INTERNET PROTOCOL

→ The main network protocol is internet protocol (IP). IP is an unreliable & connectionless protocol that provides its best effort to deliver the datagram to its destination. But IP doesnot give any guarantee of reliable data transfer.

→ IP doesnot support flow control & error control mechanism. Therefore, it is an unreliable protocol.

→ All the datagram or packets that are produced in IP protocol from the same message behave independent of each other & the datagrams take different path or route to arrive at the destination. Hence IP provides connectionless service.

→ IP protocol is of 2 different types. They are:-

(a) IPV4.

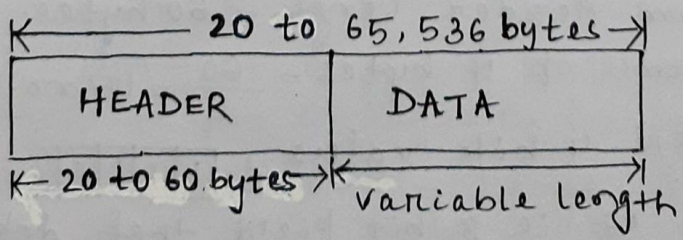
(b) IPV6.

a) IPV4 (Internet protocol version 4)

→ It is a version of IP. Packets in IPV4 is known as datagram. A datagram is a variable length packet consist of 2 different parts. They are,

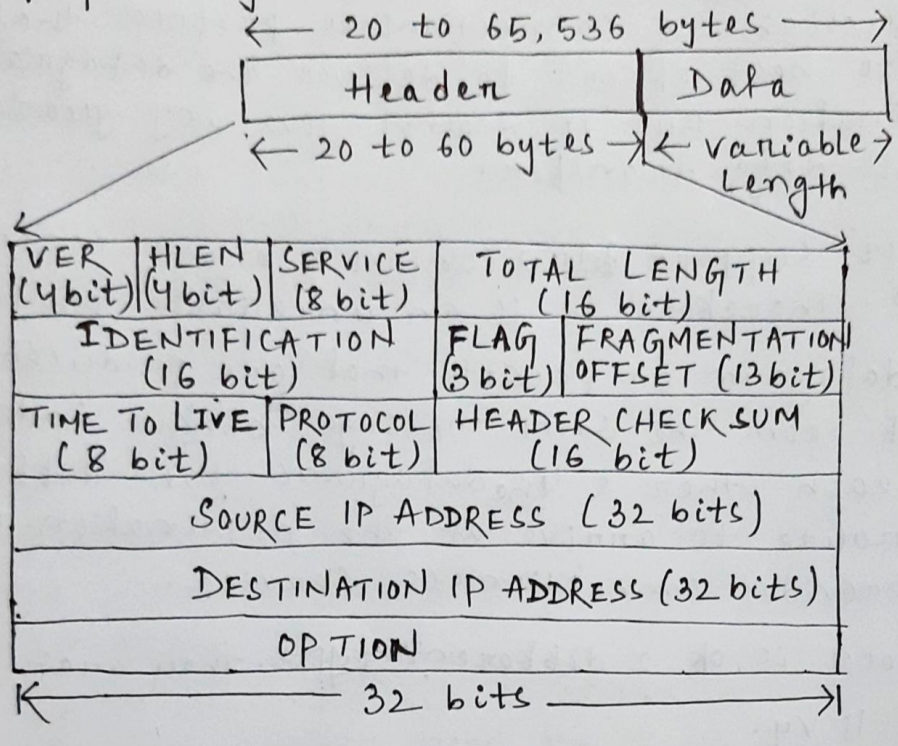
- Header
- Data

→ The Header is of 20 to 60 bytes in length & contain necessary information to routing & delivery.



Description of IPv4 Header →

IPv4 Datagram Header format,



(a) VER (VERSION) – It is 4 bit field that defines the version of IP address. i.e: whether the IP address is of version 4 or version 6. (IPv4 or IPv6).

(b) Header Length (HLEN) – It is 4 bit field that define the header size of datagram & in terms of 4 bytes.

Minimum Header Length = 20 byte.

in terms of 4 bytes = $\frac{20}{4}$ = 5 no. of 4 bytes

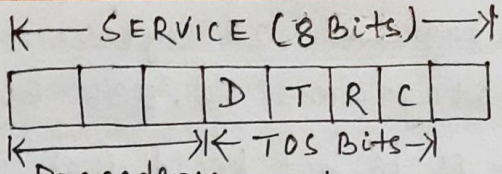
So, HLEN 4 bits value, | 0 | 1 | 0 | 1 |

Maximum Header Length = 60 bytes.

in terms of 4 bytes = $\frac{60}{4}$ = 15 no. of 4 bytes.

So, HLEN 4 bits value, | 1 | 1 | 1 | 1 |

(c) SERVICE – It is 8-bit field that define the service types. The types of services are,



↳ Type of Service

D : Minimize Delay

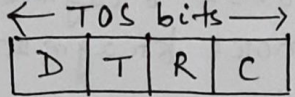
T : Maximize Throughput

R : Maximize Reliability

C : Minimize Cost.

Precedence :- The first 3 bits field of service is known as precedence field. The precedence field value range from 000 (=0) to 111 (=7). The precedence defines priority of datagram. Whenever there is congestion over network then some of the datagrams get dropped. So in this case the datagrams with lowest precedence value or lowest priority get dropped.

TOS field :- It is 4 bit subfield with each bit have a special meaning. Only one bit can be '1' at a time. Each bit position can be either 0 or 1 but only a single bit can be 1 at a time.



				Description
0	0	0	0	Normal (Default)
0	0	0	1	Minimize Cost
0	0	1	0	Maximize Reliability
0	1	0	0	Maximize Throughput
1	0	0	0	Minimize Delay.

(d) Total Length - It is 16 bits field that defines total length of the datagram in bytes. i.e:

Total Length of Datagram = Length of Header
+
Length of Data

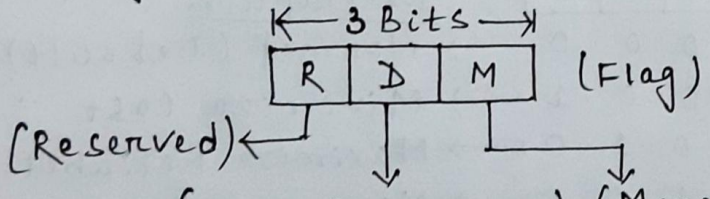
Minimum Length of Datagram = 20 Bytes.
Maximum Length of Datagram = 65,536 Bytes.

(c) IDENTIFICATION – It is 16 bit field that is used when datagram is fragmented. Identification field identifies a datagram originating from the source host.

The datagram identification number along with source IPv4 address will uniquely identifies a datagram of a host. There is a counter that is initialized to a (+ve) number & go on increament by 1 for subsequent new generated datagram. This counter's current value is copied to identification field. But when a datagram is fragmented then the identification value for all the fragments of the same datagram is same as the identification value of original datagram.

This helps in assembling all the fragments of same identification value into one datagram

(d) Flags – It is 3 bit field whose 1st bit is reserve and 2nd bit is for donot fragment. The 3rd bit of flag field is for more fragment.



→ If D = 1, then the datagram must not be fragmented.

→ If D = 0, then the datagram can be fragmented.

→ If M = 1 then this datagram is not the last fragment or some more fragments of datagrams are there.

→ If M = 0, then this is the last fragment of the datagram.

(g) Fragmentation offset → It is 13 bit field that shows the relative position of this fragment with respect to the whole datagram.

It is the offset of the data in the original datagram measured in units of 8 bytes.

e.g- Original datagram size = 1024 bytes.
(0 to 1023)

when this original datagram is fragmented, each fragment carrying 32 bits, then the fragmentation offset is,

Fragment 0 → 0 to 31 → Fragmentation offset = 0
0/8 = 0

Fragment 1 → 32 to 63 → Fragmentation offset = 4
32/8 = 4

Fragment 2 → 64 to 95 → Fragmentation offset = 8
64/8 = 8

Fragment 3 → 96 to 127 → Fragmentation offset = 12
96/8 = 12

& so on.

NOTE: Fragmentation - Divide the datagram to make it possible to pass through the network.
Divide according to maximum transfer unit (MTU) size of protocol used in network

(h) Time to Live (TTL) - It is 8 bit field that define timestamp or limitation over lifetime when a datagram is travelling through an Internet.

TTL value is decreamented by 1 when a datagram visited a router. when TTL value decreases to '0' then the datagram is discarded from the network.

When a source host sends datagram then the source host set TTL value in its datagram which is approxi-mately 2 times the maximum no. of routers between any two host.

(i) Protocol - It is 8bit field that defines high level protocol that uses the services of IPV4.

Different high level protocols that uses the services of IPV4 are, ICMP, IGMP, TCP, UDP etc.

The protocol values for these high level protocols by using 8 bit can be,

High Level protocol	protocol values
ICMP	1 (0000 0001)
IGMP	2 (0000 0010)
TCP	6 (0000 0110)
UDP	17 (0001 0001)

(j) Header checksum - It is 16 bit field that check whether there is an error in the header of the datagram or not.

(k) Source Address - It is 32-bit field that defines the IPV4 address of the source.

(l) Destination Address - It is 32-bit field that defines IPV4 address of destination.

—o—

b) IPV6 Header Format- (or IPng - Internetworking Protocol, next generation)

(Internet Protocol version 6)

Advantages of IPV6 over IPV4 are-

1. Real time audio & video transmission requires minimum delay & reservation of resources, which is supported by IPV6 not IPV4.
2. Encryption or Decryption of Data and authentication of data is supported by IPV6 not IPV4.
3. Address space of IPV6 is of larger size than IPV4

IPV6 address space size: 2^{128}

IPV4 address space size: 2^{32}

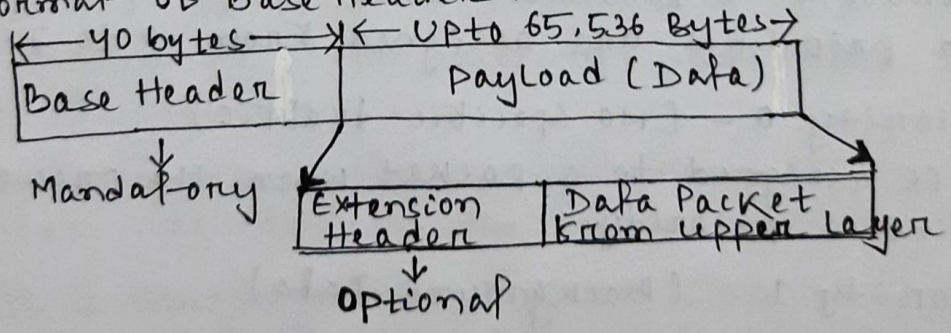
Packet Format of IPV6 Datagram

→ Packet consist of mandatory base header followed by payload or data. And the payload consist of optional header extension followed by data from upper layer.

→ Base header occupies 40 bytes.

→ Extension header & data from upper layer occupies upto 65,536 bytes.

→ Format of Base Header →



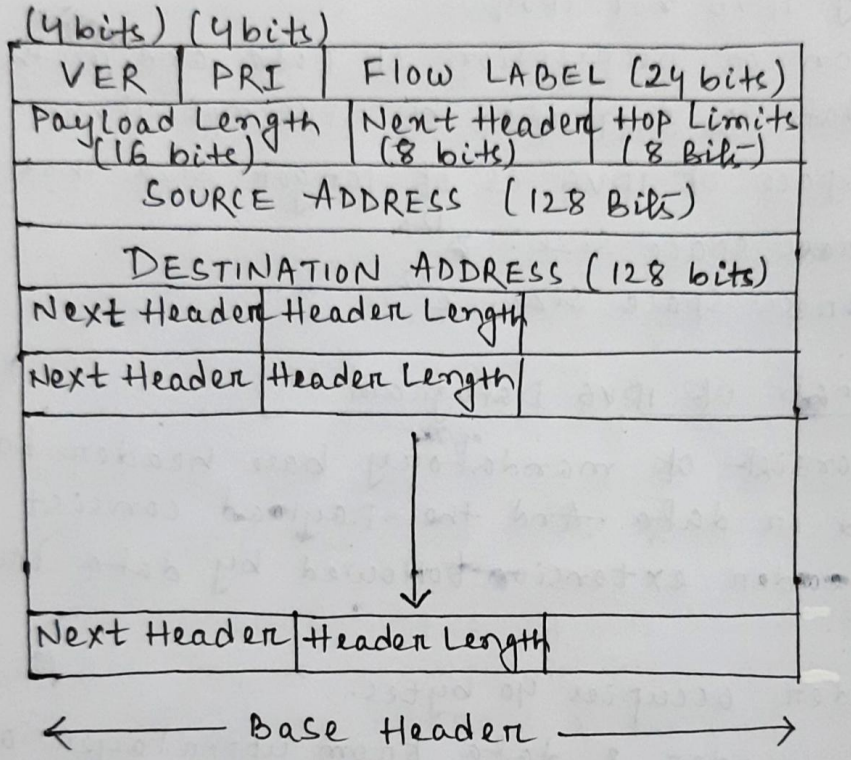
Description of different fields of Base header:-

a) version (VER) - It is 4bit field that define the version number of IPV6.

b) Priority (PRI) - It is 4bit priority field that define priority of packets with respect to traffic congestion, so that during congestion time the

low priority packets can be discarded than high priority. Two different types of data traffic in IPV6 are :-

→ Congestion controlled.
→ Non-congestion controlled.



→ On Congestion Controlled, a source adapt itself to traffic to slowdown when there is congestion. Here priorities are assigned from 0 to 7.

Priority 0 - (No specific traffic)
It is assigned to a packet when the process doesnot define a priority.

Priority 1 - (Background Data)
It is assigned to a packet that are usually delivered in background.
e.g. News Deliver

Priority 2 - (Unattended Data traffic)
It is assigned to packet when the receiver of the sending packet doesnot wait for the data to be received. e.g - e-mail

Priority 4-(Attended Bulk Data transfer)
It is assigned to packet when a user is waiting to receive the data (with Delay). e.g- FTP or HTTP

Priority 6-(Interactive traffic)
It is assigned to TELNET packets where user interactions are required.

Priority 7 - (control traffic)
It is assigned to network management or SNMP Packets.

→ In Non-congestion Controlled traffic, a source doesnot adapt itself to congestion. Here the data traffic expects minimum delay & discarding of packets is not desirable. e.g- Real-time audio & video

Priority for non-congestion controlled data traffic are assigned from 8 to 15.

c) Flow Control - It is 24 bits field that provide handling for a perticular flow of data. The combin-ation of source address & the value of flow label uniquely define a flow of packets. It is handled by router. To a router, a flow is a sequence of packets that share the same characteristics s.a. same source same destination, same priority, same path, same kind of security.

In flow label table, each entry defines the services required by the corresponding flow label.

If a source doesnot support flow label then the source set the flow label field to '0'.

If a router doesnot support flow label then the router simply ignores it.

Flow label assigned to a packet by source host is a random number between 1 to $(2^{24}-1)$. This assigning of random number can not be reused again.

d) Payload Length - It is 2 byte field that defines length of IP Datagram excluding Base header.

e) Hop Limit - It is 8-bit field same as like TTL (Time-to-Live) field of IPv4.

f) Source Address - It is 128 bit IPV6 address of the original source that has generated the datagram or packet.

g) Destination Address - It is 128 bit IPV6 address that identify the final destination or required destination.

h) Next Header - It is 8 bit field that define the header that follows the base header in the datagram.

The Next header is either one of the optional extension header used by IP or the header of an encapsulated packet E.g. TCP or UDP.

—o—