Unit-4

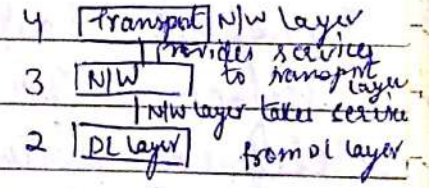
NETWORK LAYER

Major Responsibilities are - / Duties.

- Addressing < classful / classless
- Routing
- Congestion Control < VC / Datagram
- Internetworking < Tunneling / Internetwork Routing
- Packetizing (IP)
  - IPV4
  - IPV6.
- Fragmentation.

N/W layer is concerned with getting packets from the source on the way to the destination. Getting to the destination may require making many hops at intermediate routers along the way. To achieve its goal the N/W layer must know about the topology of the comm^n subnet and choose appropriate path through it.

Position of N/W Layer -

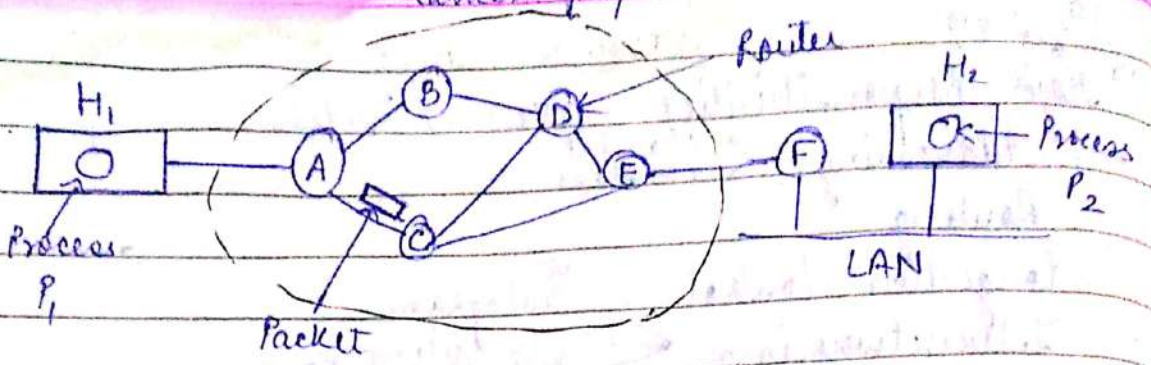


N/W Layer Design Issues -

There are various N/W layer design issues. These issues include the service provided to the transport layer & the internal design of the subnet.

1. Store & Forward Packet Switching - The context in which the N/W layer protocol works can be shown as follows:

Host H1 is directly connected to one of the carrier routers i.e. A, in contrast H2 is on local area network and connected with



Router F.

A host with a packet to send transmits it to the nearest router, either on its LAN or over a point to point link to the carrier. The packet is stored there & then it is forwarded to the next routes along the path until it reach the destination. This mechanism is called store & fwd packet switching.

2. Services provided to the Transport Layer -

The N/W layer provides services to the transport layer at the N/W / transport layer interface. The N/W layer services have been designed with the following goal in mind -

a.) The services should be independent of the router technology.

b.) The transport layer should be shielded from the number, type & topology of the routers present

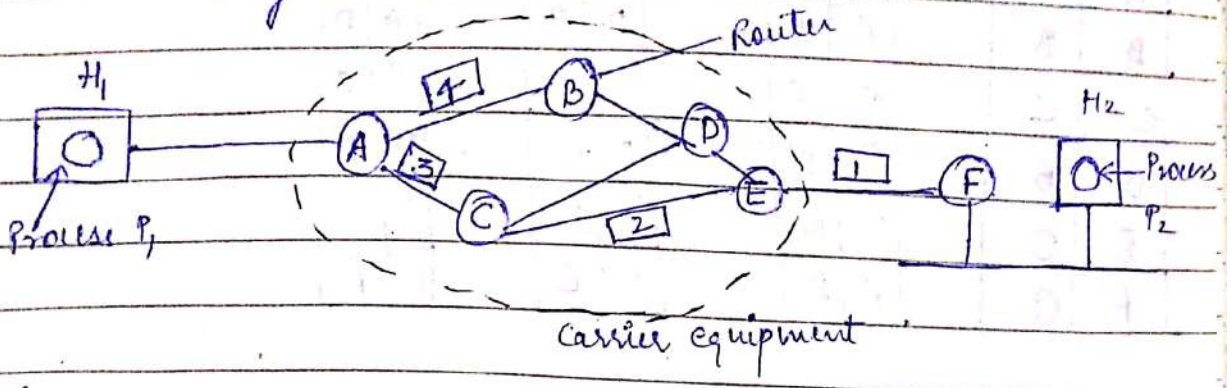
c.) The N/W addresses made available to the transport layer should use a uniform numbering system.

ex - postal system.

3. Implementation of Connectionless Service -

In connectionless service, packets are injected into the subnet individually & routed independently of each other. No advance

setup is required. In this context, the packets are called datagram & subnet is called datagram subnet. Fig shows how the datagram subnet works -



Suppose that the process P_1 has a long message for P_2. It hands the message to the transport layer with instruction to deliver it to process P_2 on host H_2. It prepends a transport header to the front of the message & hands the result to the N/W layer.

Let us assume that the message is 4 times longer than the maximum packet size, therefore the N/W layer breaks this packet into 4 packets 1, 2, 3 & 4 and sends each of them to Router A.

Every router has an internal table telling it where to send to packets for each possible destination. Each table entry is a pair consisting of a destination & the outgoing line to use for that destination. Eg. in fig, A has 2 outgoing lines to B & to C. So every incoming packet must be sent to one of these routers.

The initial routing table of A is shown in figure with label initially

A's table initially

A	—
B	B
C	C
D	B
E	C
F	C

later

A	—
B	B
C	C
D	B
E	B
F	B

C's table

A	A
B	A
C	—
D	D
E	E
F	E

E's table

A	C
B	D
C	C
D	D
E	—
F	F

As they arrived at A, packets 1, 2 & 3 were stored & then each was forwarded to C acc. to A's table. Packet 1 was then forwarded to E and then to F. When it go to F it was encapsulated in a datalink layer frame & send to H_2 over the LAN. Packets 2 & 3 follow the same route.

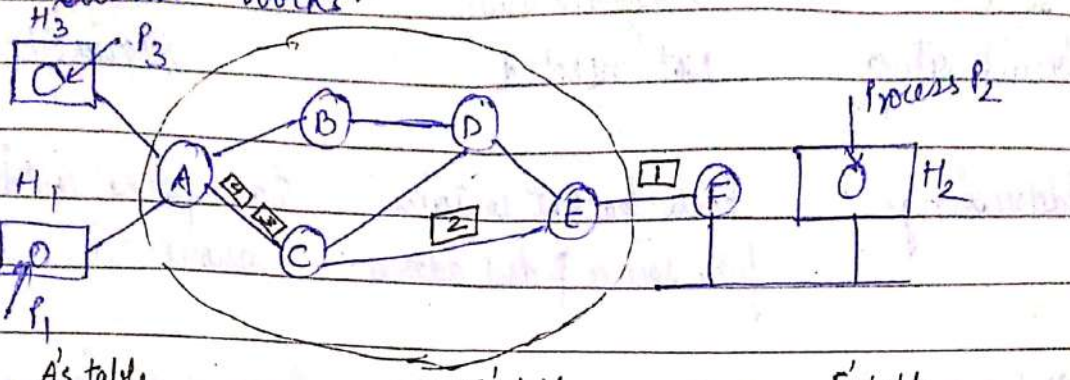
Packet 4 when go to A, it was sent to router B. for some reason A decided to send packet ~~for~~ 4 via a different route then that of the first three (perhaps it detect a traffic jam somewhere along the path ACE & updated its routing table). The algorithm that manage the tables & make routing decisions is called routing algorithm.

ex- telephone call.

4. Implementation of connection-oriented service -

If connection oriented service is used, a path from source router to the destination router must be established before any data packet can be sent. This connection is called a virtual

circuit (VC) and the subnet is called virtual circuit subnet. fig shows an example of how the VC subnet works.



A's table

in		out
H_1	1	C 1
H_3	1	C 2

C's table

in		out
A	1	E 1
A	2	E 2

E's table

in		out
C	1	F 1
C	2	F 2

Host H_1 has established connection 1 with host H_2. It is remembered as the first entry in each of the routing tables. The first line of A's table says that if a packet having connection identifier 1 comes in from H_1, it is to be sent to router C and given the conn^c identifier 1. Similarly, the first entry at C routes the packet to E with conn^c identifier 1.

If H_3 also wants to establish a connection to H_2, it selects conn^c identifier 1 and tells the subnet to establish the V.C. This leads to the second row in the table. Note that we have a conflict here because A can easily distinguish conn^c 1 packets from H_1 and conn^c 1 packets from H_3 but C cannot do this. For this reason, A assign a different conn^c identifier to the outgoing traffic for the second conn^c.

Comparison of VC and datagram subnet –

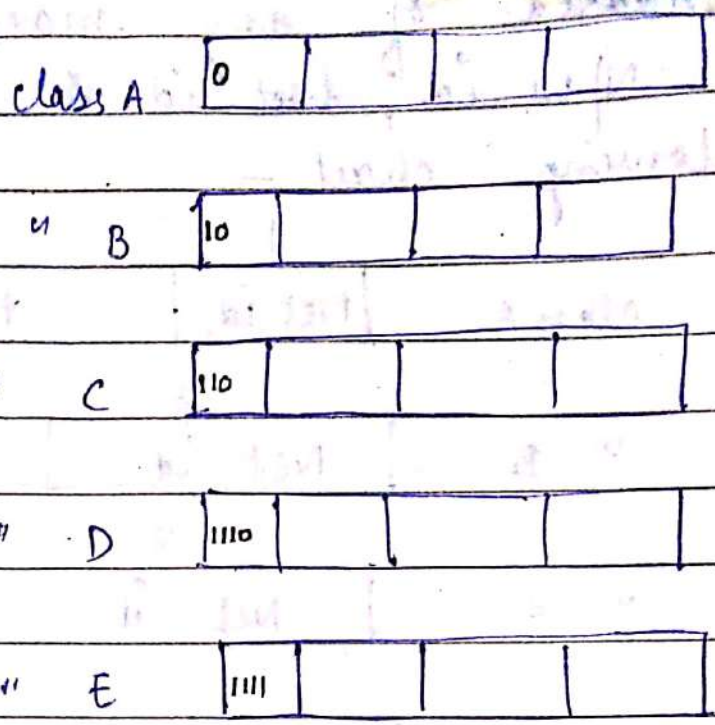
Issue	Datagram subnet	VC subnet
circuit setup	Not needed	Required.
Addressing	Each packet contains full source & dest" address.	Each packet contains a short VC number.
State information	Routers donot hold state information about connections	Each VC requires router table space per connection
Routing	Each packet routed independently.	Route selected when VC is setup & all packets follow it.
Effect of Router failure	None except for packets lost during crash.	All VC's that passed through the failed router are terminated.
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC.
Repairs	Easy to Repair	harder to repair.

IP Addresses – (Logical address or IPV4 addresses)

IPV4 → 32 bit address

Total no. of possible addresses is 2^{32}. This is address space. Each device on the Internet has a unique address called IP address.

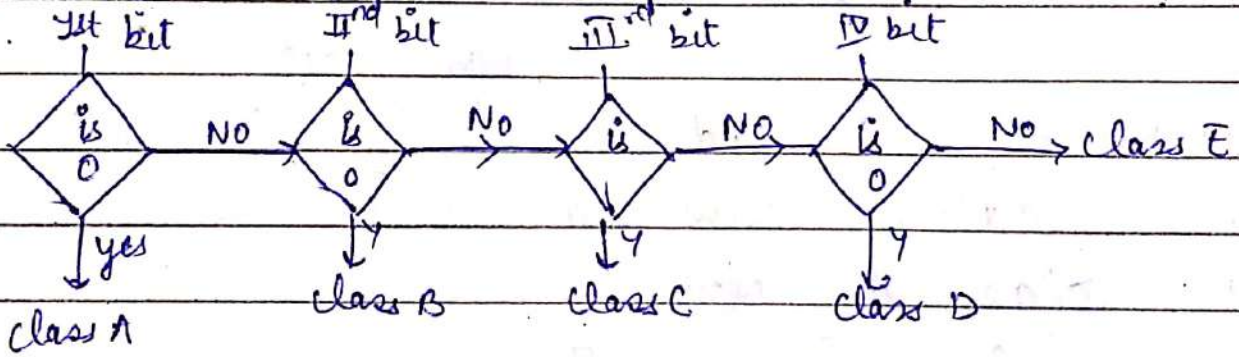
Classful Addressing –



- 4 byte address
- It uses 2 notations
1.) Binary
2.) Dotted Decimal

Binary – 10000000 00001011 00000011 00011111

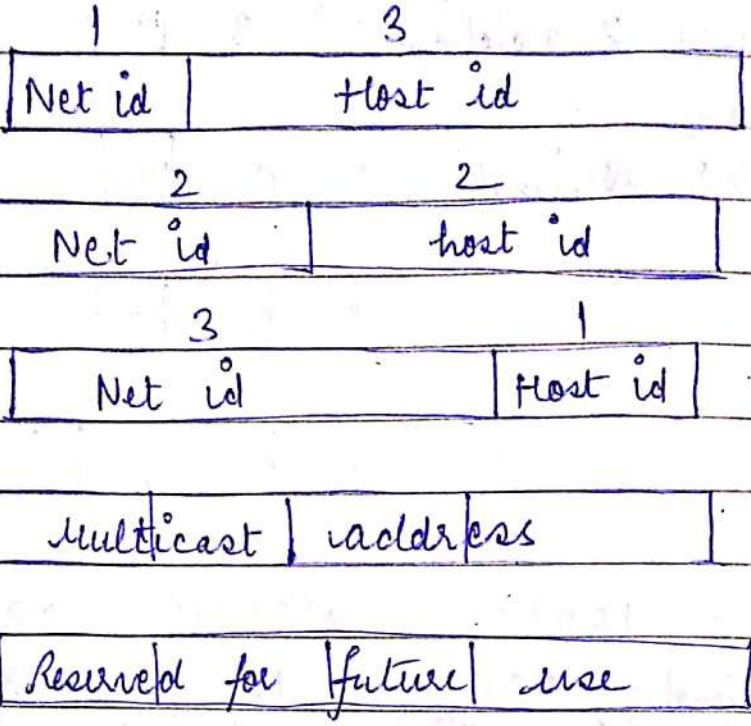
Dotted decimal – 128 . 11 . 3 . 31



For dotted decimal

class A	0 to 127
class B	128 to 191
" C	192 to 223
" D	224 to 239
" E	240 to 255

IP address of any machine can be used to find N/W id, host id & N/W address acc. to following chart –



N/W M/C.

Ques. a) Given the address 23.56.7.91, find the N/W address, N/W id and the host id.

Ans. class A. N/W

Net id – 23

host id – 56.7.91

N/W address – 23.0.0.0

b.) 132.6.17.85

class B m/W

Net id – 132.6.

host id – 17.85

N/W address – 132.6.0.0

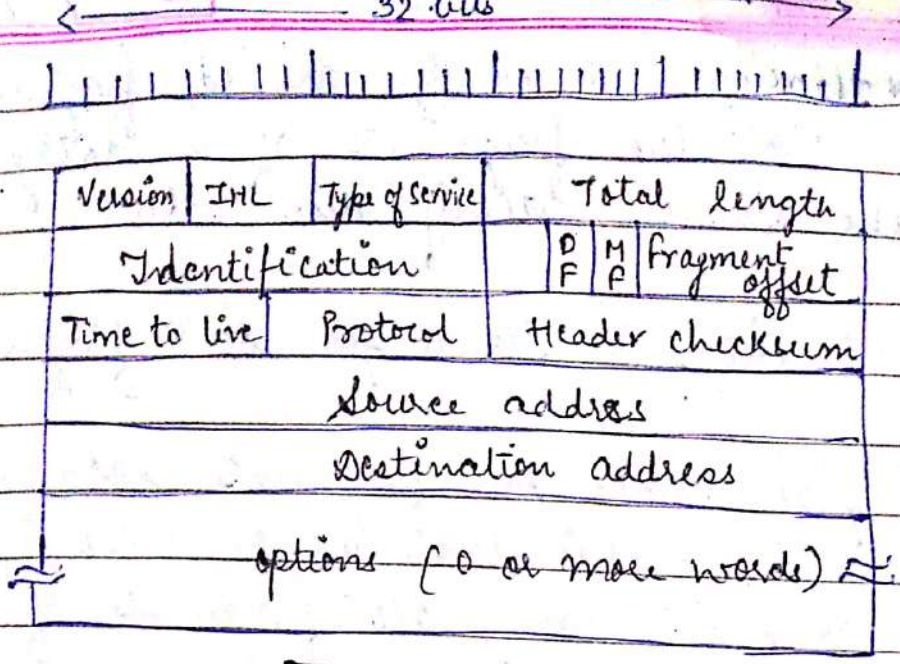
Ques. A N/W address is given as 17.0.0.0. find its class.

→ It is class A ~~addre~~ N/W.

IPV4-

IPV4 is the delivery mechanism used by TCP/IP protocol. IPV4 is unreliable & connectionless datagram protocol. If reliability is important, IPV4 must be paired with a reliable protocol such as TCP IPV4 uses the datagram approach, this means that each datagram is handled independently and each datagram can follow a different route to the destination. This implies that the datagrams sent by the same source to the same destination can arrive out of order. Also some can be corrupted during transmission. To take care of these problems, IPV4 relies on a higher level protocol.

Packets in the IPV4 are called datagrams. An IPV4 datagram consist of a header part and data part. The header is a 20 byte fixed part and a variable length optional part. The IPV4 datagram format is shown in figure -



IP PACKET

Version – This ~~format~~ 4-bit field defines the version of the protocol. For the IPV4, its value is 4. For IPV6, its value is 6.

IHL – IHL is provided to tell how long the header is in 32 bit words. Min. value of IHL is 5 & max. value is 15.

Type of Service – It define the service out of the various services provided by various protocols.
e.g: ICMP, IGMP, Bootp
(Internet control message protocol)

Total Length – It is a 16 bit field. It defines the total length of datagram including the header. The maximum length can be 65,535 bytes. To find the length of data, we can use,

Length of data = Total length - header length

Identification – This field is used to determine

which datagram, a newly arrived fragment belongs to. All the fragments of a datagram contain the same identification value.

DF- This 1 bit field stands for don't fragment.

MF- (More fragments). All fragments except the last one has this bit as one. It is required to know when all fragments of a datagram have arrived.

Fragment offset - It tells where in the current datagram, this fragment belongs to. It is 13 bit field, therefore max. value is 8192 fragments per datagram.

Time to Live - This field is a counter used to limit packet lifetime. When a source sends the datagram, it stores a number in this field which is decremented on each router. The datagram is discarded when the value becomes zero.

Protocol - This 8 bit field defines the higher level protocol that uses the services of IPV4.
eg. TCP

Header Checksum - It verifies the header only.

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

Dest^{n} address - This 32 bit field defines IP address of the destination.

FRAGMENTATION EXAMPLE

Note: The offset is measured in units of 8 bytes

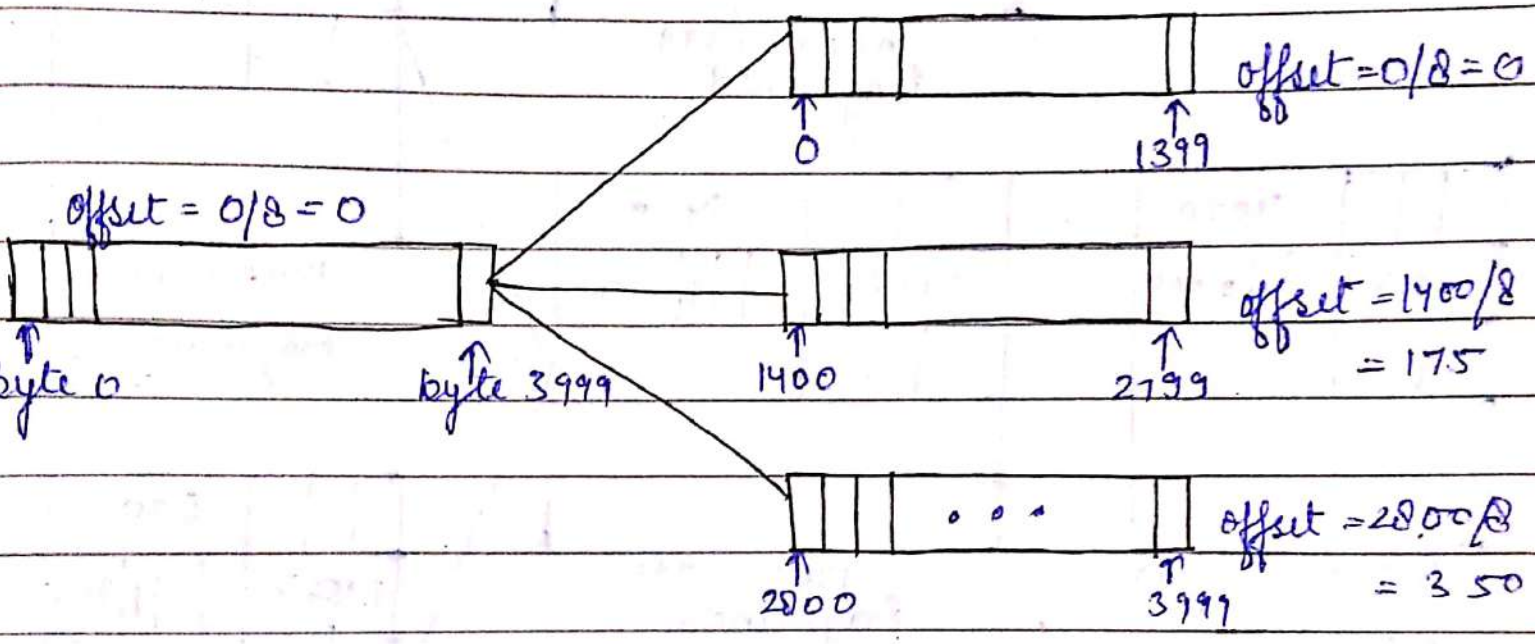


Fig. shows an example of a DATAGRAM with a DATA SIZE of 4000 BYTES fragmented into 3 SEGMENTS

IPV6 :- (Internetworking Protocol, version 6)

IPV6 has some advantages over IPV4 that can be summerised as follows :-

Longer Address Space :- An IPV6 address is 128 bits long compared with the 32 bit address of IPV4

Better Header format → IPV6 uses a new header format in which options are seperated from the base header and inserted when needed.

New options :- IPV6 has new options to allow for additional functionalities.

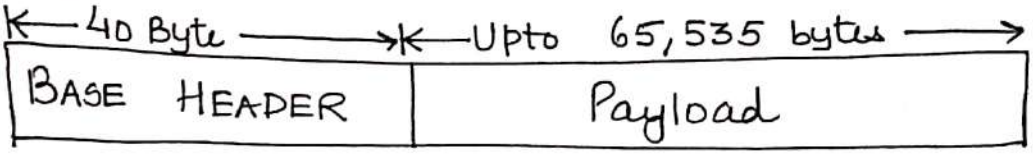
Allowance for Extension :- IPV6 is designed to allow the extension of the protocal, if required by new technologies or applications.

Support for resource allocations :- In IPV6, type of service field has been removed, but a mechanism (called flow label) has been added to enable the source to request special handling of the packet.

Support for more Security:- The encryption & authentication options in IPV6 provide confidentiality & integrity of the packet.

IPV6 Packet format

IPV6 packet is shown below:-



The payload consists of 2 parts:-

→ Optional extension headers

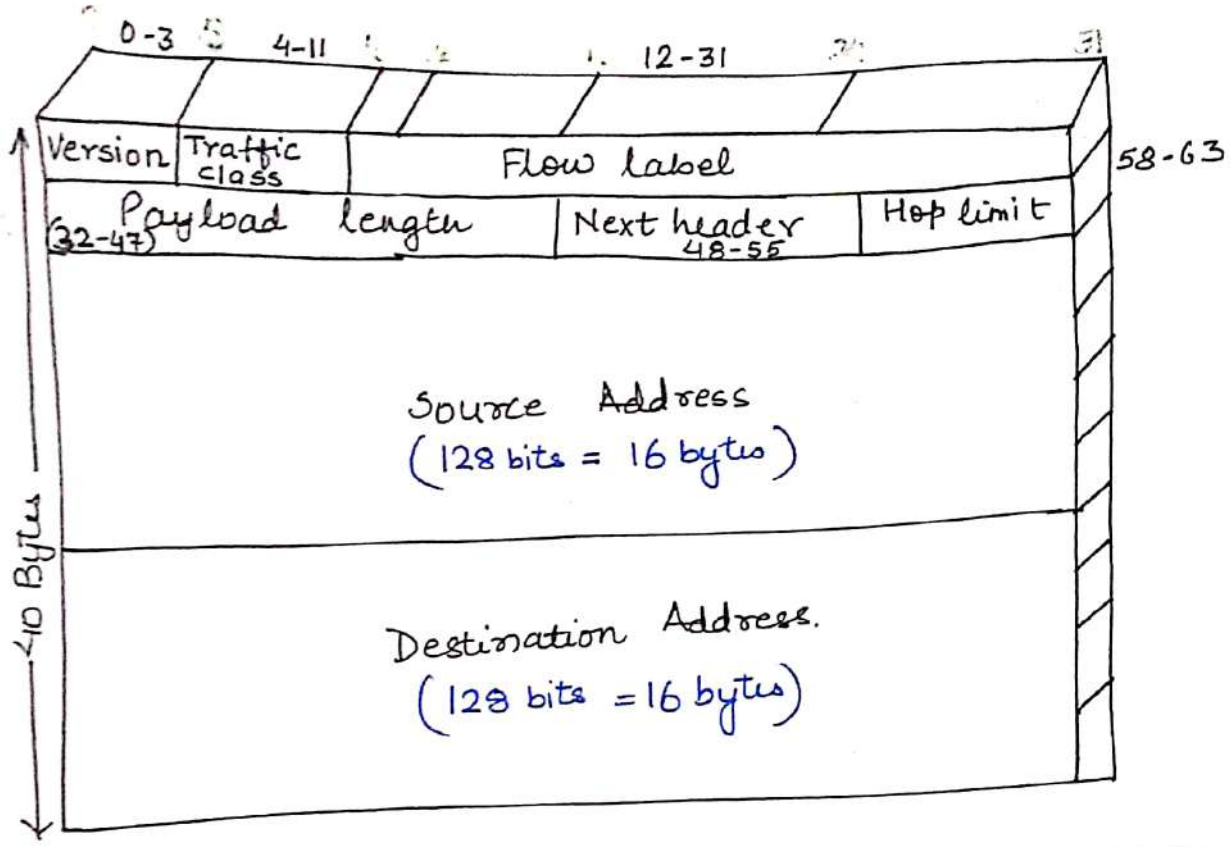
→ data from upper layers.

Fixed Header

→ All the necessary information that is essential for a router is kept in the fixed header.

→ The Extension header contains optional information that helps routers to understand how to handle a packet/flow.

→ The IPV6 fixed header has a fixed length of 40 bytes, consisting of the following fields.



Version :- (4bits) Represents the version of Internet protocol
i.e 0110 → 6.

Traffic class :- (8bits) field is used to distinguish b/w packets with different real time delivery requirements.

Flow Label :- (20 bits) Field is designed to provide special handling for particular flow of data.

Payload Length :- (16 bits) This field is used to tell the routers how much information, a particular packet contains in its payload.

Next header (8 bits) :- Identifies the type of header immediately following the IPV6 header, this will either be an IPV6 extension header or a higher level header, such as TCP or UDP.

Hop limit (8 bits) :- This field is used to stop packet to loop in the network infinitely. The hop limit is set to some desired maximum value by the source & decremented by 1 by each node that forwards the packet. The packet is discarded if Hop limit is decremented to zero.

Source Address (128 bits) → This indicates the address of originator of the packet.

Destination Address (128 bits) → This field provides the address of intended recipient of the packet.

Extension Headers
- → Hop by hop options
- → Routing Header
- → Fragment Header
- → Authentication Header
- → Encapsulating security payload header.
- → Destination options header.

Hop-by Hop options header → Defins special options that require hop-by-hop processig.

Routing header :- Provids extended routing, contains methods to support making routing decision.

Fragment Header :- Contains fragmentation & reassembly information.

Authentication Headr :- Provides packunt integrity & authuntication

Encasulating Security Payload header :- Provide privaly.

Destination options header :- Contain optional information to be examined by the distination node.