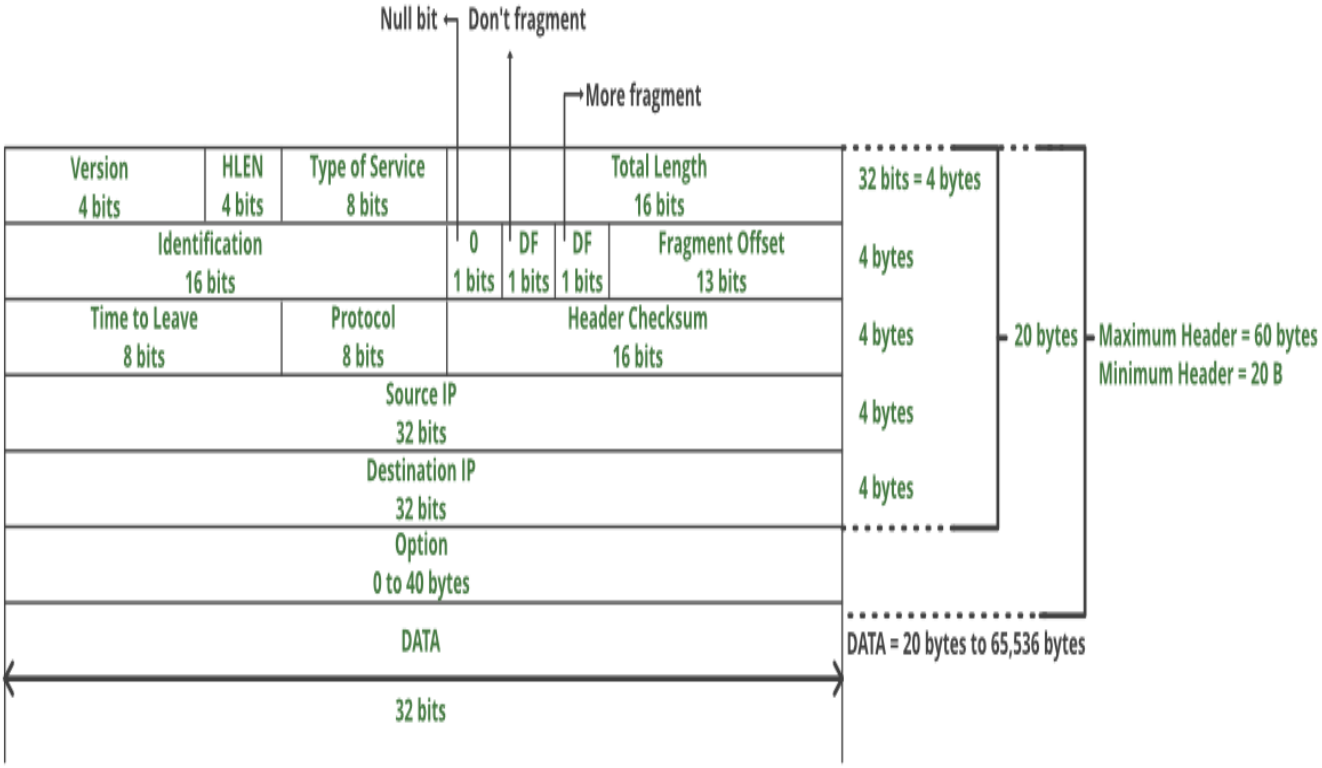
IPv4 Datagram Header
Size of the header is 20 to 60 bytes.



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 h eader. 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 valu e 20 bytes and the maximum is 65,535 bytes.*

Identification: *Unique Packet Id for identifying the group of fragments of a si ngle IP datagram (16 bits)*

Flags: *3 flags of 1 bit each : reserved bit (must be zero), do not fragment fla g, more fragments flag (same order)*

Fragment Offset: *Represents the number of Data Bytes ahead of the partic ular fragment in the particular Datagram. Specified in terms of number of 8 b ytes, which has the maximum value of 65,528 bytes.*

Time to live: *Datagram’s lifetime (8 bits), It prevents the datagram to loop th rough the network by restricting the number of Hops taken by a Packet befor e delivering to the Destination.*

Protocol: *Name of the protocol to which the data is to be passed (8 bits)*

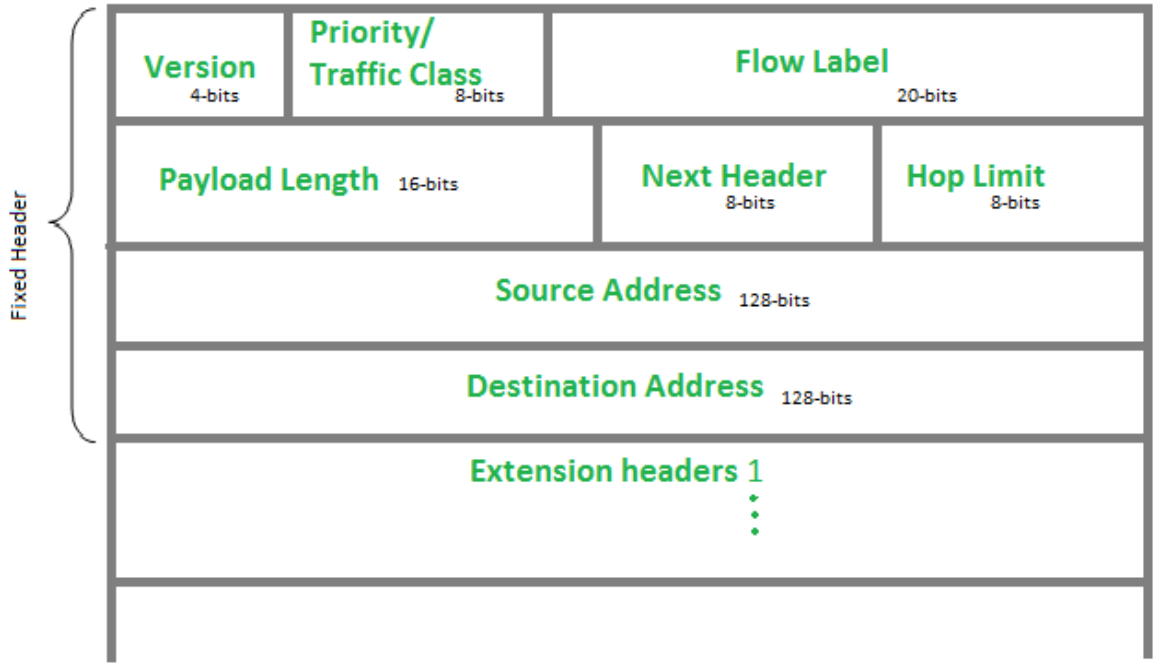
Header Checksum: *16 bits header checksum for checking errors in the data gram header*

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 th e Network administrator to check whether a path is working or not.*

IP version 6 Header Format: 128,bit long address 2^128 bits.



Version (4-bits): Indicates version of Internet Protocol.

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.

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.

Payload Length (16-bits): It is a 16-bit 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.

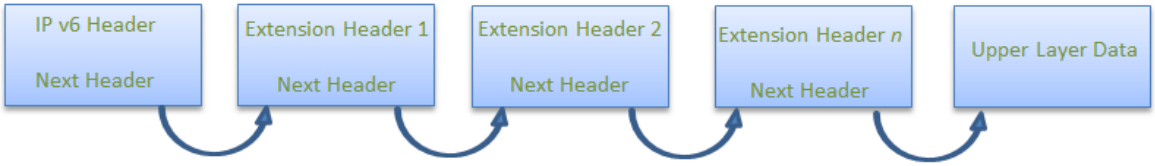
Next Header (8-bits): Next Header indicates the type of extension header(if present) immediately following the IPv6 header

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 .

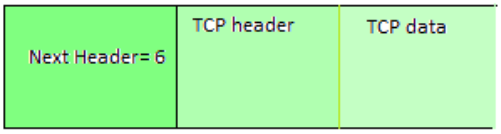
Extension Headers: In order to rectify the limitations of the *IPv4 Option Field*, Extension Headers are introduced in IP version 6. The extension header mechanism is a very important part of the IPv6 architecture. The next Header field of IPv6 fixed header points to the first Extension Header and this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



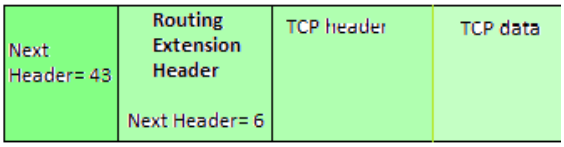
IPv6 packet may contain zero, one or more extension headers but these should be present in their recommended order:

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