UNIT-III

POINT TO POINT NETWORKS

A Point to Point Network is a private data connection securely connecting two or more locations for private data services. A point to point network is a closed network data transport service which does not traverse the public Internet and is inherently secure with no data encryption needed. Point to Point connections are available in a range of a bandwidth speeds from 10Mbps to 100Gbps. A point to point connection provides unparalleled quality of service (QoS) as it is not a shared service (a private line) and follows the same direct network path every time. Point to Point links are used by businesses to provide reliable, secure point to point network data service for applications including credit card processing, file sharing, data backup, VOIP, and video conferencing. A point to point network can also be configured to carry voice, video, Internet, and data services together over the same point to point connection. Point to Point circuits are also known as a **Point to Point Link**, **Wavelength**, **Private Line**, **Leased Line**, or **Data Line**.

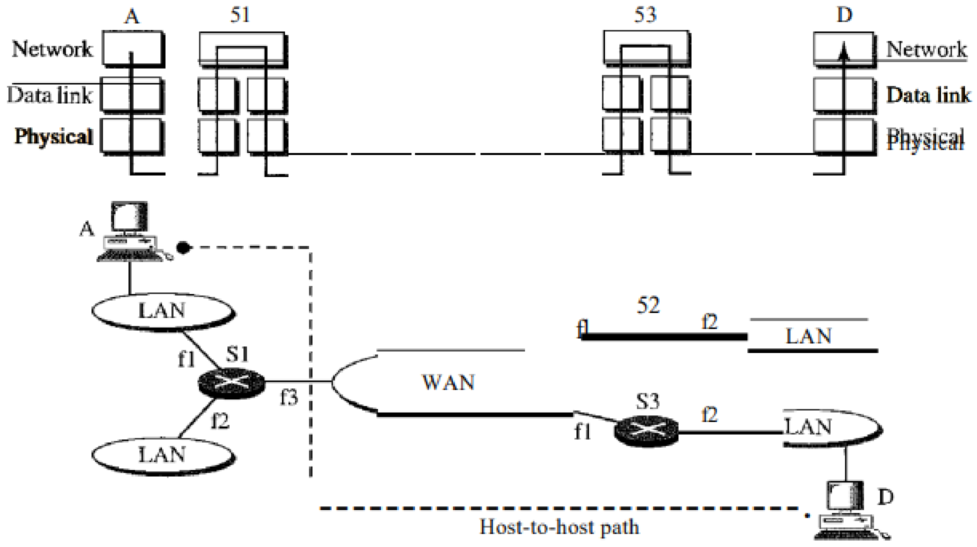
INTERNETWORKING

The physical and data link layers of a network operate locally. These two layers are jointly responsible for data delivery on the network from one node to the next, as shown in Figure 20.1. This internetwork is made of five networks: four LANs and one WAN. If host A needs to send a data packet to host D, the packet needs to go first from A to Rl (a switch or router), then from Rl to R3, and finally from R3 to host D. We say that the data packet passes through three links. In each link, two physical and two data link layers are involved. However, there is a big problem here. When data arrive at interface fl of Rl, how does RI know that interface f3 is the outgoing interface? There is no provision in the data link (or physical) layer to help Rl make the right decision. The frame does not carry any routing information either. The frame contains the MAC address of A as the source and the MAC address of Rl as the destination. For a LAN or a WAN, delivery means carrying the frame through one link, and not beyond

Need for Network Layer

To solve the problem of delivery through several links, the network layer (or the internetwork layer, as it is sometimes called) was designed. The network layer is responsible for host-to-host delivery and for routing the packets through the routers or switches. Figure 20.2 shows the same internetwork with a network layer added.

Figure 20.2 *Network layer in an internetwork*



SCTP

SCTP stands for Stream Control Transmission Protocol. It is a new reliable, messageoriented transport layer protocol. SCTP, however, is mostly designed for Internet applications that have recently been introduced. These new applications, such as IUA (ISDN over IP), M2UA and M3UA (telephony signaling), H.248 (media gateway control), H.323 (IP telephony), and SIP (IP telephony), etc.

SCTP combines the best features of UDP and TCP. SCTP is a reliable message-oriented protocol. It preserves the message boundaries, and at the same time, detects lost data, duplicate data, and out-of-order data. It also has congestion control and flows control mechanisms.

Features of SCTP

There are various features of SCTP, which are as follows −

Transmission Sequence Number

The unit of data in TCP is a byte. Data transfer in TCP is controlled by numbering bytes by using a sequence number. On the other hand, the unit of data in SCTP is a DATA chunk that may or may not have a one-to-one relationship with the message coming from the process because of fragmentation.

Stream Identifier

In TCP, there is only one stream in each connection. In SCTP, there may be several streams in each association. Each stream in SCTP needs to be identified by using a stream identifier (SI). Each data chunk must carry the SI in its header so that when it arrives at the destination, it can be properly placed in its stream. The 51 is a 16-bit number starting from O.

Stream Sequence Number

When a data chunk arrives at the destination SCTP, it is delivered to the appropriate stream and in the proper order. This means that, in addition to an SI, SCTP defines each data chunk in each stream with a stream sequence number (SSN).

Packets

In TCP, a segment carries data and control information. Data is carried as a collection of bytes; control information is defined by six control flags in the header. The design of SCTP is totally different: data is carried as data chunks; control information is carried as control chunks.

Flow Control

Like TCP, SCTP implements flow control to avoid overwhelming the receiver.

Error Control

Like TCP, SCTP implements error control to provide reliability. TSN numbers and acknowledgement numbers are used for error control.

Congestion Control

Like TCP, SCTP implements congestion control to determine how many data chunks can be injected into the network.

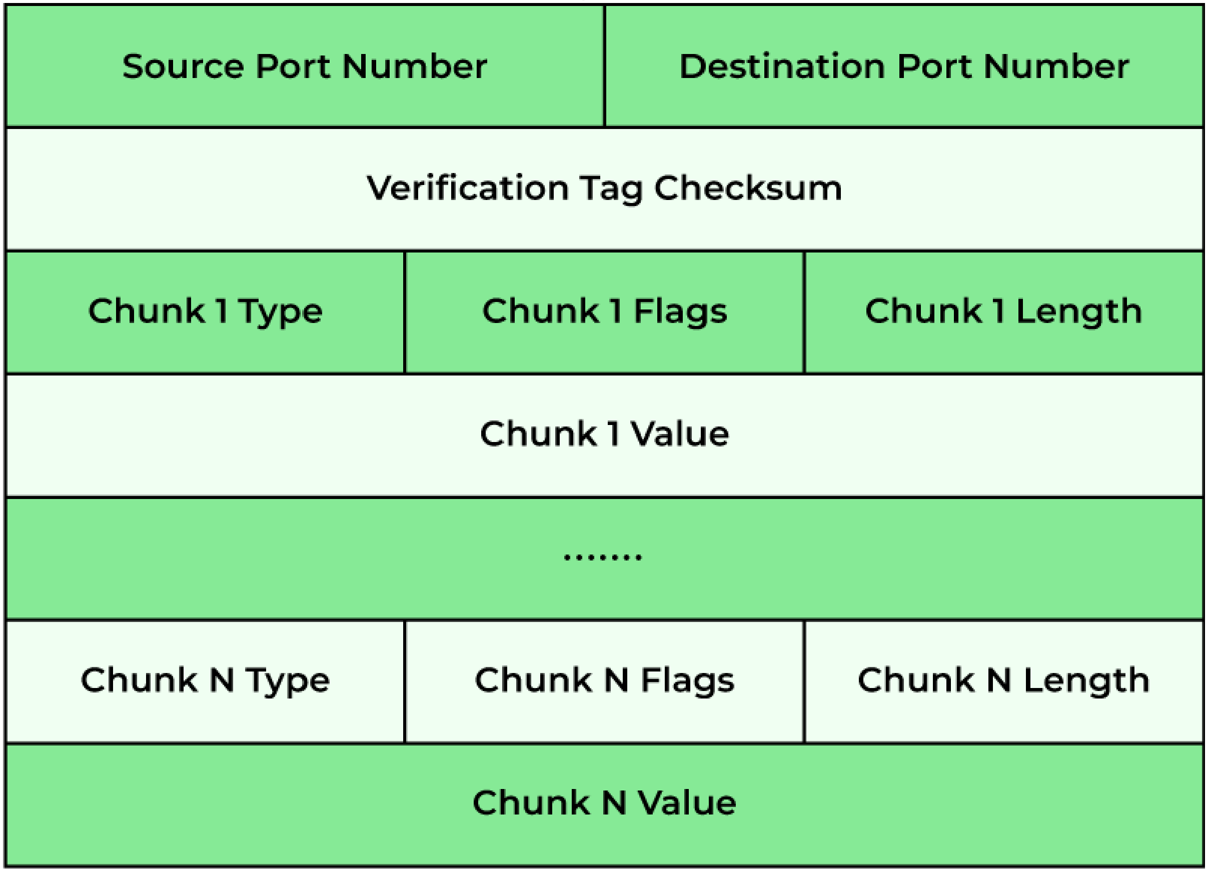
SCTP Packet Field

1. Transmission Sequence Number: In TCP(transmission control protocol) the unit of data is a **byte** because it is a byte-oriented protocol. Therefore TCP controls the data transfer by numbering bytes with the sequence numbers. However, the data unit in SCTP is a **Data chunk** and it may or may not have a one-to-one relationship with the messages produced by the sending process. (This happens due to fragmentation) .Therefore in SCTP, the data chunks are numbered with **transmission sequence number (TSN)** in order to control the data transfer. Each TSN is a unique 32-bit number which is stored in the header of the data chunk. TSN has a value between (2^32 – 1).

2. Stream Identifier (SI): In SCTP there is more than one stream in each association, and each such stream should be identified using a Stream Identifier (SI). The SI is a 16-bit number which starts from 0, and it is stored in the header of the Corresponding data chunk. This will help in placing the data chunk in its stream after receiving it at the destination. Thus SCTP uses SI to distinguish between different streams.

3. Stream Sequence Number(SSN): SCTP uses the stream sequence number (SSN) to distinguish between different data chunks which belong to the same stream. The received data chunk at the destination is delivered to the appropriate stream in proper order by the destination SCTP. This becomes possible as SCTP defines each data chunk in each stream with a stream sequence number (SSN) in addition to an SI.

4. Packets: The SCTP packet design is completely different from that of TCP. In SCTP, the data is carried in the form of data chunks while control information is carried as control chunks. The below figure shows the SCTP packet.



Source Port Number		Destination Port Number
Verification Tag Checksum		
Chunk 1 Type	Chunk 1 Flags	Chunk 1 Length
Chunk 1 Value		
....		
Chunk N Type	Chunk N Flags	Chunk N Length
Chunk N Value		

The role of an SCTP packet is the same as that of a TCP packet. In SCTP the control information is not a part of the header, but it is included in the control chunks. The control chunks are of different types. In SCTP the data is not treated as one entity. Instead, it is in the form of several data chunks, and each chunk can belong to a different stream. There is no option section in SCTP like TCP. We have to define new chunk types to handle options in SCTP.

The length of the general header in SCTP is 12 bytes as compared to 20 bytes in

TCP. The checksum length in SCTP is 32 bits as compared to 16 bits in TCP. The verification tag field in the SCTP packet is used as an association identifier. Each association is defined by a unique verification tag. We can have multihoming in SCTP by using different IP addresses. In an SCTP packet, several different data chunks will be present and each one is defined by TSN, IS and SSN. In SCTP, control information and data information are carried out in separate chunks. In SCTP the TSN, IS and SSN numbers (identifiers) are used only to identify the data chunks. The control chunks never use these three identifiers. In SCTP the data is contained in data chunks, streams and packets.

The relationship between these three is as follows :

- An association may send many **packets.**
- Each **packet** may contain many chunks.
- These chunks may belong to different **streams.**

5. Acknowledgement Number: In TCP the acknowledgement numbers are byte -oriented and they refer to the sequence numbers. But the acknowledgement numbers in SCTP are chunk-oriented, and they refer to the TSN. In SCTP, the control chunks carry the control information. The control chunks do not need the TSN. These control chunks are acknowledged by another appropriate type of control chunk. The sequence number or acknowledgement number is not necessary for the control chunks in SCTP.

IP ADDRESSES

Today, we use the term IP address to mean a logical address in the network layer of the TCP/IP protocol suite. The Internet addresses are 32 bits in length; this gives us a maximum of 232 addresses. These addresses are referred to as IPv4 (IP version 4) addresses or simply IP addresses if there is no confusion. The need for more addresses, in addition to other concerns about the IP layer, motivated a new design of the IP layer called the new generation of IP or IPv6 (IP version 6). In this version, the Internet uses 128-bit addresses that give much greater flexibility in address allocation. These addresses are referred to as IPv6 (IP version 6) addresses

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.

An IPv4 address is 32 bits long.

IPv4 addresses are unique. They are unique in the sense that each address defines one, and only one, connection to the Internet. Two devices on the Internet can never have the same address at the same time. We will see later that, by using some strategies, an address may be assigned to a device for a time period and then taken away and assigned to another device

On the other hand, if a device operating at the network layer has m connections to the Internet, it needs to have m addresses. We will see later that a router is such a device. The IPv4 addresses are universal in the sense that the addressing system must be accepted by any host that wants to be connected to the Internet.

The IPv4 addresses are unique and universal.

Address Space A protocol such as IPv4 that defines addresses has an address space. An address space is the total number of addresses used by the protocol. If a protocol uses N bits to define an address, the address space is 2^N because each bit can have two different values (0 or 1) and N bits can have 2^N values. IPv4 uses 32-bit addresses, which means that the address space is 232 or 4,294,967,296 (more than 4 billion). This means that, theoretically, if there were no restrictions, more than 4 billion devices could be connected to the Internet. We will see shortly that the actual number is much less because of the restrictions imposed on the addresses. The address space of IPv4 is 2^{32} or 4,294,967,296.

Notations There are two prevalent notations to show an IPv4 address: binary notation and dotted-decimal notation.

Binary Notation In binary notation, the IPv4 address is displayed as 32 bits. Each octet is often referred to as a byte. So it is common to hear an IPv4 address referred to as a 32-bit address or a 4-byte address. The following is an example of an IPv4 address in binary notation:

01110101 10010101 00011101 00000010

Dotted-Decimal Notation To make the IPv4 address more compact and easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separating the bytes. The following is the dotted~decimal notation of the above address:

117.149.29.2

Figure 19.1 shows an IPv4 address in both binary and dotted-decimal notation. Note that because each byte (octet) is 8 bits, each number in dotted-decimal notation is a value ranging from 0 to 255

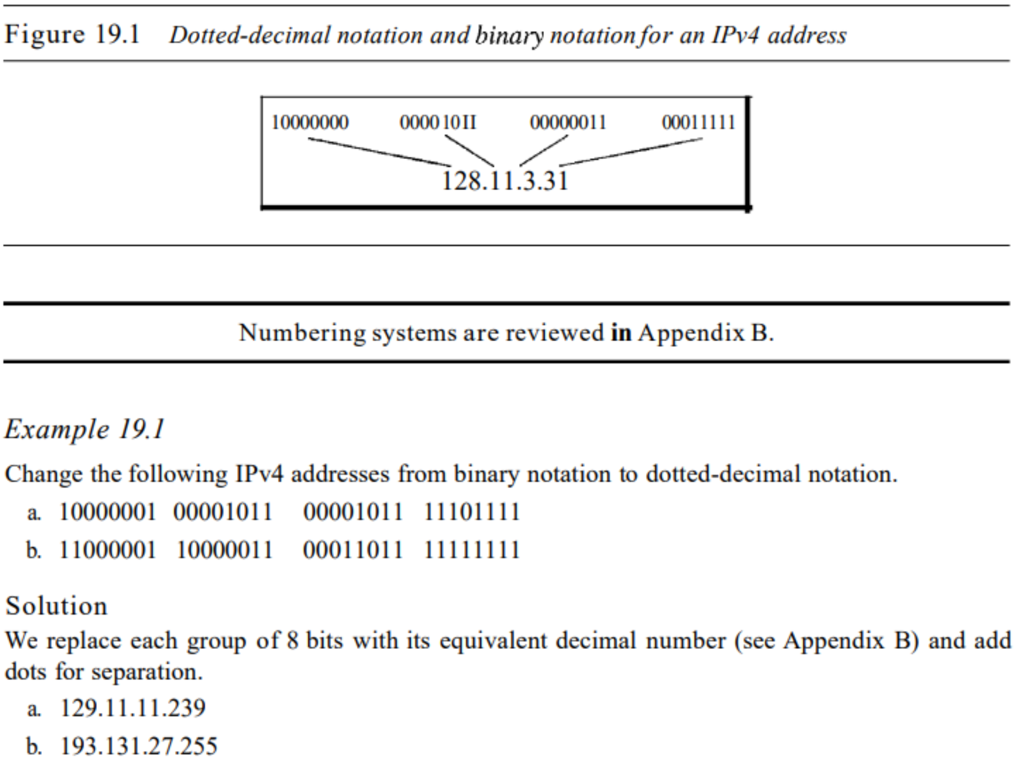


Figure 19.1 *Dotted-decimal notation and binary notation for an IPv4 address*

10000000
0000 10II
00000011
00011111
128.11.3.31

Numbering systems are reviewed **in** Appendix B.

Example 19.1

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

Classful vs Classless addressing

IPV4 Addresses, Classful Addressing, Classless Addressing, and the difference between Classful and Classless addressing are discussed in this article.

Let's first discuss about IPV4 addresses

IPV4 ADDRESSES

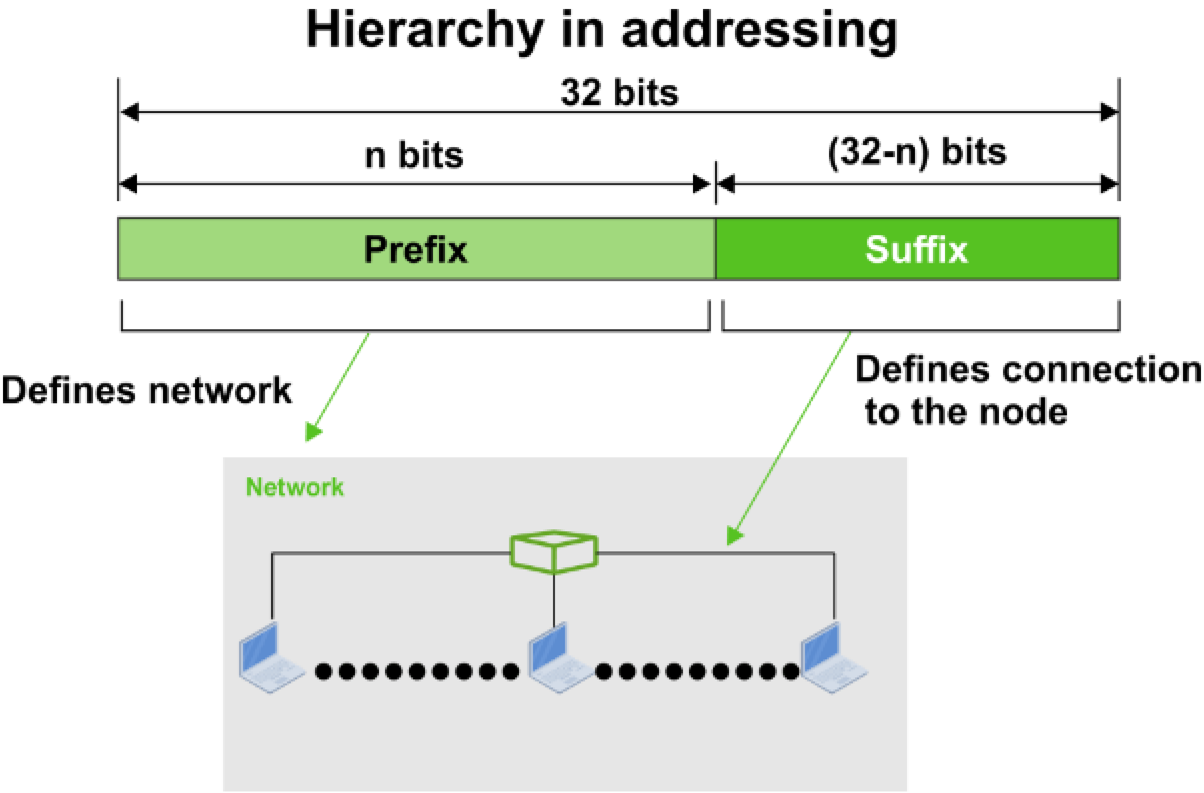
The IP address, often known as the Internet address, is the unique identifier used in the IP layer of the TCP/IP protocol suite to identify each device's connection to the Internet. A host's or router's connection to the Internet is defined by its 32-bit IPv4 address, which is unique and used worldwide. The IP address, not the host or router, is what identifies the connection because it could change if the device is relocated to a different network.

Since each address specifies a single and exclusive connection to the Internet, IPv4 addresses are distinctive. A device has two IPv4 addresses if it has two networks connecting to the Internet through it. Because every host that wishes to connect to the Internet must use the IPv4 addressing scheme, IPv4 addresses are considered universal.

Hierarchy in Addressing

The addressing system is hierarchical in every type of communication network that requires delivery, including phone and postal networks.

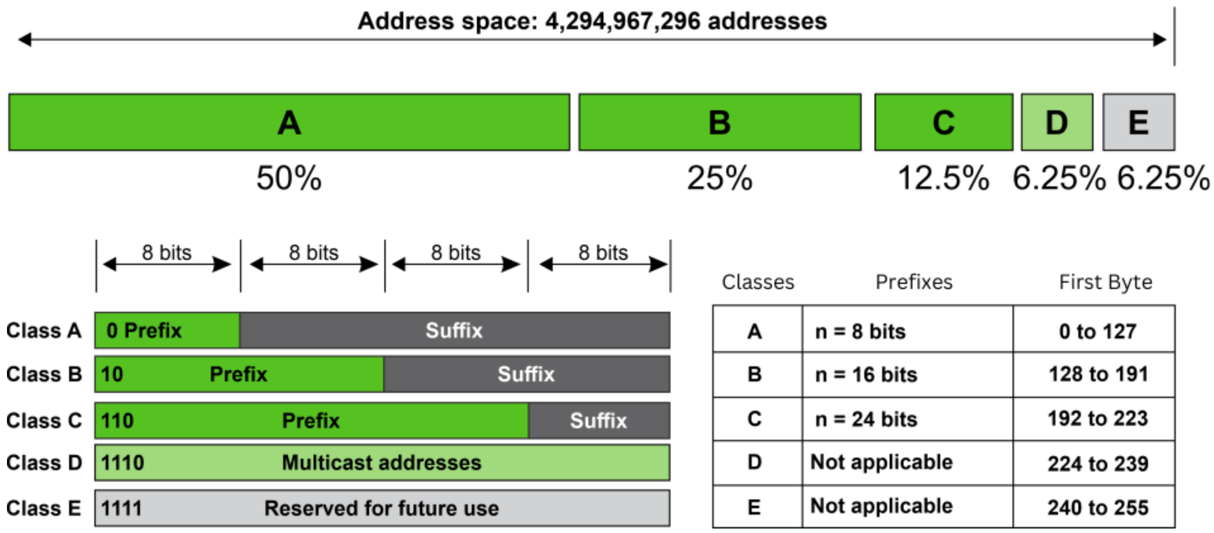
Although it is separated into two parts, a 32-bit IPv4 address is also hierarchical. The network is defined by the first component of the address, known as the **prefix**, and the node is defined by the second component, known as the **suffix** (connection of a device to the Internet). A 32-bit IPv4 address's prefix and suffix are shown in the given figure. The lengths of the prefix and suffix are n bits and (32 - n) bits, respectively.



Prefixes can have variable or fixed lengths. The IPv4 network identification was initially intended to be a fixed-length prefix. ***Classful*** **addressing** is the term used to describe this outmoded system. ***The brand-new addressing method, known as classless addressing, makes use of a variable-length network prefix.*** Prior to focusing on classless addressing, we briefly explore classful addressing.

1. CLASSFUL ADDRESSING

An IPv4 address originally had a fixed-length prefix, but three fixed-length prefixes (n = 8, n = 16, and n = 24) were created in order to support both small and big networks. As shown in the figure below, the entire address space was partitioned into five classes (classes A, B, C, D, and E). Classful addressing is the term used to describe this system. Despite being a thing of the past, classful addressing aids in the comprehension of classless addressing, which is covered in the later section.



Occupation of the address space in classful addressing

Classes	Prefixes	First Byte
A	n = 8 bits	0 to 127
B	n = 16 bits	128 to 191
C	n = 24 bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

CLASS A - Despite the fact that the network length is 8 bits, we can only use seven bits for the network identifier since the first bit, which is 0 and determines the class, is part of the length. This indicates that only 2^7 = 128 networks can have a class A address globally.

- Net ID = 8bits long and Host ID = 24 bits long
- Method to identify class A addresses:
  - The first bit is reserved to 0 in binary
  - Range of the first octet is [0, 127] in dotted decimal
- Total number of connections in Class A = 2^{31} (2, 14, 74, 83, 648)
- There are 2^7 - 2 = 126 networks in the Class A network.
  - There are 2 fewer networks available overall since IP Address 0.0.0.0 is set aside for broadcasting needs. For usage as a loopback address while testing software, the IP address 127.0.0.1 is set aside.
  - Hence, the range of the first octet becomes [1, 126]
- Total number of Host IDs in Class A = 2^{24} - 2 [1, 67, 77, 214]
  - There are 2 fewer hosts that can be established across all classes due to the two reserved IP addresses, where all of the host ID bits are either zero or one.
  - The Network ID for the network is represented when all of the Host ID bits are set to 0.
  - The Broadcast Address is represented when all of the Host ID bits

are set to 1.

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

CLASS B - Despite the fact that the first two bits of class B's network, which are 10 in binary or we can write it as $(10)_2$, determine the class, we can only use 14 bits as the network identification, as class B's network length is 16 bits. As a result, only 2^{14} = 16,384 networks in the entire world are capable of using a class B address.

- Length of Net Id = 16 bits and length of Host ID 16 bits.
- Method to identify Class B networks:
  - First two bits are reserved to 10 in binary notation
  - The Range of the first octet is [128, 191] in dotted decimal notation
- 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.

CLASS C - All addresses that begin with the number $(110)_2$ fall under class C. Class C networks are 24 bits long, but since the class is defined by three bits, the network identifier can only be 21 bits long. As a result, 2^{21} = 2, 097, 152 networks worldwide are capable of using a class C address.

- The length of the Net Id and the Host Id = 24 bits and 16 bits respectively.
- Method to identify Class C networks:
  - First three bits are reserved for 110 in binary notation or $(110)_2$.
  - The range of the first octet is [192, 223] in dotted decimal notation.
- Total number of connections in Class C = 2^{29} = 53, 68, 70, 912.
- Total number of networks available in Class C = 2^{24} = 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.

Quick Quiz - *The maximum number of networks that can use Class C addresses in the IPv4 addressing format is* __________

1. 2^{14}
2. 2^{7}
3. 2^{21}
4. 2^{24}

Ans. (c)

CLASS D - Prefix and suffix categories do not exist for Class D. It is employed for multicast addresses.

- There is no concept of Host ID and Net ID
- Method to identify Class D network:
  - The first four bits are reserved to 1110 in binary notation or $(1110)_2$
  - The range of the first octet is [224, 239] in dotted decimal notation
- Total number of IP addresses available is 2^{28} = 26, 84, 35, 456
- Because data is not intended for a specific host, Class D is set aside for multicasting, which eliminates the requirement to extract the host address from the IP address.

CLASS E - All binary addresses with the prefix 1111 fall under class E. Class E, like Class D, does not have a prefix or a suffix and is used as a reserve.

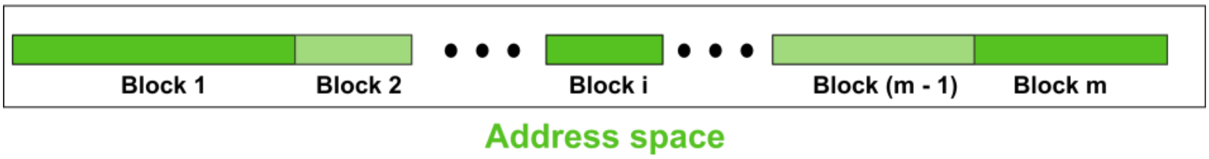
- Like in Class D, there is also no concept of Host ID and Net ID.
- Method to identify Class E networks:
  - The first four bits are reserved to 1111 in binary notation or (1111)
  - The range of the first octet is [240, 255] in dotted decimal notation.
- Total number of IP addresses available is 2^{28} = 26,84,35,456.
- Class E is set aside for hypothetical or experimental uses.

2. CLASSLESS ADDRESSING

The address depletion issue was not fully resolved by classful addressing's subnetting and supernetting techniques. As the Internet expanded, it became obvious that a bigger address space was required as a long-term fix. However, the expanded address space necessitates that IP addresses should be longer as well, necessitating a change in IP packet syntax. The short-term solution, which uses the same address space but modifies the distribution of addresses to deliver a fair amount to each business, was developed despite the fact that the long-term solution, known as IPv6, has already been developed. ***Classless addressing is the temporary fix, which nevertheless makes use of IPv4 addresses.*** In order to make up for address depletion, the class privilege was taken out of the distribution.

The entire address space is partitioned into blocks of varying lengths with classless addressing. An address's prefix designates the block (network); its suffix designates the node (device). We are capable of having a block of 20, 21, 22 ,...., 232 addresses, theoretically. One of the limitations is that a block of addresses must have a power of two addresses. One address block may be given to an organization. The given figure demonstrates the non-overlapping block segmentation of the entire address space.

Variable-length block in classless addressing



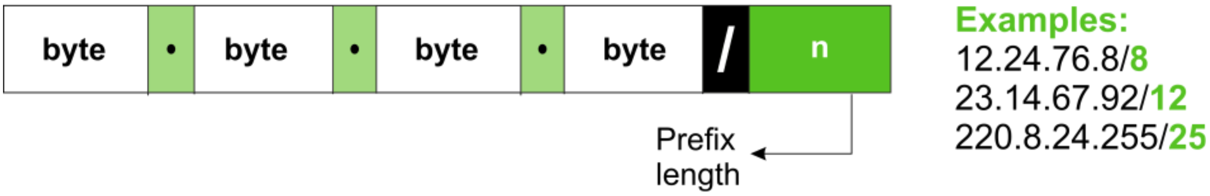
In contrast to classful addressing, classless addressing allows for varying prefix lengths. Prefix lengths that vary from 0 to 32 are possible. The length of the prefix has an inverse relationship with network size. A smaller network has a large prefix; a larger one has a small prefix.

We must stress that classful addressing is just as easily adaptable to the concept of classless addressing. Consider an address in class A as a classless address with a prefix length of 8. Class B addresses can be viewed as classless addresses with the prefix 16 and so on. Putting it another way, ***classless addressing is a specific instance of classful addressing.***

Prefix Length - Slash Notation

In classless addressing, the first issue that needs to be resolved is how to determine the prefix length if an address is provided. We must individually provide the prefix length because it is not a property of the address. The address is inserted in this scenario, followed by a slash, and the prefix length, n. Slash notation is the colloquial name for the notation, while classless interdomain routing, or CIDR (pronounced cider) method, is the official name. An address in classless addressing can thus be expressed as illustrated in the figure below.

Slash notation (CIDR)



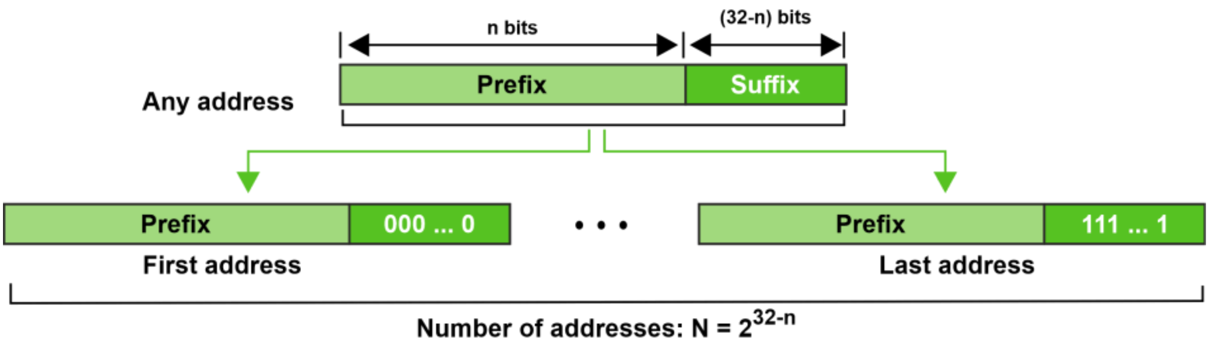
To put it another way, we must also provide the prefix length in classless addressing because an address does not automatically define the block or network to which it belongs.

Extracting Information from an Address

With respect to any given address in the block, we typically like to know three things: the number of addresses in the block, the start address in the block, and the last address. These three pieces of information, which are depicted in the picture below, are simple to locate because the prefix length, n, is known.

- The block has N = 232n addresses, according to the calculation.
- The n leftmost bits are kept, and the (32 - n) rightmost bits are all set to zeroes to determine the first address.
- The n leftmost bits are kept, while the (32 - n) rightmost bits are all set to 1s to determine the last address.

Information extraction in classless addressing

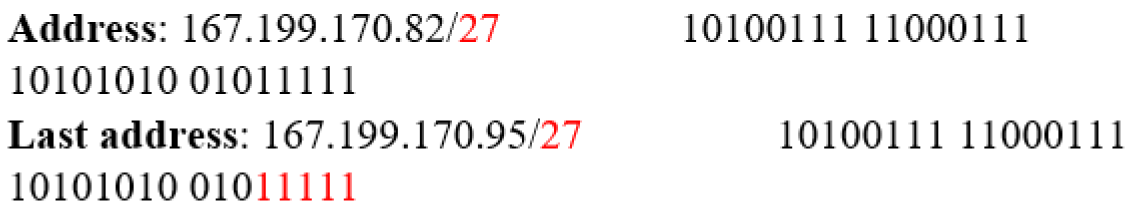


For Example - The address 167.199.170.82/27 is a classless address. The following is where we can find the aforementioned three pieces of data. In the network, there are 2^{32-n} = 2^5 = 32 addresses in all.

The first 27 bits are kept while the remaining bits are converted to 0s to determine the first address.

Address: 167.199.170.82/27 10100111 11000111
10101010 01010010
First address: 167.199.170.64/27 10100111 11000111
10101010 01000000

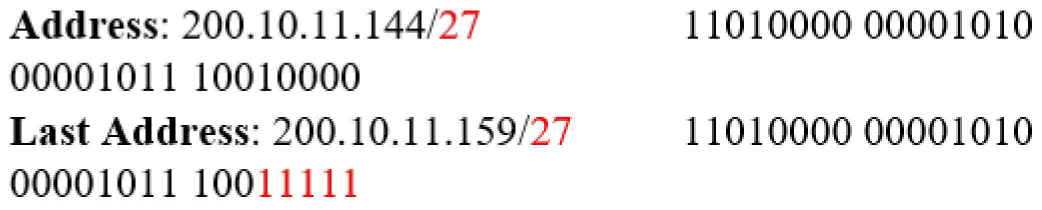
Keeping the first 27 bits and turning the remaining bits to 1s will allow you to determine the last address.



Address: 167.199.170.82/27 10100111 11000111
10101010 01011111
Last address: 167.199.170.95/27 10100111 11000111
10101010 01011111

Quick Quiz - In the network 200.10.11.144/27, the fourth octet (in decimal) of the last IP address of the network, which can be assigned to a host is _____ (GATE 2015, 2 Marks)

Ans.



Address: 200.10.11.144/27 11010000 00001010
00001011 10010000
Last Address: 200.10.11.159/27 11010000 00001010
00001011 10011111

Here, the maximum possible value of the last octet is 159 in decimal. Hence, the fourth octet of the last IP address, which can be assigned to a host is 10011110 in binary or 158 in decimal. Hence***, the answer to the question is 158***.

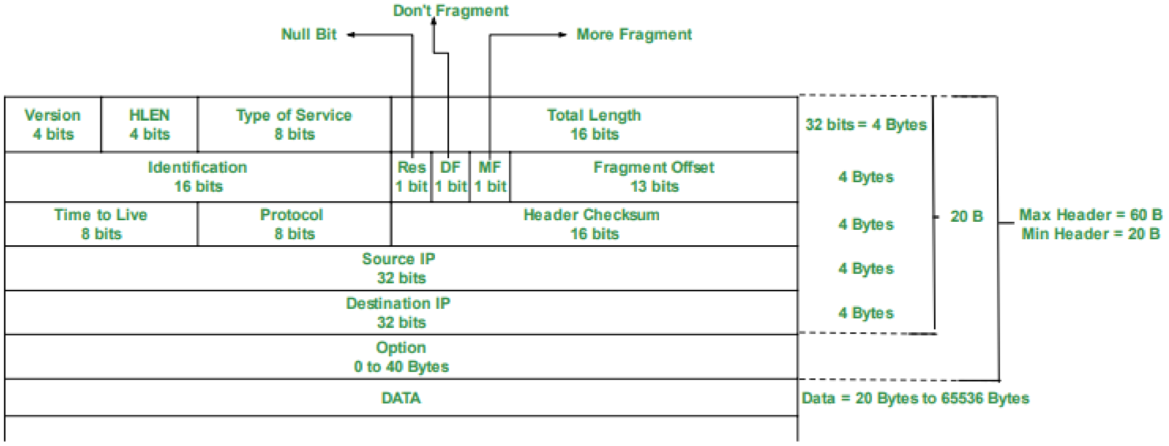
Difference Between Classful and Classless Addressing

1. IP addresses are divided into five groups using the classful addressing approach when they are assigned. In order to prevent the depletion of IP addresses, classless addressing is used. It is a method of IP address allocation that will eventually replace classful addressing.
2. A further distinction is the usefulness of classful and classless addressing. Comparatively speaking, classless addressing is more beneficial and useful than classful addressing.
3. In classful addressing, the network ID and host ID are adjusted according to the classes. However, the distinction between network ID and host ID does not exist with classless addressing. This opens up the possibility of making yet another contrast between both addressing.

IPV4 PACKET FORMAT

IPv4 is a connectionless protocol used for packet-switched networks. It operates on a best-effort delivery model, in which neither delivery is guaranteed, nor proper sequencing or avoidance of duplicate delivery is assured. Internet Protocol Version 4 (IPv4) is the fourth revision of the Internet Protocol and a

widely used protocol in data communication over different kinds of networks. IPv4 is a connectionless protocol used in packet-switched layer networks, such as Ethernet. It provides a logical connection between network devices by providing identification for each device. There are many ways to configure IPv4 with all kinds of devices – including manual and automatic configurations – depending on the network type. IPv4 is defined and specified in IETF publication RFC 791. IPv4 uses 32-bit addresses for Ethernet communication in five classes: A, B, C, D and E. Classes A, B and C have a different bit length for addressing the network host. Class D addresses are reserved for multicasting, while class E addresses are reserved for military purposes. IPv4 uses 32-bit (4-byte) addressing, which gives 2^{32} addresses. IPv4 addresses are written in the dot-decimal notation, which comprises of four octets of the address expressed individually in decimal and separated by periods, for instance, 192.168.1.5.
IPv4 Datagram Header Size of the header is 20 to 60 bytes.



IPv4 Datagram Header

***VERSION:** Version of the IP protocol (4 bits), which is 4 for IPv4*

***HLEN:** IP header length (4 bits), which is the number of 32 bit words in the header. The minimum value for this field is 5 and the maximum is 15.*
***Type of service:** Low Delay, High Throughput, Reliability (8 bits)*
***Total Length:** Length of header + Data (16 bits), which has a minimum value 20 bytes and the maximum is 65,535 bytes.*
***Identification:** Unique Packet Id for identifying the group of fragments of a single IP datagram (16 bits)*
***Flags:** 3 flags of 1 bit each : reserved bit (must be zero), do not fragment flag, more fragments flag (same order)*
***Fragment Offset:** Represents the number of Data Bytes ahead of the particular fragment in the particular Datagram. Specified in terms of number of 8 bytes, which has the maximum value of 65,528 bytes.*
***Time to live:** Datagram's lifetime (8 bits), It prevents the datagram to loop through the network by restricting the number of Hops taken by a Packet before delivering to the Destination.*
***Protocol:** Name of the protocol to which the data is to be passed (8 bits)*
***Header Checksum:** 16 bits header checksum for checking errors in the datagram header*
***Source IP address:** 32 bits IP address of the sender*

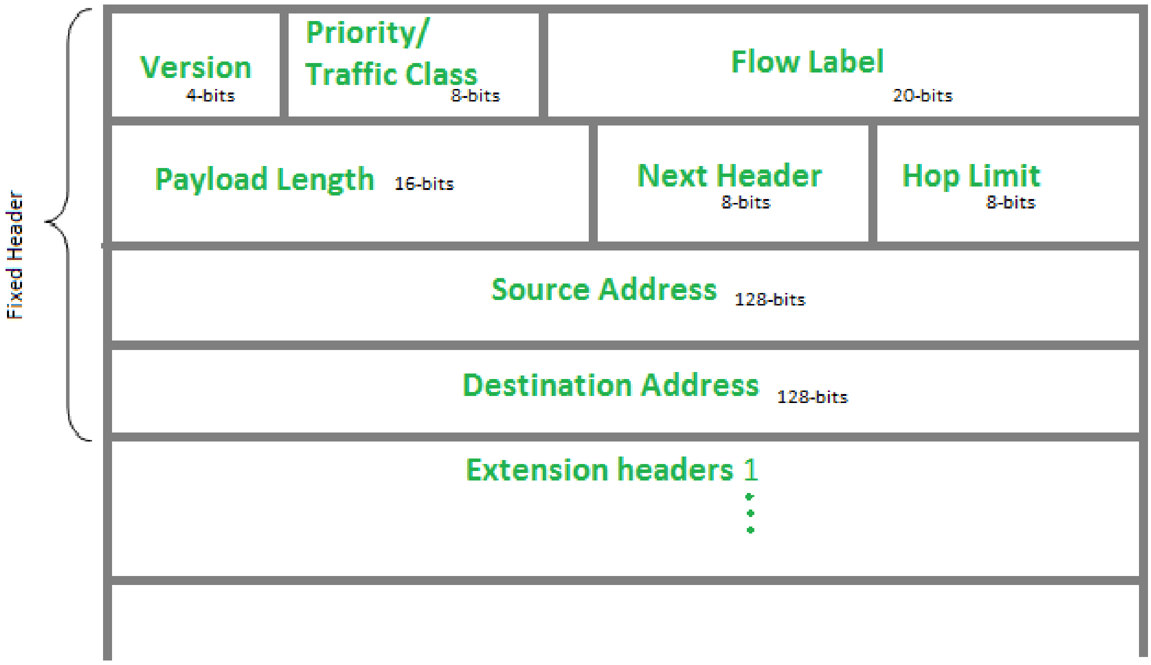
Destination IP address: *32 bits IP address of the receiver*
Option: *Optional information such as source route, record route. Used by the Network administrator to check whether a path is working or not.*

Due to the presence of options, the size of the datagram header can be of variable length (20 bytes to 60 bytes).

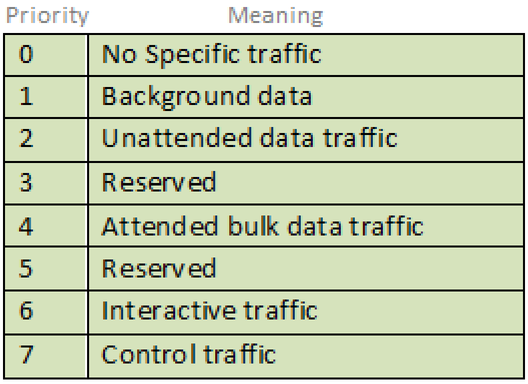
IPV6 HEADER FORMAT

IP version 6 is the new version of Internet Protocol, which is way better than IP version 4 in terms of complexity and efficiency. Let's look at the header of IP version 6 and understand how it is different from the IPv4 header.

IP version 6 Header Format :



Version (4-bits): Indicates version of Internet Protocol which contains bit sequence 0110.
Traffic Class (8-bits): The Traffic Class field indicates class or priority of IPv6 packet which is similar to *Service Field* in IPv4 packet. It helps routers to handle the traffic based on the priority of the packet. If congestion occurs on the router then packets with the least priority will be discarded.
As of now, only 4-bits are being used (and the remaining bits are under research), in which 0 to 7 are assigned to Congestion controlled traffic and 8 to 15 are assigned to Uncontrolled traffic.
Priority assignment of Congestion controlled traffic :

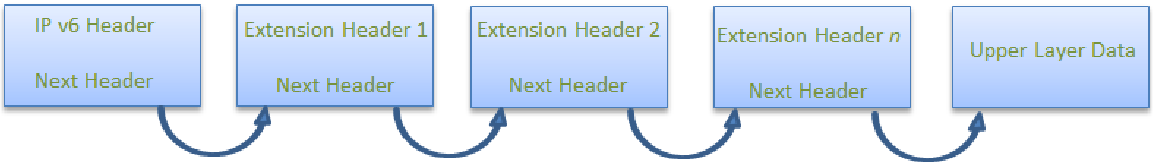


Priority	Meaning
0	No Specific traffic
1	Background data
2	Unattended data traffic
3	Reserved
4	Attended bulk data traffic
5	Reserved
6	Interactive traffic
7	Control traffic

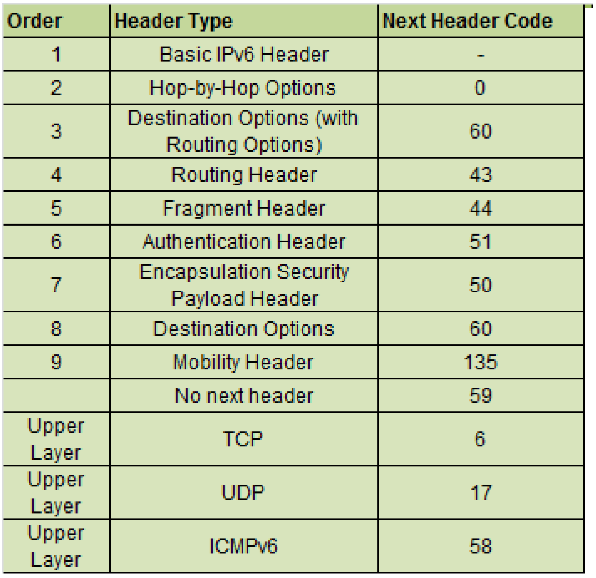
Uncontrolled data traffic is mainly used for Audio/Video data. So we give higher priority to Uncontrolled data traffic.
The source node is allowed to set the priorities but on the way, routers can change it. Therefore, the destination should not expect the same priority which was set by the source node.

Flow Label (20-bits): Flow Label field is used by a source to label the packets belonging to the same flow in order to request special handling by intermediate IPv6 routers, such as non-default quality of service or real-time service. In order to distinguish the flow, an intermediate router can use the source address, a destination address, and flow label of the packets. Between a source and destination, multiple flows may exist because many processes might be running at the same time. Routers or Host that does not support the functionality of flow label field and for default router handling, flow label field is set to 0. While setting up the flow label, the source is also supposed to specify the lifetime of the flow.
Payload Length (16-bits): It is a 16-bit (unsigned integer) field, indicates the total size of the payload which tells routers about the amount of information a particular packet contains in its payload. The payload Length field includes extension headers(if any) and an upper-layer packet. In case the length of the payload is greater than 65,535 bytes (payload up to 65,535 bytes can be indicated with 16-bits), then the payload length field will be set to 0 and the jumbo payload option is used in the Hop-by-Hop options extension header.
Next Header (8-bits): Next Header indicates the type of extension header(if present) immediately following the IPv6 header. Whereas In some cases it indicates the protocols contained within upper-layer packets, such as TCP, UDP.
Hop Limit (8-bits): Hop Limit field is the same as TTL in IPv4 packets. It indicates the maximum number of intermediate nodes IPv6 packet is allowed to travel. Its value gets decremented by one, by each node that forwards the packet and the packet is discarded if the value decrements to 0. This is used to discard the packets that are stuck in an infinite loop because of some routing error.
Source Address (128-bits): Source Address is the 128-bit IPv6 address of the original source of the packet.
Destination Address (128-bits): The destination Address field indicates the IPv6 address of the final destination(in most cases). All the intermediate nodes can

use this information in order to correctly route the packet.
Extension Headers: In order to rectify the limitations of the *IPv4 Option Field*, Extension Headers are introduced in IP version 6. The extension header mechanism is a very important part of the IPv6 architecture. The next Header field of IPv6 fixed header points to the first Extension Header and this first extension header points to the second extension header and so on.

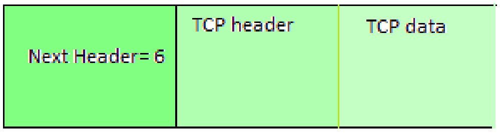


IPv6 packet may contain zero, one or more extension headers but these should be present in their recommended order:

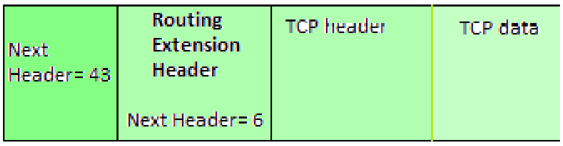


Order	Header Type	Next Header Code
1	Basic IPv6 Header	-
2	Hop-by-Hop Options	0
3	Destination Options (with Routing Options)	60
4	Routing Header	43
5	Fragment Header	44
6	Authentication Header	51
7	Encapsulation Security Payload Header	50
8	Destination Options	60
9	Mobility Header	135
	No next header	59
Upper Layer	TCP	6
Upper Layer	UDP	17
Upper Layer	ICMPv6	58

Example: *TCP is used in IPv6 packet*



Example2:

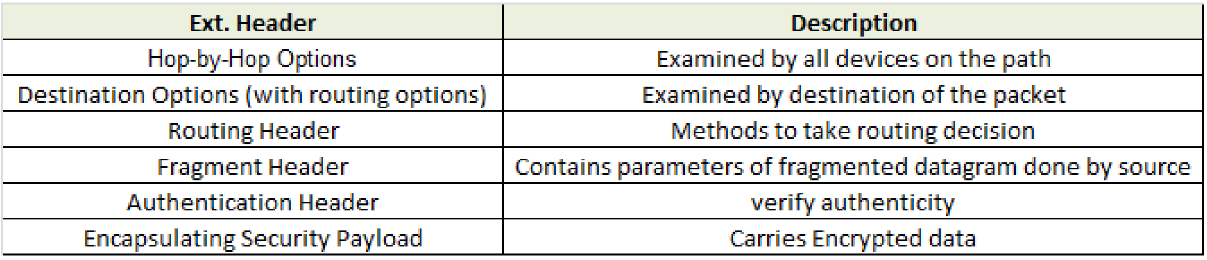


Rule: Hop-by-Hop options header(if present) should always be placed after the IPv6 base header.

Conventions :

1. Any extension header can appear at most once except Destination Header because Destination Header is present two times in the above list itself.
2. If Destination Header is present before Routing Header then it will be examined by all intermediate nodes specified in the routing header.
3. If Destination Header is present just above the Upper layer then it will be examined only by the Destination node.

Given order in which all extension header should be chained in IPv6 packet and working of each extension header :



Ext. Header	Description
Hop-by-Hop Options	Examined by all devices on the path
Destination Options (with routing options)	Examined by destination of the packet
Routing Header	Methods to take routing decision
Fragment Header	Contains parameters of fragmented datagram done by source
Authentication Header	verify authenticity
Encapsulating Security Payload	Carries Encrypted data

SUBNETTING

Subnetting is a combination of two words i.e. Sub and Netting. Here Sub word means Substitute and netting word means Network. The Substitute Network created for a function to happen is known as Subnetting.

Here, Substitute Network does not mean a new network is created. A full piece of network is broken into small pieces and each piece a different is assigned.

Subnet is the name given to piece of the broken network or can also be called as the Substitute network is known as Subnet. Subnets are the legal small parts of IP (Internet Protocol) Addressing process

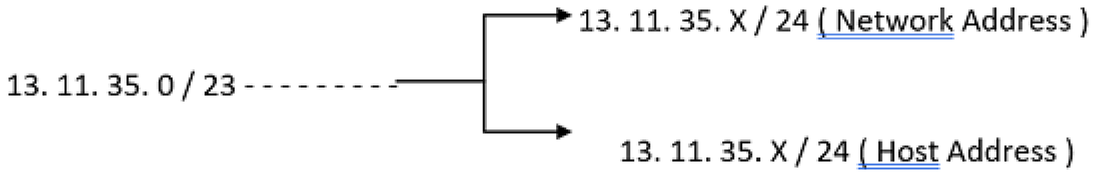
Subnetting should be done in such a way that network does not gets affected. This means that we can divide the network into different parts but all when put together should perform the same task when done before splitting in to small parts.

Subnets reduce the need for traffic to use unnecessary routes, which speeds up the network. To help with the lack of IP addresses on the internet, subnets were developed

- **Division of IP Addresses**

An IP address is split into its network address and host address via subnetting.

The split address may then be further divided into units using the subnet mask approach, and those units can be assigned to different network devices.


13. 11. 35. 0 / 23
13. 11. 35. X / 24 (Network Address)
13. 11. 35. X / 24 (Host Address)

Here, X refers to the Host ID. This is the only thing which gets changed in the Internet Protocol Address

Now, we are going to learn how these subnets provide the different addresses to different devices and also the process of subnetting in computer networks. So, by this example we would easily understand the working of the Subnet.

We are going to learn how Subnets are formed for Internet Protocol version 4 (IPv4) Addressing.

The IPv4 Addressing has five different classes. They are:

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

The total number of Internet Protocol Addresses (IP Address) gives the total number of Subnets that can be formed by using a network.

- Class A has 24 Host ID Bits
- Class B has 16 Host ID Bits
- Class C has 8 Host ID Bits

The number of usable IP Addresses that can be created is

The total number of IP Addresses creatable = $2^{\text{The total number of Host ID Bits}}$ - 2.

Class A Network can have 2^{24} - 2

Class B Network can have 2^{16} - 2

Class C Network can have 2^{8} - 2

Class D and Class E do not contribute for IP Address creation.

Class D is used for multicasting purpose

Class E is used for Address Range Calculator

They are saved for future purposes.

Class Network	Total Number of Hosts that can be accommodated	Total Number of IP Addresses Formula Substitution	Total Number of IP Addresses	Total Number of IP Addresses in Words
Class A	2^{24}	2^{24} - 2	1, 67, 77, 214	One Crore Sixty Seven Lakhs Seventy Seven

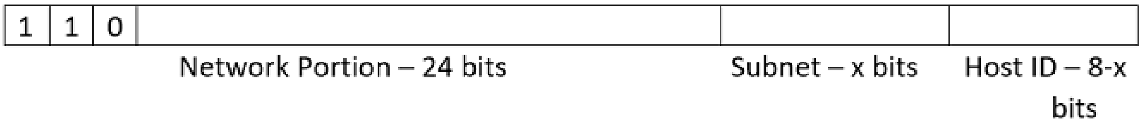
				Thousand Two Hundred And Thirty Four
Class B	2^{16}	2^{16} - 2	65, 534	Sixty Five Thousand Five Hundred and Thirty Four
Class C	2^{8}	2^{8} - 2	254	Two Hundred And Fifty Four

Subnetting

We have arrived at the subject at hand, Subnetting, thanks to the problem of IP address waste. By taking bits from the Host ID section of the address, subnetting enables the creation of smaller networks (sub networks; subnets) within of a larger network. With the help of those borrowed bits, we can build more networks with a reduced overall size.

A Subnet is created from the bits taken from the Host ID.

To understand about this concept let take an example of a network this belongs to class C.



Our goal is to create to build a network. The capacity of each network must be Thirty (30) Devices. We have three networks of type Class C Network based on IPv4 Addressing.

Each Class C Network can provide Two Hundred and Fifty Four (254) Internet Protocol Addresses.

The Capacity of each device which we require is very less than the Capacity which we require.

So, now we divide the four networks based on the requirement. Let us see how this division happens.

We have four Class C Networks of imaginary Internet Protocol (IP) Addresses like:

1. Network 1 : 255.147.1.0
2. Network 2 : 255.147.2.0

3. Network 3 : 255.147.3.0
4. Network 4 : 255.147.4.0

We know that each network can produce 254 IP Addresses alone. This means four networks can produce 254 * 4 = 1016 (Thousand and Sixteen) Internet Protocol Addresses can be formed. But what we require is only thirty Internet Protocol Addresses from each Network. This means we only need hundred and Twenty (120) IP Addresses only.

This means 1016 - 120 = 896

Eight Hundred and Ninety-Six Addresses created are wasted. So, we need to use the Host ID bits wisely.

So, by some calculation we will get to know that if we take 5 bits from each network we will be able to get 30 IP Addresses from each Network.

The formula for number of IP Addresses is:

The total number of IP Addresses creatable = $2^{\text{The total number of Host ID Bits}}$ - 2.

So, now we will consider 5 Host ID Bits.

2^5 - 2 = 30 Internet Protocol Addresses from each Network.

So, by considering we can create 30 Usable IP Addresses from each Class C Network.

So, now we have 3 more Host ID Bits left over unused. We also have different ways in using these remaining bits.

Other Ways are:

1. These remaining Host ID Bits can be used to increase the capacity of the IP Addresses to be created in future, if required.
2. We can also create a new six subnets from each network using these three Host ID Bits.

First method is usually chosen because creation of two different subnets causes wastage of IP Addresses. Let me explain this problem with the help of the above example.

Example:

The network belongs to Class C Network which has 8 Host ID Bits.

In the above first created Subnet we have only used 30 IP Addresses only.

In the newly created Subnet we have created only 6 IP Addresses only.

This means we have used the full potential of the Class C Network. We might have used the whole 8 bits. But, this is considered as wastage of resources.

This is called wastage because we have now a capacity of 36 IP Addresses to be created.

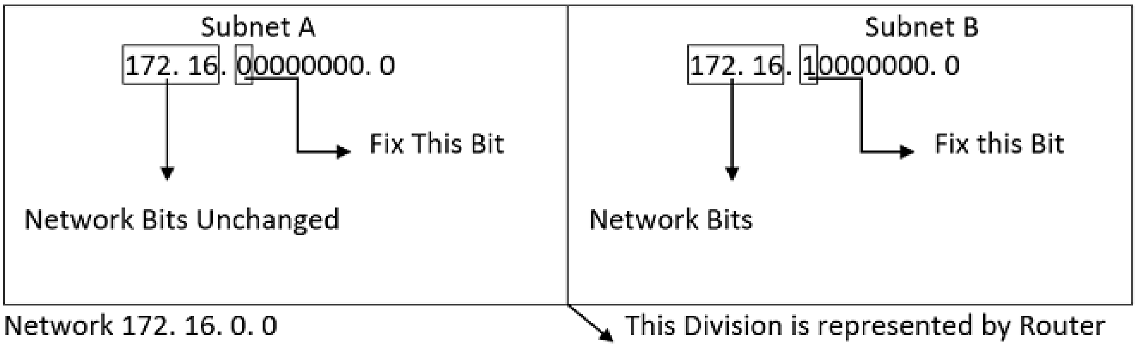
But, the actual capacity of the Class C is 254 IP Addresses.

This means 254 - 36 = 218 IP Addresses are wasted now because of this Host ID Bits Division.

So, it is better to save the remaining Host ID Bits for future purpose rather than dividing it for these kind of resource wasting purpose.

Subnetting, as we all know, separates the network into small subnets. While each subnet permits communication between the devices connected to it, subnets are connected together by routers. The network technology being utilized and the connectivity requirements define the size of a subnet. Each organization is responsible for selecting the number and size of the subnets it produces, within the constraints of the address space available for its use.

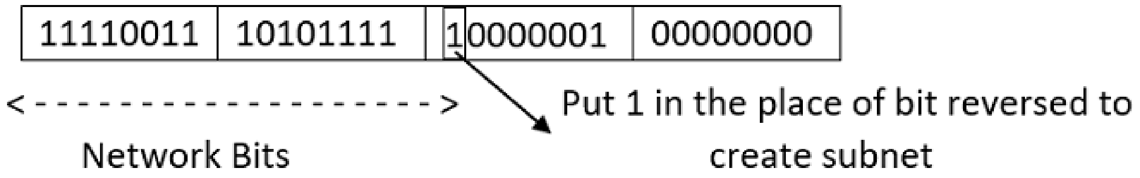
- For the construction of the subnets, we usually check the MSB (Most Significant Bit) bits of the host ID and if found wrong we make it right. In order to create two network subnets, we fix one of the host's MSB (Most Significant Bit) bits in the table below. We are unable to alter network bits since doing so would alter the entire network.



We need a subnet mask to identify a subnet, which is created by substituting the number "1" for each Network ID bit and the amount of bits we reserve for Host ID to create the subnet. A data packet from the internet is intended to be forwarded to the specified subnet network using the subnet mask.

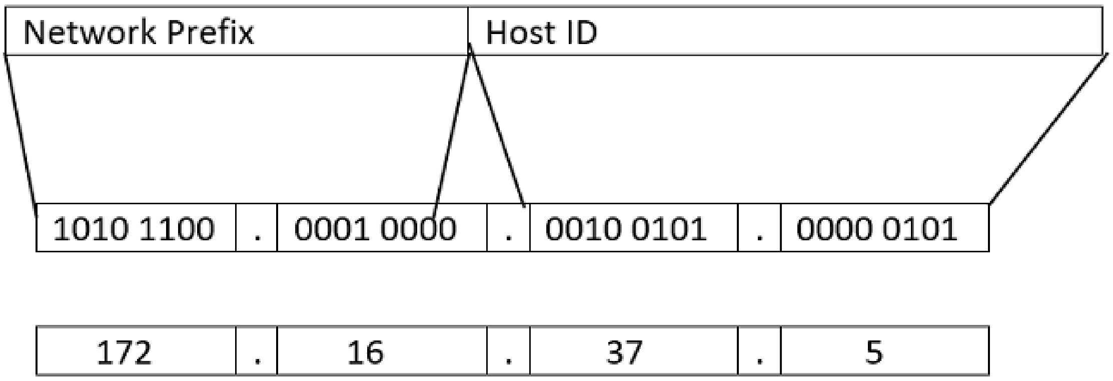
A part of an address should be used as the Subnet ID is also specified by the subnet mask. In order to apply the subnet mask to the whole network address, a binary AND operation is utilized. When performing an AND operation, it is assumed that the result will be "true" if both inputs are. If not, "false" is presented. This is only possible when both bits are 1.

The Subnet ID results from this. The Subnet ID is used by routers to choose the best route among the sub - networks.



Subnet Mask = 243. 175. 129. 0

- The two components that make up an IP address are the Network Prefix (sometimes called the Network ID) and the Host ID. Depending on whether the address is Class A, B, or C, either the Network Prefix or the Host ID must be separated. A Class B IPv4 address, 172.16.37.5, is seen in the image below. The Network Prefix is 172.16.0.0, and the Host ID is 37.5.



- We use permutations to the amount of bits set aside to form subnets if we wish to produce subnets of varied length. Variable Length Subnet Masking is the name of this subnetting (VLSM).
- After setting aside some bits to indicate the subnet, the broadcast address of a subnet is computed by setting all the remaining bits of the host id to 1.The message is sent to all network hosts using the broadcast address.

Advantages of Subnetting

- Subnetting is used to decrease the presence of Internet Protocol (IP) range.
- Subnets helps in stopping the devices or gadgets from occupying the whole network, only allowing the hosts to control which kind of user can have access to the important information. Simply, we can tell that network is safe just because of the subnetting concept.
- Subnetting concept increases the performance of the total network by deleting the repeated traffic causing errors.
- We can convert the whole big network into smaller networks by using the concept of subnetting as discussed earlier.

Disadvantages of Subnetting

- If the number of subnets increases, then the number of routers must also increase along with the subnet increase number. This happens because each subnet has its own subnet mask, broadcast address and network address.
- As told earlier, if we create many subnets many IP Addresses are wasted because of the wastage of Host ID Bits
- The cost of the entire network is increased by subnetting, which calls for the acquisition of pricey internal routers, switches, hubs, and bridges, among other things.
- The complexity of the network is increased through subnetting. The subnet network must be managed by a skilled network administrator.