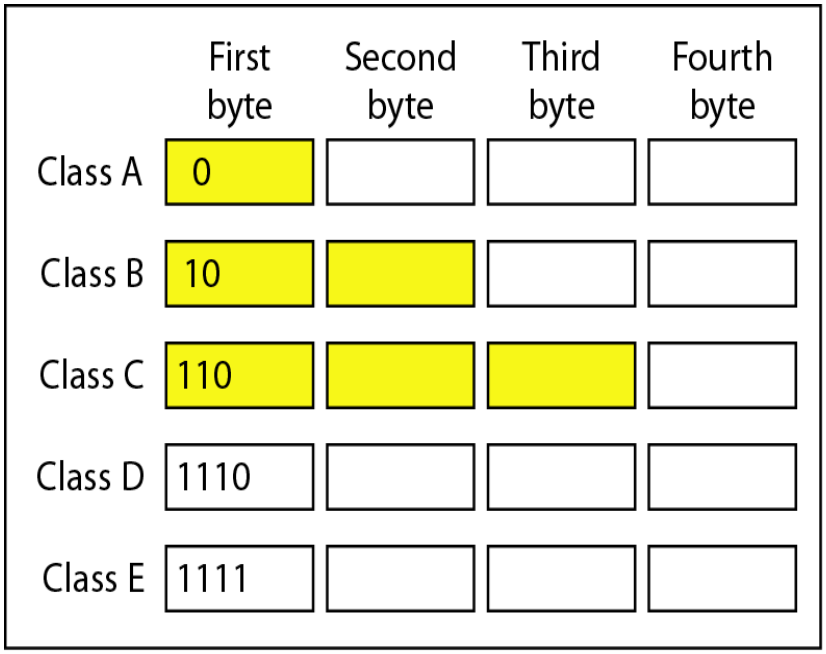
In the second level of the hierarchical addressing scheme, each address is further divided into two addresses: the network address and host address.

Network addresses are used to combine multiple IP addresses in a group while host addresses are used to provide a unique identity to each IP address in the group. A network address is the group address. All group members use the same network address. A host address is a unique address in the group.

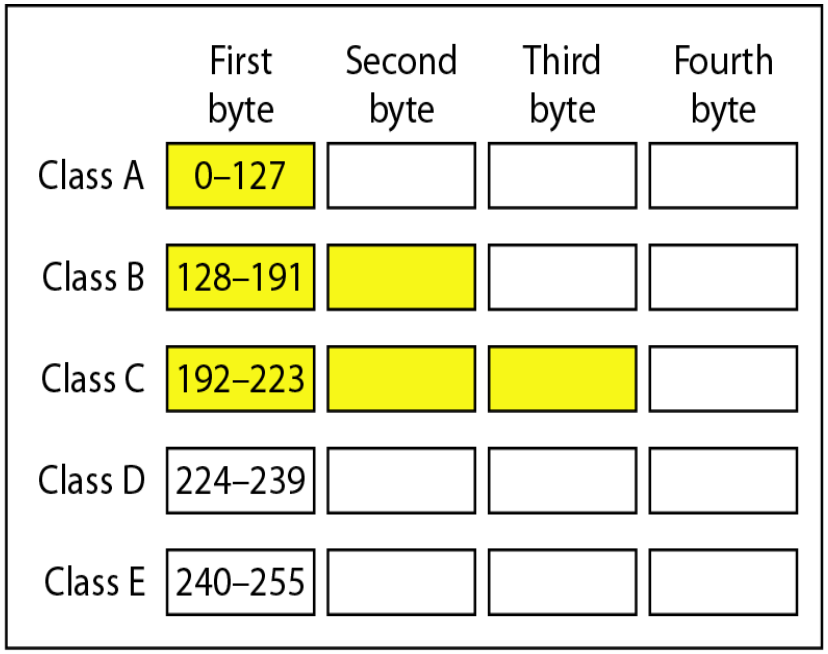
In classful addressing, the address space is divided into five classes: A, B, C, D, and E.

```
Class A
  0.  0.  0.  0 = 00000000.00000000.00000000.00000000
127.255.255.255 = 01111111.11111111.11111111.11111111
                  0nnnnnnn.HHHHHHHH.HHHHHHHH.HHHHHHHH

Class B
128.  0.  0.  0 = 10000000.00000000.00000000.00000000
191.255.255.255 = 10111111.11111111.11111111.11111111
                  10nnnnnn.nnnnnnnn.HHHHHHHH.HHHHHHHH

Class C
192.  0.  0.  0 = 11000000.00000000.00000000.00000000
223.255.255.255 = 11011111.11111111.11111111.11111111
                  110nnnnn.nnnnnnnn.nnnnnnnn.HHHHHHHH

Class D
224.  0.  0.  0 = 11100000.00000000.00000000.00000000
239.255.255.255 = 11101111.11111111.11111111.11111111
                  1110XXXX.XXXXXXXX.XXXXXXXX.XXXXXXXX

Class E
240.  0.  0.  0 = 11110000.00000000.00000000.00000000
255.255.255.255 = 11111111.11111111.11111111.11111111
                  1111XXXX.XXXXXXXX.XXXXXXXX.XXXXXXXX
```

- *n* indicates a bit used for the network ID.
- *H* indicates a bit used for the host ID.
- *X* indicates a bit without a specified purpose.



a. Binary notation



b. Dotted-decimal notation

Finding the classes in binary and dotted-decimal notation

1. Class A:

An IP address is allocated to networks with a high number of hosts in Class A. The network ID has an 8-bit length. The host ID has a length of 24 bits. The first bit in the higher order bits of the first octet is always set to 0 in Class A, while the following 7 bits define the network ID.

There are 2^7 - 2 = 126 networks in the Class A network

Total number of Host IDs in Class A = 2^{24} - 2 [1, 67, 77, 214]

Total number of connections in Class A = 2^{31} (2, 14, 74, 83, 648)

Organizations needing very large networks, like Indian Railways, employ class A.

An example of a Class address is 102.168.212.226. Here, “102” helps you identify the network and 168.212.226 identify the host.

127.0.0.1 IP Address	0.0.0.0 IP Address
It is a loopback address(localhost address).	It is a non-routable address.
This address is used to connect to the same machine or computer the end-user is using.	It indicates an invalid, unknown, or inapplicable end-user address
127.x.y.z also is another address of the computer. 127.0.0.0 is a loopback subnet and 127.255.255.255 is a broadcast address for the loopback subnet.	0.0.0.0 is not the address of anything.

127.0.0.1 signals the TCP/IP of your computer that it don not want to connect to the Internet. It states a connection to a server hosted on the same computer. As such, you'll typically enter it when telling the software to connect to a server via a web browser or a game.
0.0.0.0, on the other hand, is more of a wildcard than a specific location. When you use 0.0.0.0, you tell the software to allow connections from every local IP address possible instead of just 127.0.0.1.

2. Class B:

An IP address is issued to Class B networks, which range in size from modest to big. The Network ID is made up of 16 bits. The Host ID has a length of 16 bits.

The higher order bits of the first octet are always 10 in Class B, while the remaining 14 bits define the network ID. The last 16 bits define the Host ID.

- Total number of connections in the class B network is 2^{30} = 1, 07, 37, 41, 824
- Total number of networks available in class B is 2^{14} = 16, 384
- Total number of hosts that can be configured in Class B = 2^{16} - 2 = 165, 534
- Organizations needing medium-sized networks typically utilize class B.

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.

3. Class C:

Only small-sized networks are allocated an IP address in Class C. The Network ID has a length of 24 bits. The host ID has an 8-bit length.

Total number of connections in Class C = 2^{29} = 53, 68, 70, 912.

Total number of networks available in Class C = 2^{21} = 20, 97, 152.

Total number of hosts that can be configured in every network in Class C = 2^{8} - 2 = 254.

Organizations needing small to medium-sized networks typically choose class C.

4. Class D:

An IP address in Class D is designated for multicast addresses. It doesn't have subnetting. The first octet's higher order bits are always 1110, while the remaining bits decide the host ID in any network. 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

5. Class E:

An IP address is utilised in Class E for future usage or for research and development. It doesn't have any subnetting. The first octet's higher order bits are always 1111, while the remaining bits decide the host ID in any network.

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

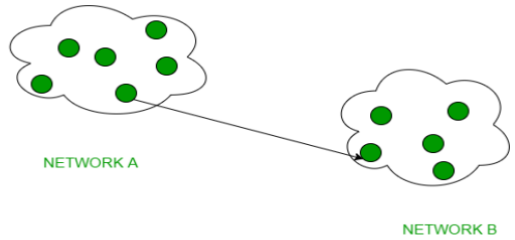
Class	IP Address Range	Usages
A	1.0.0.0 - 127.255.255.255	Very large organizations
B	128.0.0.0 - 191.255.255.255	Mid size organizations
C	192.0.0.0 - 223.255.255.255	Very small organizations
D	224.0.0.0 - 239.255.255.255	Multi-casting
E	240.0.0.0 - 255.255.255.255	Experimental purposes (Reserved)

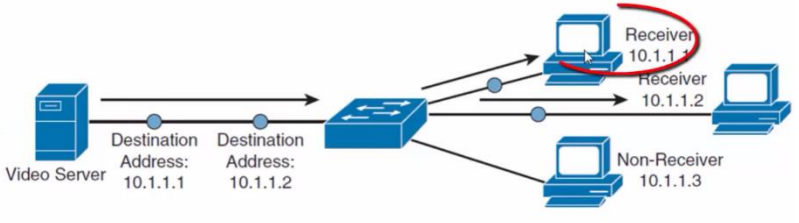
Summary

- 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 is divided into two parts: 1) Prefix 2)Suffix
- IP address works in a network like a postal address. For example, a postal address combines two addresses, address, or your area your house address.
- 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.
- In class B type of network, the first 16 bits (known as two octets) help you identify the network. The other remaining 16 bits indicate the host within the network.
- In class C, three octets are used to indent the network. This IP ranges between 192 to 223.
- Class D addresses are 32-bit network addresses. All the values within the range are used to identify multicast groups uniquely.
- Class E IP address is defined by including the starting four network address bits as 1.
- Important rule for assigning network id is that the network ID cannot start with 127 as this number belongs to class A address and reserved for internal loopback functions.

Unicast:

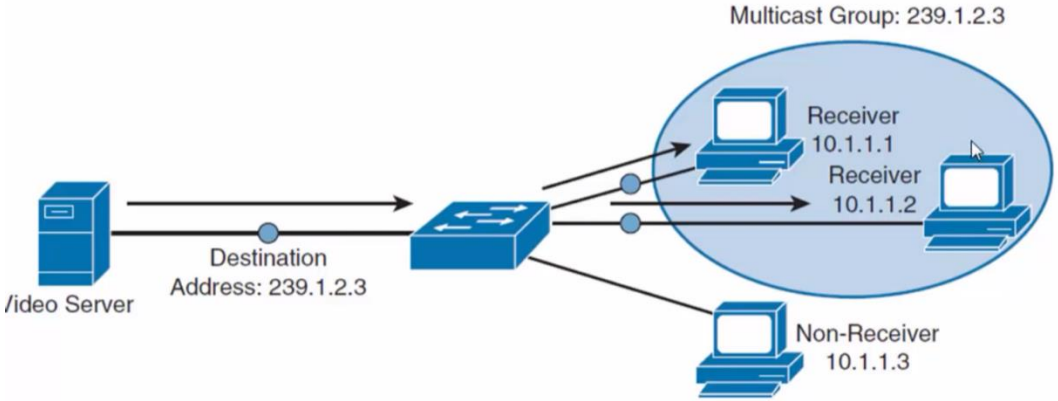
This type of information transfer is useful when there is a participation of a single sender and a single recipient. So, in short, you can term it a one-to-one transmission.
For example, if a device having IP address 10.1.2.0 in a network wants to send the traffic stream(data packets) to the device with IP address 20.12.4.2 in the other network, then unicast comes into the picture. This is the most common form of data transfer over networks.





Multicast:

In multicasting, one/more senders and one/more recipients participate in data transfer traffic. In this method traffic recline between the boundaries of unicast (one-to-one) and broadcast (one-to-all). Multicast lets servers direct single copies of data streams that are then simulated and routed to hosts that request it. IP multicast requires the support of some other protocols like **IGMP (Internet Group Management Protocol), Multicast routing** for its work. Also in Classful IP addressing **Class D** is reserved for multicast groups.

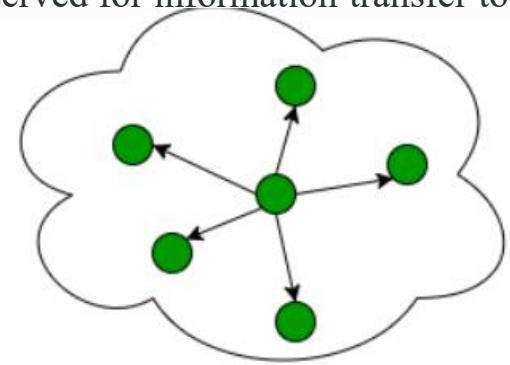


In IPv6 networks, multicast addresses have a prefix of ff00::/8.

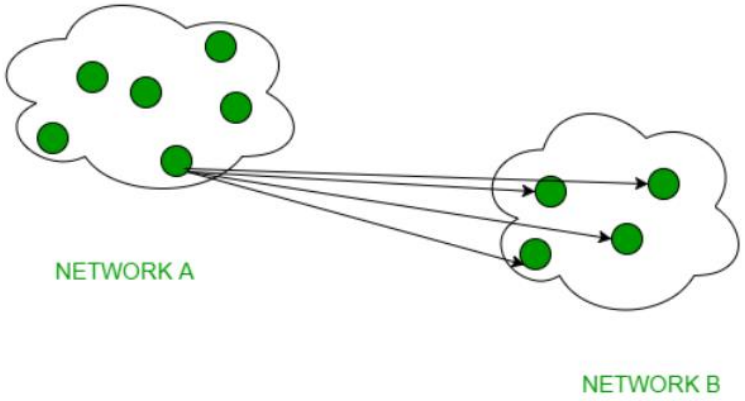
Broadcast:

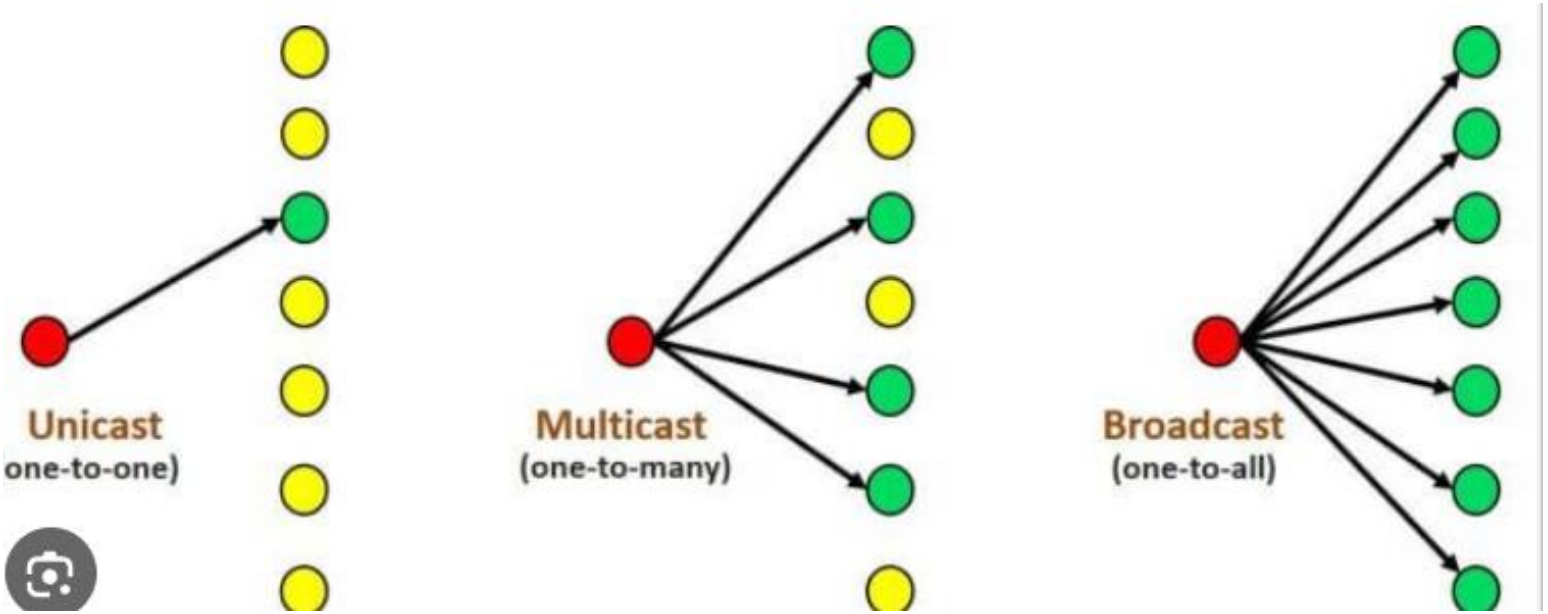
Broadcasting transfer (one-to-all) techniques can be classified into two types:

Limited Broadcasting: Suppose you have to send a stream of packets to all the devices over the network that your reside, this broadcasting comes in handy. For this to achieve, it will append 255.255.255.255 (all the 32 bits of IP address set to 1) called **Limited Broadcast Address** in the destination address of the datagram (packet) header which is reserved for information transfer to all the recipients from a single client (sender) over the network.



Direct Broadcasting: This is useful when a device in one network wants to transfer packet stream to all the devices over the other network. This is achieved by translating all the Host ID part bits of the destination address to 1, referred to as **Direct Broadcast Address** in the datagram header for information transfer.




Unicast
one-to-one)
Multicast
(one-to-many)
Broadcast
(one-to-all)

Subnet Mask

A subnet mask is used in a process known as subnetting, in which a large network is divided into smaller networks.

A subnet mask is used to determine the network address and host address:

Class	Default Subnet mask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

In simple words, the subnet mask tells, how many bits in the IP address are used as the network address and how many bits are left for the host address.

IP addresses are always written with the subnet mask.

Examples of IP addresses

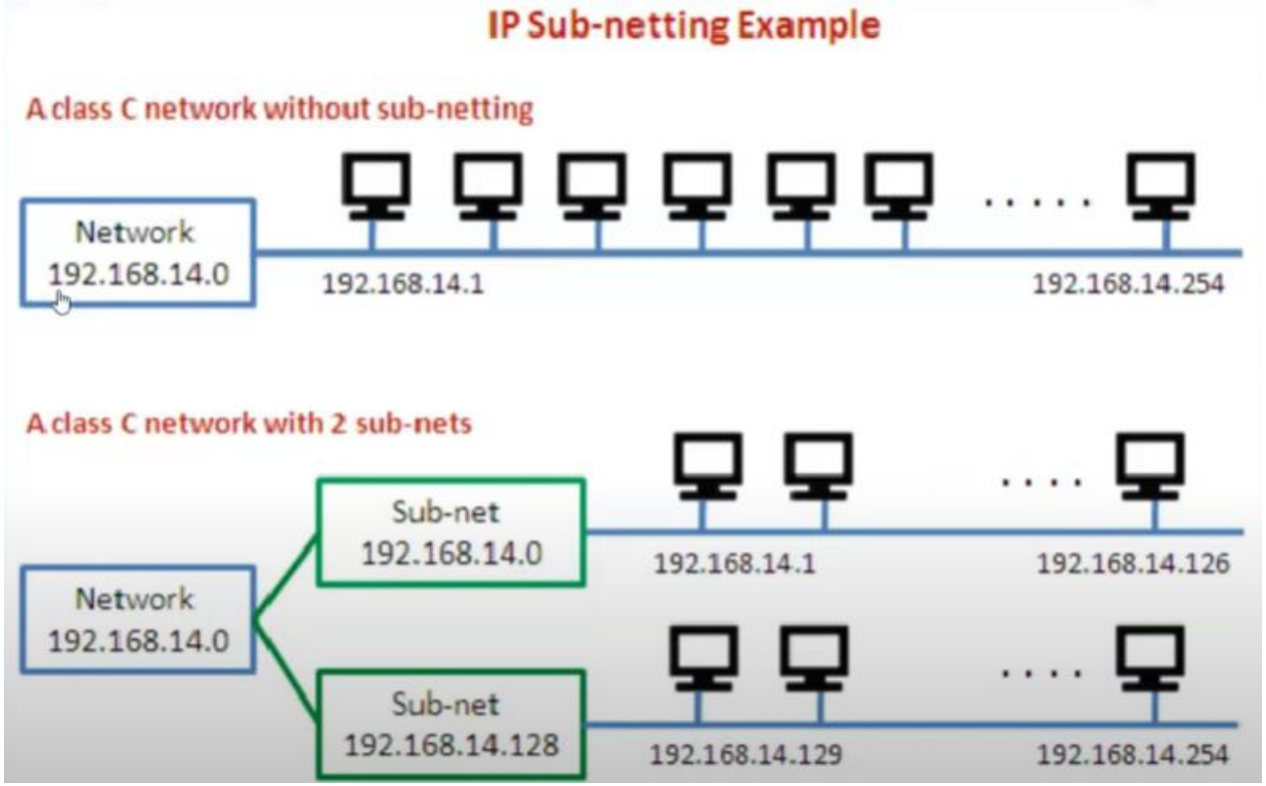
Decimal notation	Binary notation
1.2.3.4 255.0.0.0	00000001.00000010.00000011.00000100 11111111.00000000.00000000.00000000
168.172.1.1 255.255.0.0	10101000.10101100.00000001.00000001 11111111.11111111.00000000.00000000
210.20.30.40 255.255.255.0	11010010.00010100.00011110.00101000 11111111.11111111.11111111.00000000

Examples of class C IP addresses are the following.

Decimal notation	Binary notation
192.168.1.1 255.255.255.0	11000000.10101000.00000001.00000001 11111111.11111111.11111111.00000000
210.20.30.40 255.255.255.0	11010010.00010100.00011110.00101000 11111111.11111111.11111111.00000000
216.123.145.16 255.255.255.0	11011000.01111011.10010001.00010000 11111111.11111111.11111111.00000000
220.86.76.43 255.255.255.0	11011100.01010110.01001100.00101011 11111111.11111111.11111111.00000000
220.60.80.100 255.255.255.0	11011100.00111100.01010000.01100100 11111111.11111111.11111111.00000000

SUBNETTING

- ★ A subnetwork or subnet is a logical subdivision of an IP network.
- ★ The practice of dividing a network into two or more networks is called subnetting.
- ★ Computers that belong to a subnet are addressed with an identical most-significant bit-group in their IP addresses.



Uses of Subnetting

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

The reasons to use subnetting are:

- Conservation of IP addresses
- Reduced network traffic
- Simplified troubleshooting

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.

Subnet	1	2	4	8	16	32	64	128	256
Host	256	128	64	32	16	8	4	2	1

Subnetting – 5 Steps

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

192.168.50.0 /24 = 1 network of 256 hosts (minus the network and the broadcast

or

/25 (255.255.255.128) = 2 subnets of 128 hosts (minus 2)

or

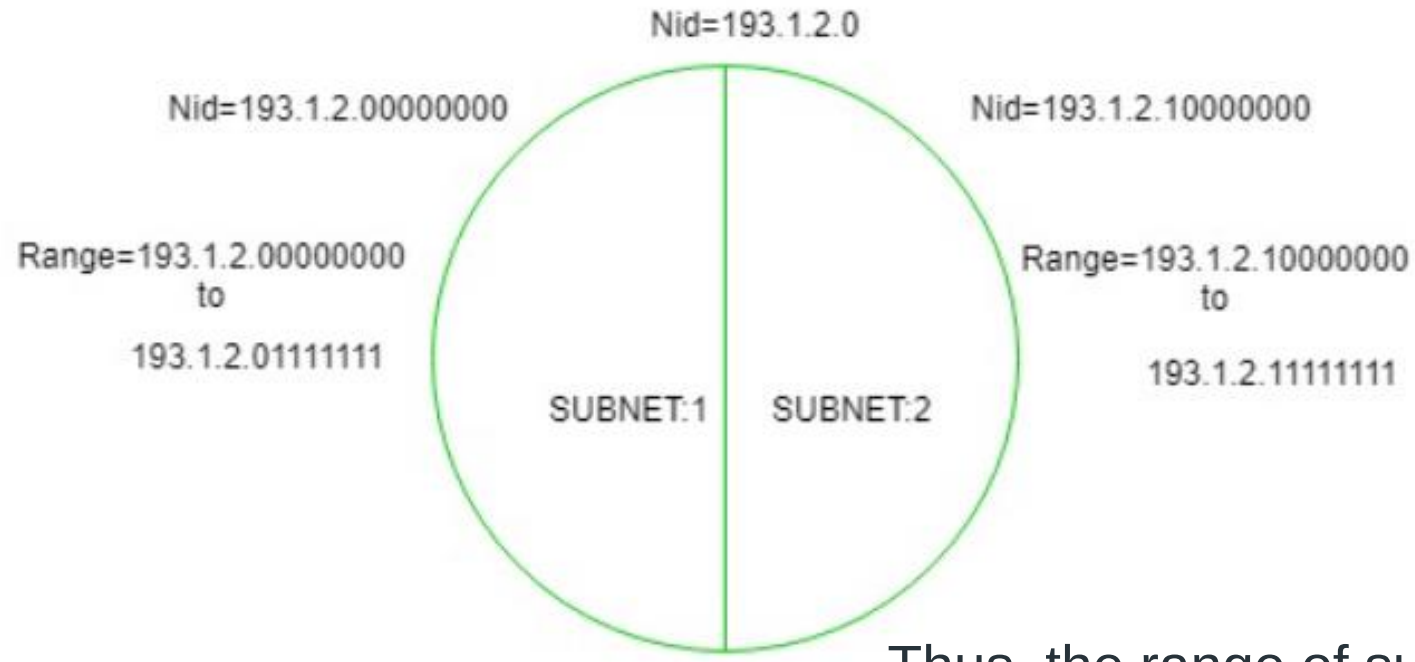
/26 (255.255.255.192) = 4 subnets of 64 hosts (minus 2)

or

/27 (255.255.255.224) = 8 subnets of 32 hosts (minus 2)

or

/28 (255.255.255.240) = 16 subnets of 16 hosts (minus 2)



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

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.

QUESTION

Subnet the IP address 216.21.5.0 into 30 hosts in each subnet.

SOLUTION

1. Class C – Default Subnet Mask: 255.255.255.0

2. 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 0 0 0 0 0 0 0 0

3. No. of hosts/subnet: 30 (11110) – 5 bits SG: 32 Octet Position: 4

   1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 0 0 0 0 0

4. New subnet mask: 255.255.255.224 or /27

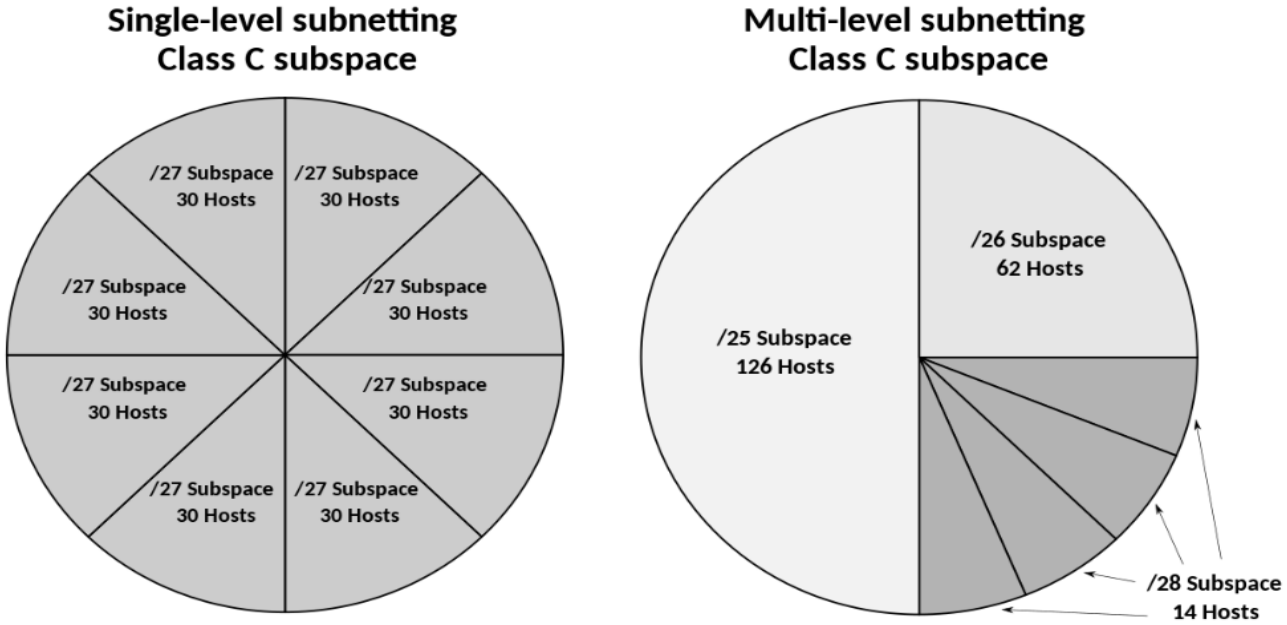
5. Network Ranges (Subnets)

   216.21.5.0 – 216.21.5.31
   216.21.5.32 – 216.21.5.63
   216.21.5.64 – 216.21.5.95
   216.21.5.96 – 216.21.5.127
   216.21.5.128 – 216.21.5.159
   and so on....

FLSM vs VLSM:

FLSM stands for Full Length Subnet Mask. It means all the subnets are of the same size. In FLSM, the subnet mask remains the same for all the subnets. FLSM creates subnets of the same size and an equal number of host identifiers

VLSM stands for Variable Length Subnet Mask. It means the size of the subnet varies according to the needs. In VLSM, the subnet mask is different normally but it can be same for any two or more subnets depending upon the situation.



FLSM:

Q. Suppose you are network administrator with provided network 172.16.0.0/24. You need to manage the entire n/w by dividing into subnetworks so that each of the Development, Sales, Reception, HR and Production. How would you do so?

VLSM: Example. An administrator has 192.168.1.0/24 network. The administrator has three different departments with different number of hosts. Sales department has 100 computers, Purchase department has 50 computers, Accounts has 25 computers and Management has 5 computers; the subnets are of fixed size. Calculate the network id, subnet mask, No. of usable host, host range, broadcast address.

Solution:

1. Allocate the highest range of IPs to the highest requirement, so let's assign 192.168.1.0 /25 (255.255.255.128) to the Sales department. This IP subnet with Network number 192.168.1.0 has 126 valid Host IP addresses which satisfy the requirement of the Sales department. The subnet mask used for this subnet has 10000000 as the last octet.

2. Allocate the next highest range, so let's assign 192.168.1.128 /26 (255.255.255.192) to the Purchase department. This IP subnet with Network number 192.168.1.128 has 62 valid Host IP Addresses which can be easily assigned to all the PCs of the Purchase department. The subnet mask used has 11000000 in the last octet.

3. Allocate the next highest range, i.e. Accounts. The requirement of 25 IPs can be fulfilled with 192.168.1.192 /27 (255.255.255.224) IP subnet, which contains 30 valid host IPs. The network number of Accounts department will be 192.168.1.192. The last octet of subnet mask is 11100000.

4. Allocate the next highest range to Management. The Management department contains only 5 computers. The subnet 192.168.1.224 /29 with the Mask 255.255.255.248 has exactly 6 valid host IP addresses. So, this can be assigned to Management. The last octet of the subnet mask will contain 11111000.

VLSM subnetting:

The given network address is: 192.168.1.0/24

Given requirement in descending order is:

Sales 100

Purchase 50

Accounts 25

Management 5

The complete range of the address in the above provided network is:

192.168.1.0 to 192.168.1.255

Divide the given network consisting 256 hosts into 2 networks with 128 hosts each:

192.168.1.0-192.168.1.127 (192.168.1.0/25)

192.168.1.128-192.168.1.255 (192.168.1.128/25)

The largest network requirement is of 100 hosts for Sales department. For this, we need to assign subnetwork with 128 hosts.

Let us assign the first divided subnetwork 192.168.1.0/25 to Sales Department.

We now have remaining subnetwork 192.168.1.128/25.

Dividing this subnetwork, two subnetworks with 64 hosts each are formed.

192.168.1.128 to 192.168.1.191 (192.168.1.128/26)

192.168.1.192 to 192.168.1.255 (192.168.1.192/26)

Our second network requirement is of 50 hosts for Purchase department. We need to assign subnetwork consisting of 64 hosts.

Assigning 192.168.1.128/26 to Purchase department.

The remaining subnetwork available is 192.168.192/26.

Dividing this subnetwork, two subnetworks with 32 hosts each are formed.

192.168.1.192 to 192.168.1.223 (192.168.1.192/27)
192.168.1.224 to 192.168.1.255 (192.168.1.224/27)
The third largest requirement is of 25 hosts for Account department.
Assigning 192.168.1.192/27 to Account Department.

Remaining subnetwork is 192.168.1.224/27

Dividing this subnetwork, two subnetworks with 16 hosts each are formed.
192.168.1.224 to 192.168.1.239 (192.168.1.224/28)
192.168.1.240 to 192.168.1.255 (192.168.1.240/28)
Our fourth network requirement is of 5 hosts for Management department. We need to assign subnetwork consisting of 8 hosts, which is sufficient.
So, again dividing the subnetwork 192.168.1.240/28, two subnetworks with 8 hosts each are formed.

192.168.1.240 to 192.168.1.247 (192.168.1.240/29)
192.168.1.248 to 192.168.1.255 (192.168.1.248/29)
Our fourth network requirement is of 5 hosts for Management department. We need to assign subnetwork consisting of 8 hosts.

Summarizing the subnetting results,

Network Name	Network ID	Subnet mask	No. of usable hosts	Usable Host ID Range	Broadcast address
Sales	192.168.1.0	/25	126	192.168.1.1 to 192.168.1.126	192.168.1.127
Purchase	192.168.1.128	/26	62	192.168.129 to 192.168.1.190	192.168.1.191
Account	192.168.1.192	/27	30	192.168.1.193 to 192.168.1.222	192.168.1.223
Management	192.168.1.240	/29	6	192.168.1.241 to 192.168.1.246	192.168.1.247
Unused	192.168.1.224/28 (192.168.1.224 to 192.168.1.239)				
Unused	192.168.1.247/29 (192.168.1.247 to 192.168.1.255)				

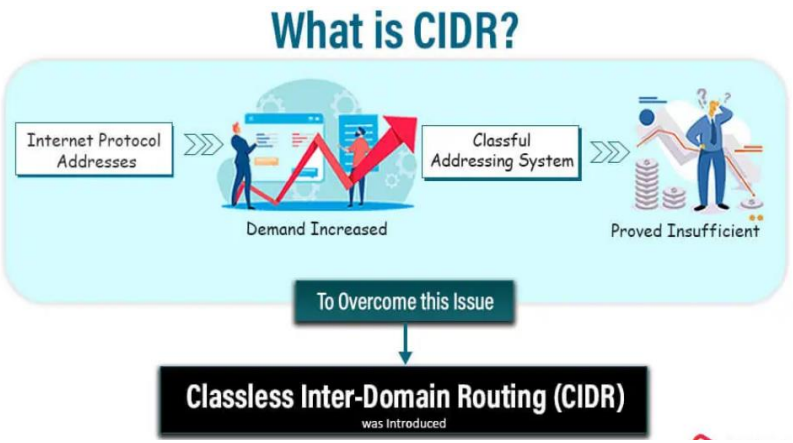
Classless Inter-Domain Routing (CIDR):

Classless Inter-Domain Routing (CIDR) is an IP address allocation method that improves data routing efficiency on the internet. Every machine, server, and end-user device that connects to the internet has a unique number, called an IP address, associated with it.

It is an IP address assigning method that improves the efficiency of address distribution. It is also known as supernetting that replaces the older system based on classes A, B, and C networks.

By using a single CIDR IP address many unique IP addresses can be designated. CIDR IP address is the same as the normal IP address except that it ends with a slash followed by a number.

172.200.0.0/16 It is called IP network prefix.



Supernetting is a technique for combining multiple smaller network addresses into a single larger network address. Doing it allows more efficient routing and reduces the size of the routing table.

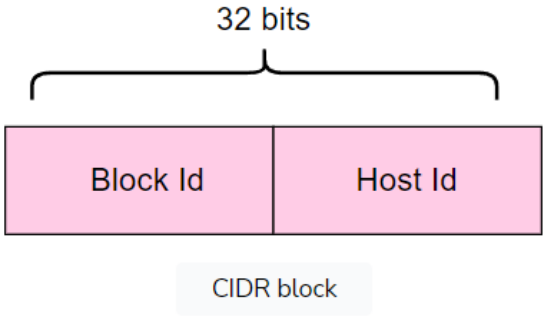
Classless Addressing in IP Addressing

Classless addressing, also called **Classless Inter-Domain Routing (CIDR)**, is an improved IP addressing system. It increases the effectiveness of IP address allocation because of the absence of class distribution.

Structure

The CIDR block comprises two parts. These are as follows:

- Block id is used for the network identification, but the number of bits is not pre-defined as it is in the classful IP addressing scheme.
- Host id is used to identify the host part of the network.



Notation

CIDR IP addresses as follows:

w.x.y.z/n

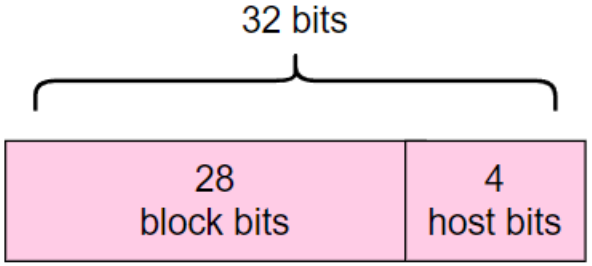
In the example above, *w,x,y,z* each defines an 8-bit binary number, while *n* tells us about the number of bits used to identify the network and is called an **IP network prefix** or **mask**.

Block information

Given the following IP address, let's find the network and host bits.

200.56.23.41/28

The following illustration gives a clear understanding of the aforementioned IP address scheme:



CIDR block with block and host ids' bits

To find the network and host bits, we will use the stated formula, where b represents the number of hosts in the network.

$$n_h = 2^{32-n}$$

This particular case, in which n equals 28, represents the block id bits, so subtracting it with 32 leaves us with the total number of hosts expected in the network.

$$n_h = 2^{32-28}$$

$$n_h = 2^4$$

Benefits

Following are the benefits of classless IP addressing:

- Efficient IP address allocations.
- More balanced use of IP address ranges.
- More efficient routing.

Characteristics of CIDR

It dynamically allocates the IP addresses by using CIDR blocks on the requirement of the user based on certain rules.

The assignment of the CIDR block is handled by the Internet Assigned Number Authority (IANA).

CIDR block consists of IP addresses and it consists of some rules:

1. All IP addresses which are allocated to host must be continuous.
2. The block size must be of power 2 and equal to the total number of IP addresses.
3. The size of the block must be divisible by the first IP address of the block.

Example: If the Block size is 2^5 then, Host Id will contain 5 bits and Network will contain 32 – 5 = 27 bits. First IP address of the Block must be evenly divisible by the size of the block. in simple words, the least significant part should always start with zeroes in Host Id.

The **Internet Assigned Numbers Authority** (**IANA**) is a standards organization that oversees global IP address allocation, autonomous system number allocation, root zone management in the Domain Name System (DNS), media types, and other Internet Protocol–related symbols and **Internet numbers**.

Example: The IP address range is from 21.19.35.64 and 21.19.35.127. Find the CIDR block?

The IP address ranges are from 21.19.35.64 and 21.19.35.127.

Before proceeding further, the CIDR block rules mentioned above should be checked if they are satisfied; then, it is a CIDR block.

So the size of the block is 2^{6}. (i.e., 127 – 64 + 1 = 64)

Number of bits = 32 – 6 = 26.

CIDR block is 21.19.35.64/26.

Example: The representation is 255.255.255.255/31. Find the IP addresses of the CIDR block?

31 represents the number of bits used for the identification of the network.

The 1-bit is used for the identification of hosts.

The CIDR address is 255.255.255.255/31.

The first IP address is 255.255.255.254.

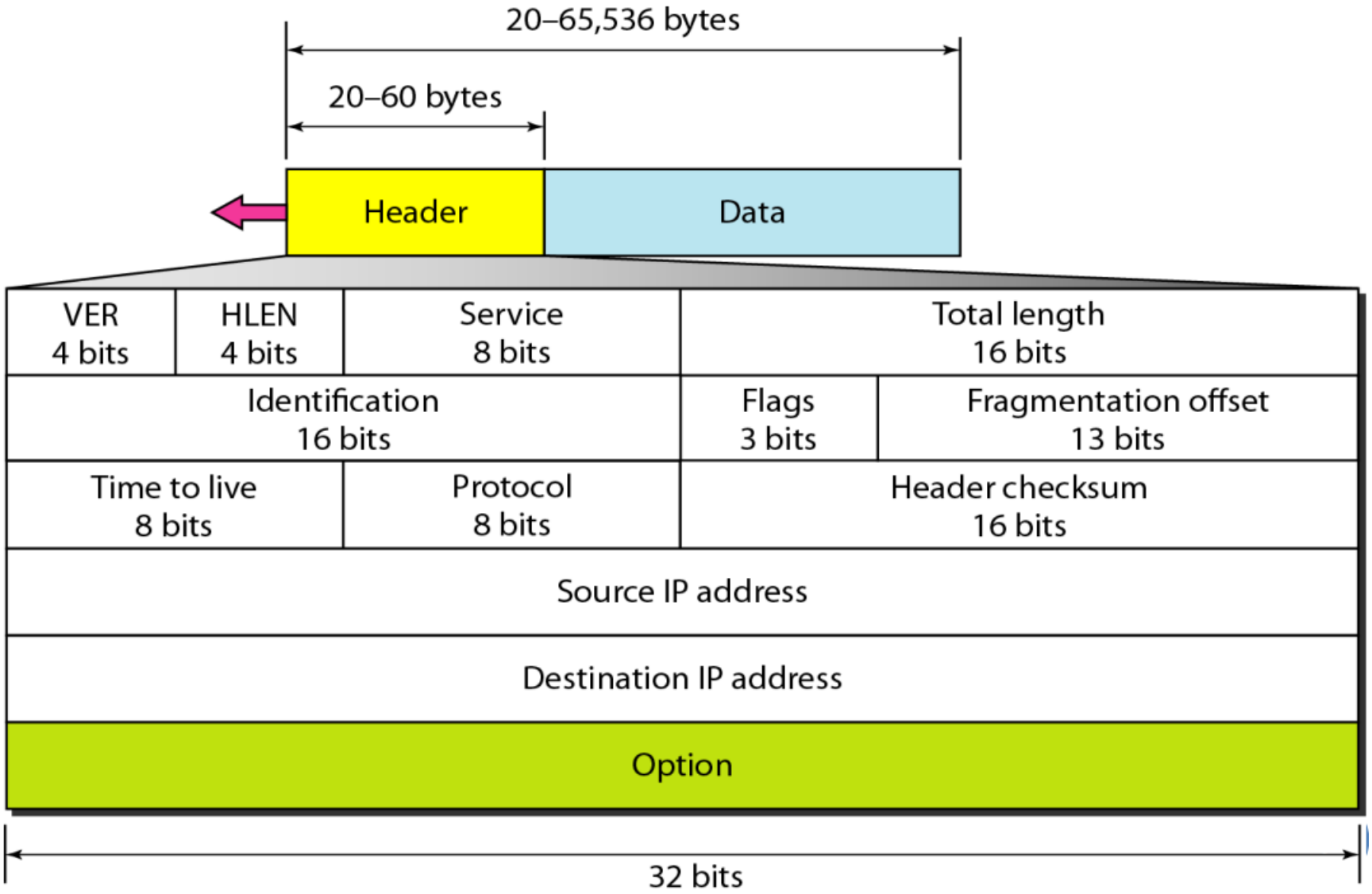
The last IP address is 255.255.255.255.

The total cost is 2.

Netmask is 255.255.255.254.

Q. If you are assigned an IP address 92.16.1.0/24 and plans to deploy CIDR. Here are some requirements which you have to fulfill for Subnet A= 120 hosts, Subnet B=60 hosts, Subnet C=30 hosts, Subnet D= 10 hosts, Subnet E= 5. You are also required to calculate subnet mask, range, netid, broadcast id for each subnet.

IPv4 Header Format:



1. Version: This 4-bit field defines the version of the IP protocol. Currently the version is 4.

2. Header Length: This 4-bit field defines the total length of the datagram header in 4-byte words. This field is needed because the length of the header is variable (between 20 and 60 bytes).

3. Service Type: In the original design of IP header, this field was referred to as type of service (TOS) , which defined how the datagram should be handled.

4. Total Length (16 bits): Total length of the datagram, measured in octets, including header and data.

5. Identification (16 bits): A value assigned to aid in assembly of fragments.

6. Flags (3 bits): Various Control Flags.

7. Bit 0: Reserved. Must be 0.

8. Bit 1: (DF) 0 = May Fragment, 1 = Don't Fragment

9. Bit 2: (MF) 0 = Last Fragment, 1 = More Fragments

10. Time to Live (8 bits): Maximum time the datagram is allowed to exist in the system. Each router that handles the datagram decrements the TTL by 1.

11. Protocol: This 8-bit field defines the higher-level protocol that uses the services of the IP layer. An IP datagram can encapsulate data from several higher level protocols such as TCP, UDP, ICMP, and IGMP.

12. Checksum: It is used to detect error in the delivery of packet.

13. Source address: This 32-bit field defines the IP address of the source.

14. Destination address: This 32-bit field defines the IP address of the destination.

15. IP Option: this field is not used often, is optional and has a variable length based on the options that were used. When you use this field, the value in the header length field will increase. An example of a possible option is “source route” where the sender requests for a certain routing path.

EXAMPLE:

An IPv4 packet has arrived with the first 8 bits as shown:

01000010

The receiver discards the packet. Why?

Solution

There is an error in this packet. The 4 leftmost bits (0100) show the version, which is correct. The next 4 bits (0010) show an invalid header length ($2 \times 4 = 8$). The minimum number of bytes in the header must be 20. The packet has been corrupted in transmission.

Disadvantage of Classful Addressing:

In classful addressing, a large part of the available addresses were wasted.

Class A with a mask of 255.0.0.0 can support 128 Network, 16,777,216 addresses per network and a total of 2,147,483,648 addresses.
Class B with a mask of 255.255.0.0 can support 16,384 Network, 65,536 addresses per network and a total of 1,073,741,824 addresses.
Class C with a mask of 255.255.255.0 can support 2,097,152 Network, 256 addresses per network and a total of 536,870,912 addresses.

IPv4	IPv6
IPv4 has a 32-bit address length	IPv6 has a 128-bit address length
It Supports Manual and DHCP address configuration	It supports Auto and renumbering address configuration
It can generate 4.29×10^9 address space	The address space of IPv6 is quite large it can produce 3.4×10^{38} address space
The Security feature is dependent on the application	IPSEC is an inbuilt security feature in the IPv6 protocol
Address representation of IPv4 is in decimal	Address Representation of IPv6 is in hexadecimal
Fragmentation performed by Sender and forwarding routers	In IPv6 fragmentation is performed only by the sender
In IPv4 Packet flow identification is not available	In IPv6 packet flow identification are Available and uses the flow label field in the header
In IPv4 checksum field is available	In IPv6 checksum field is not available
It has a broadcast Message Transmission Scheme	In IPv6 multicast and anycast message transmission scheme is available
In IPv4 Encryption and Authentication facility not provided	In IPv6 Encryption and Authentication are provided
IPv4 has a header of 20-60 bytes.	IPv6 has a header of 40 bytes fixed
IPv4 can be converted to IPv6	Not all IPv6 can be converted to IPv4
IPv4 consists of 4 fields which are separated by addresses dot (.)	IPv6 consists of 8 fields, which are separated by a colon (:)
IPv4's IP addresses are divided into five different classes. Class A , Class B, Class C, Class D , Class E.	IPv6 does not have any classes of the IP address.

Internet Protocol version 6 (IPv6)

IPv6 is a 128-bits address having an address space of 2^{128}, which is way bigger than IPv4. IPv6 use Hexa-Decimal format separated by colon (:) . Notably, IPv6 has drastically increased address space compared to IPv4.

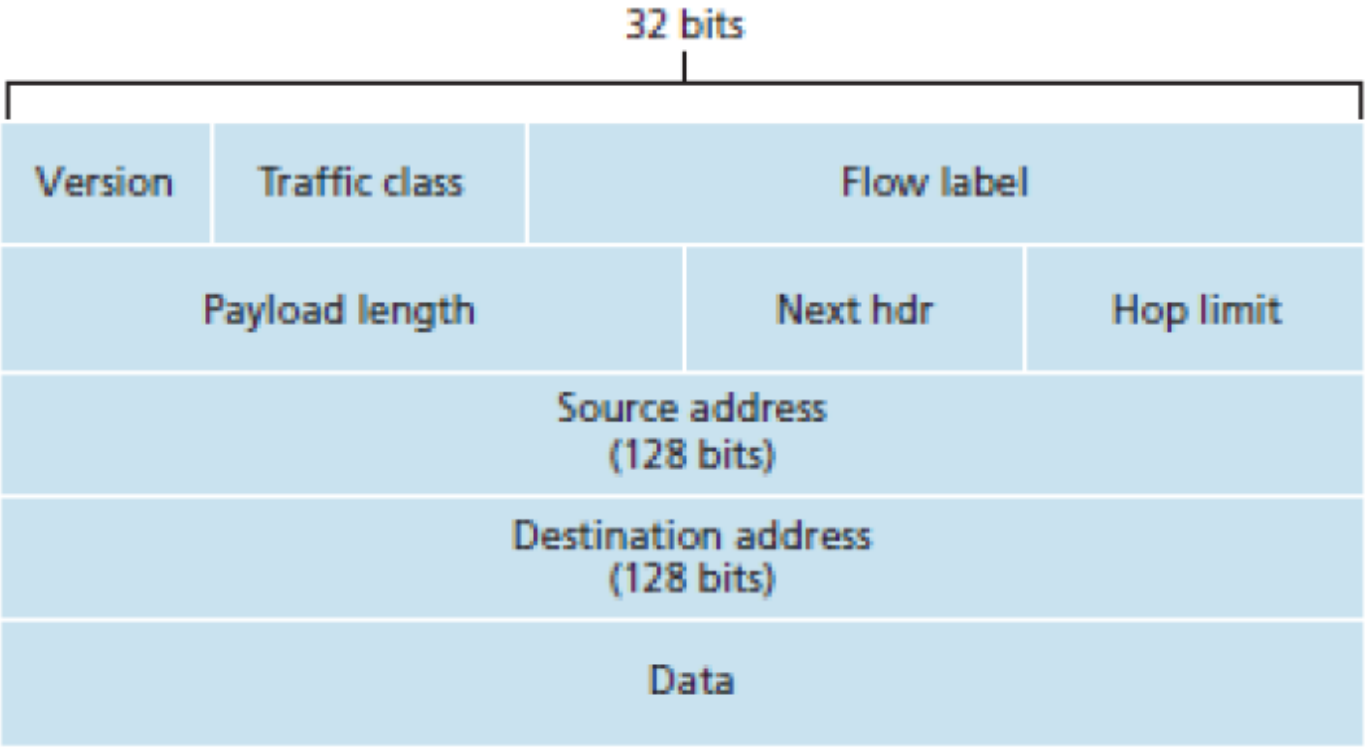
Format of an IPv6 address

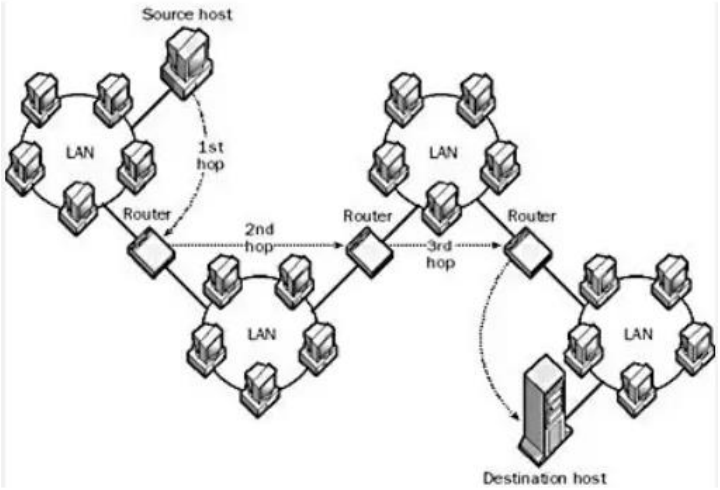
An IPv6 address is 128 bits long and is arranged in eight groups, each of which is 16 bits. Each group is expressed as four hexadecimal digits and the groups are separated by colons.

An example of a full IPv6 address could be:
FE80:CD00:0000:0CDE:1257:0000:211E:729C

An IPv6 address is split into two parts: a network and a node component. The network component is the first 64 bits of the address and is used for routing. The node component is the later 64 bits and is used to identify the address of the interface.

Internet Protocol version 6 (IPv6) Header

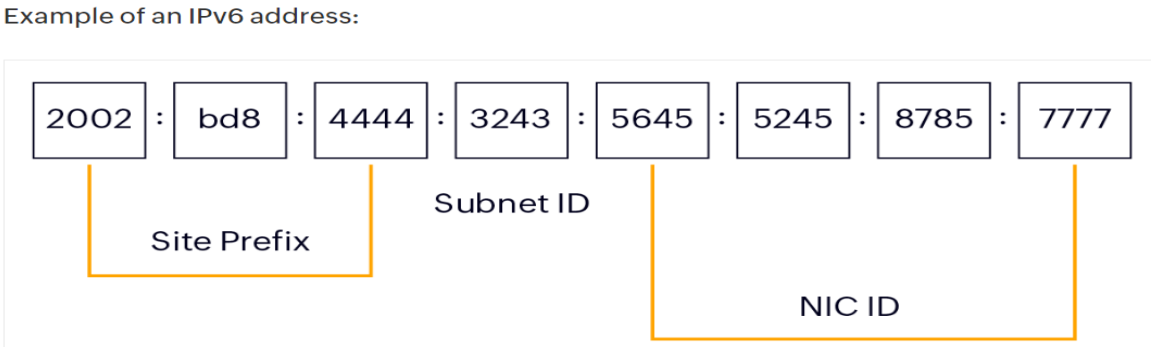




S.N.	Field & Description
1	Version (4-bits): It represents the version of Internet Protocol, i.e. 0110
2	Traffic Class (8-bits): These 8 bits are divided into two parts. The most significant 6 bits are used for Type of Service to let the Router know what services should be provided to this packet. The least significant 2 bits are used for Explicit Congestion Notification (ECN).
3	Flow Label (20-bits): This label is used to maintain the sequential flow of the packets belonging to a communication. The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information.
4	Payload Length (16-bits): This field is used to tell the routers how much information a particular packet contains in its payload. Payload is composed of Extension Headers and Upper Layer data.

5	Next Header (8-bits): This field is used to indicate either the type of Extension Header, or if the Extension Header is not present, then it indicates the Upper Layer PDU.
6	Hop Limit (8-bits): This field is used to stop packet to loop in the network infinitely. This is same as TTL in IPv4. The value of Hop Limit field is decremented by 1 as it passes a link (router/hop). When the field reaches 0, the packet is discarded.
7	Source Address (128-bits): This field indicates the address of originator of the packet.
8	Destination Address (128-bits): This field provides the address of intended recipient of the packet.

Three basic parts that make up the address are the routing prefix, the subnet ID and the interface ID.



Both the routing prefix and the subnet ID represent two main levels in which the address is constructed -- either global or site-specific. The routing prefix is the number of bits that can be subdivided -- typically, decided by Internet Registries and Internet Service Providers (ISPs). In IPv6 address, the leftmost set of numbers -- the first 48 bits -- is called the site prefix. The subnet ID is the next 16 bits. The subnet ID lays out site topology. The last 64-bits are called the interface ID, which can be automatically or manually configured.

Types of IPv6 addresses

There are different types and formats of IPv6 addresses, of which, it's notable to mention that there are no broadcast addresses in IPv6. Some examples of IPv6 formats include:

- **Global unicast.** These addresses are routable on the internet and start with "2001:" as the prefix group. Global unicast addresses are the equivalent of IPv4 public addresses.
- **Unicast address.** Used to identify the interface of an individual node.
- **Anycast address.** Used to identify a group of interfaces on different nodes.
- **Multicast address.** An address used to define Multicast Multicasts are used to send a single packet to multiple destinations at one time.
- **Link local addresses.** One of the two internal address types that are not routed on the internet. Link local addresses are used inside an internal network, are self-assigned and start with "fe80:" as the prefix group.
- **Unique local addresses.** This is the other type of internal address that is not routed on the internet. Unique local addresses are equivalent to the IPv4 addresses 10.0.0.0/8, 172.16.0.0/12 and 192.168.0.0/16.

Advantages and disadvantages of IPv6 addresses

IPv6 addresses can bring a variety of benefits, including:

- More efficient routing with smaller routing tables and aggregation of prefixes.
- Simplified packet processing due to more streamlined packet headers.
- Support of multicast packet flows.
- Hosts can generate their own IP addresses.
- Eliminates the need for network address translation (NAT).
- Easier to implement services like peer-to-peer (P2P) networks, voice over IP (VoIP) and stronger security.

IPv6 also still uses the same two families of routing protocols – Interior Gateway Protocol (IGP) and Exterior Gateway Protocol (EGP).