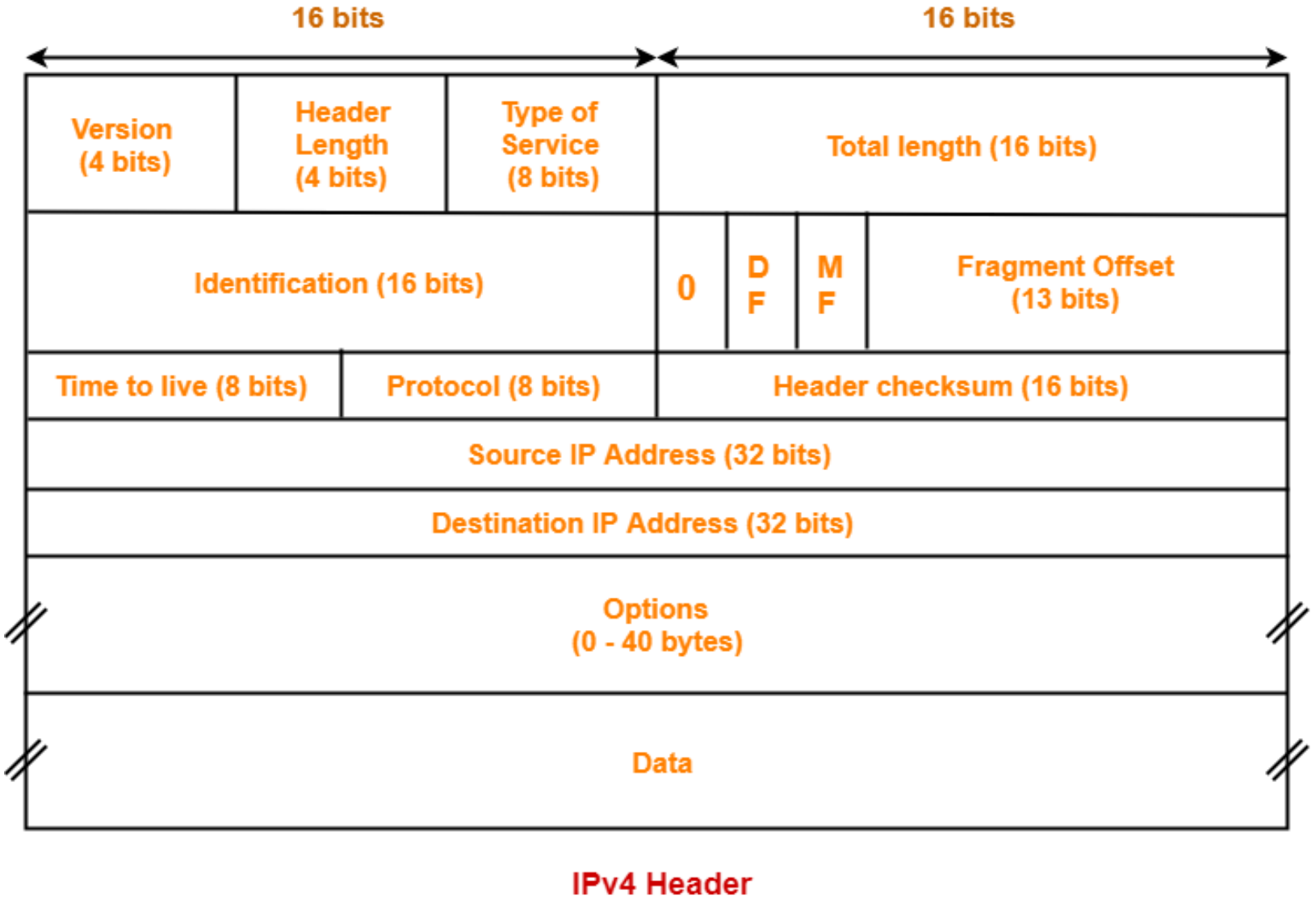
Internet Protocol Version 4

Overview

- IPv4 short for Internet Protocol Version 4 is the fourth version of the Internet Protocol (IP).
- IP is responsible to deliver data packets from the source host to the destination host.
- This delivery is solely based on the IP Addresses in the packet headers.
- IPv4 is the first major version of IP.
- IPv4 is a connectionless protocol for use on packet-switched networks.

IPv4 Header



IPv4 Header

Version

- Version is a 4-bit field that indicates the IP version used.
- The most popularly used IP versions are version-4 (IPv4) and version-6 (IPv6).
- Only IPv4 uses the above header.
- So, this field always contains the decimal value 4

Header Length

- Header length is a 4-bit field that contains the length of the IP header.
- It helps in knowing from where the actual data begins.
- Header length and Header length field value are two different things.
- Header length = Header length field value x 4 bytes
- The range of header length field value is always [5, 15].
- The range of header length is always [20, 60].

Type of Service

- Type of service is an 8-bit field that is used for Quality of Service (QoS).
- The datagram is marked for giving a certain treatment using this field.

Total Length

- Total length is a 16-bit field that contains the total length of the datagram (in bytes).
- Total length = Header length + Payload length
- Minimum total length of datagram = 20 bytes (20 bytes header + 0 bytes data)
- Maximum total length of datagram = Maximum value of 16-bit word = 65535 bytes

Identification

- Identification is a 16-bit field.
- It is used for the identification of the fragments of an original IP datagram.
- When an IP datagram is fragmented,
  - Each fragmented datagram is assigned the same identification number.
  - This number is useful during the re assembly of fragmented datagrams.
  - It helps to identify to which IP datagram; the fragmented datagram belongs to.

DF Bit

- DF bit stands for Do Not Fragment bit.
- Its value may be 0 or 1.
- When DF bit is set to 0,
  - It grants the permission to the intermediate devices to fragment the datagram if required.
- When DF bit is set to 1,
  - It indicates the intermediate devices not to fragment the IP datagram at any cost.
  - If network requires the datagram to be fragmented to travel further but settings does not allow its fragmentation, then it is discarded.
  - An error message is sent to the sender saying that the datagram has been discarded due to its settings.

MF Bit

- MF bit stands for More Fragments bit.
- Its value may be 0 or 1.
- When MF bit is set to 0,
  - It indicates to the receiver that the current datagram is either the last fragment in the set or that it is the only fragment.
- When MF bit is set to 1,
  - It indicates to the receiver that the current datagram is a fragment of some larger datagram.
  - More fragments are following.
  - MF bit is set to 1 on all the fragments except the last one.

Fragment Offset

- Fragment Offset is a 13-bit field.
- It indicates the position of a fragmented datagram in the original unfragmented IP datagram.
- The first fragmented datagram has a fragment offset of zero.

Time To Live

- Time to live (TTL) is an 8-bit field.
- It indicates the maximum number of hops a datagram can take to reach the destination.
- The main purpose of TTL is to prevent the IP datagrams from looping around forever in a routing loop.
- The value of TTL is decremented by 1 when-
  - Datagram takes a hop to any intermediate device having network layer.
  - Datagram takes a hop to the destination.
- If the value of TTL becomes zero before reaching the destination, then datagram is discarded.

Protocol

- Protocol is an 8-bit field.
- It tells the network layer at the destination host to which protocol the IP datagram belongs to.
- In other words, it tells the next level protocol to the network layer at the destination side.
- Protocol number of ICMP is 1, IGMP is 2, TCP is 6 and UDP is 17.

Header Checksum

- Header checksum is a 16-bit field.
- It contains the checksum value of the entire header.
- The checksum value is used for error checking of the header.

Source IP Address

- Source IP Address is a 32-bit field.
- It contains the logical address of the sender of the datagram.

Destination IP Address

- Destination IP Address is a 32-bit field.
- It contains the logical address of the receiver of the datagram.

Options

- Options is a field whose size vary from 0 bytes to 40 bytes.
- This field is used for several purposes such as-
  - Record route
  - Source routing
  - Padding

Record Route

- A record route option is used to record the IP Address of the routers through which the datagram passes on its way.
- When record route option is set in the options field, IP Address of the router gets recorded in the Options field.

Source Routing

- A source routing option is used to specify the route that the datagram must take to reach the destination.
- This option is generally used to check whether a certain path is working fine or not.
- Source routing may be loose or strict.

Padding

- Addition of dummy data to fill up unused space in the transmission unit and make it conform to the standard size is called as padding.
- Options field is used for padding.

Why New IP Version?

- Internet has grown exponentially and the address space allowed by IPv4 is saturating. There is a requirement to have a protocol that can satisfy the needs of future Internet addresses that is expected to grow in an unexpected manner.
- IPv4 on its own does not provide any security feature. Data has to be encrypted with some other security application before being sent on the Internet.

- Data prioritization in IPv4 is not up to date. Though IPv4 has a few bits reserved for Type of Service or Quality of Service, but they do not provide much functionality.
- IPv4 enabled clients can be configured manually or they need some address configuration mechanism. It does not have a mechanism to configure a device to have globally unique IP address.

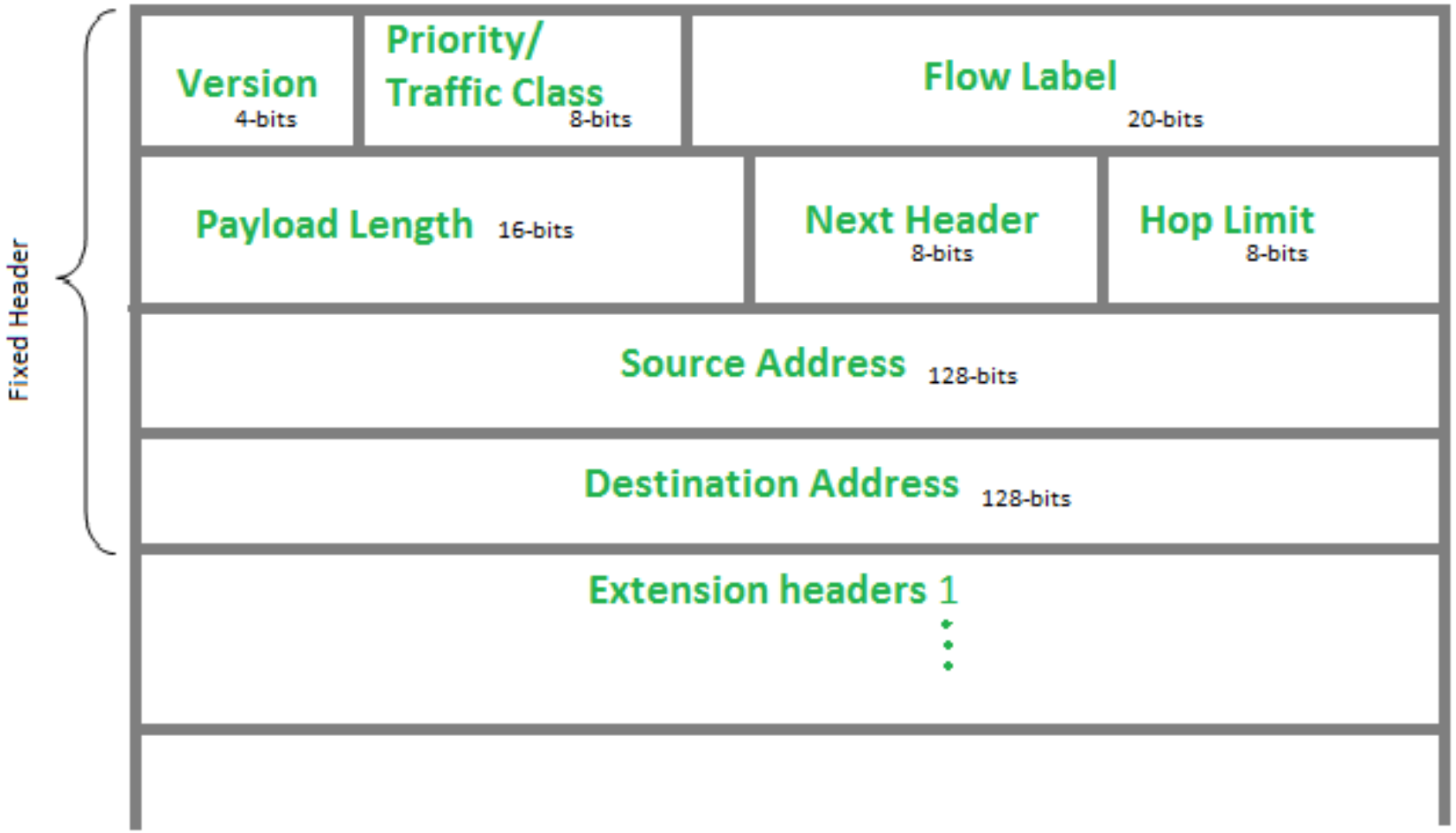
Internet Protocol Version 6

Internet Protocol version 6 (IPv6)

- IPv6 was developed by Internet Engineering Task Force (IETF) to deal with the problem of IP v4 exhaustion.
- IPv6 is 128-bits address having an address space of 2^128, which is way bigger than IPv4.
- IPv6 uses Colon-Hexa representation. There are 8 groups and each group represent 2 Bytes.
- IP version 6 is the new version of Internet Protocol, which is way better than IP version 4 in terms of complexity and efficiency.

IPv6

IPv6 Header


Fixed Header
Version
4-bits
Priority/
Traffic Class
8-bits
Flow Label
20-bits
Payload Length
16-bits
Next Header
8-bits
Hop Limit
8-bits
Source Address
128-bits
Destination Address
128-bits
Extension headers 1

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 priority of the packet. If congestion occurs on router then packets with least priority will be discarded.
- As of now only 4-bits are being used (and 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.

Traffic Class (8-bits)

- 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

Traffic Class (8-bits)

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

Flow Label (20-bits)

- Flow Label field is used by 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, intermediate router can use source address, destination address and flow label of the packets.

Flow Label (20-bits)

- Between a source and destination multiple flows may exist because many processes might be running at the same time.
- Routers or Host that do 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, source is also supposed to specify the lifetime of flow.

Payload Length (16-bits)

- It is a 16-bit (unsigned integer) field, indicates total size of the payload which tells routers about amount of information a particular packet contains in its payload.
- Payload Length field includes extension headers (if any) and upper layer packet.
- In case length of 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 jumbo payload option is used in the Hop-by-Hop options extension header.

Next Header (8-bits)

- Next Header indicates type of extension header (if present) immediately following the IPv6 header.
- Whereas In some cases it indicates the protocols contained within upper-layer packet, such as TCP, UDP.

Hop Limit (8-bits)

- Hop Limit field is 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 packet is discarded if value decrements to 0.
- This is used to discard the packets that are stuck in infinite loop because of some routing error.

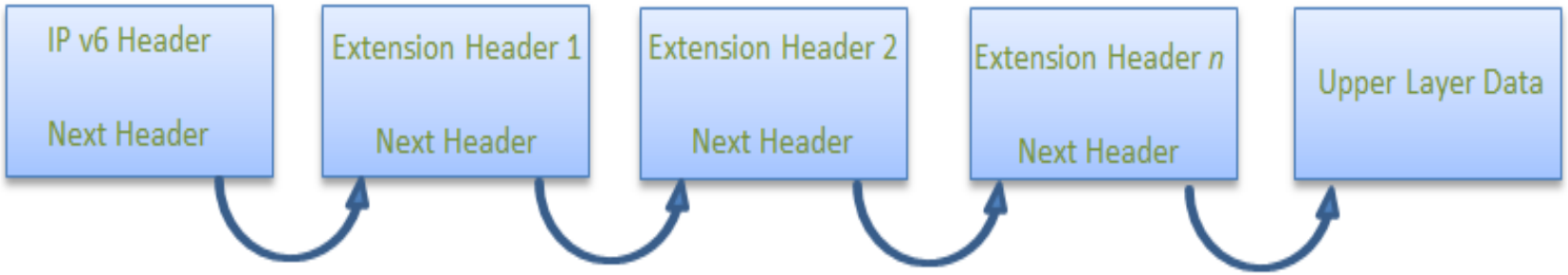
Source Address
Destination Address

- **Source Address** (128-bits): Source Address is 128-bit IPv6 address of the original source of the packet.
- **Destination Address** (128-bits): 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 IPv4 Option Field, Extension Headers are introduced in IP version 6.
- The extension header mechanism is very important part of the IPv6 architecture.
- 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.

Extension Headers



Difference Between IPv4 and IPv6

IPv4	IPv6
IPv4 has 32-bit address length	IPv6 has 128-bit address length
It Supports Manual and DHCP address configuration	It supports Auto and renumbering address configuration
In IPv4 end to end connection integrity is Unachievable	In IPv6 end to end connection integrity is Achievable
It can generate 4.29×109 address space	Address space of IPv6 is quite large it can produce 3.4×1038 address space
Security feature is dependent on application	IPSEC is inbuilt security feature in the IPv6 protocol
Address representation of IPv4 in decimal	Address Representation of IPv6 is in hexadecimal
Fragmentation performed by Sender and forwarding routers	In IPv6 fragmentation performed only by sender
In IPv4 Packet flow identification is not available	In IPv6 packetflow identification are Available and uses flow label field in the header
In IPv4 checksumfield is available	In IPv6 checksumfield is not available
It has broadcast Message Transmission Scheme	In IPv6 multicast and any cast message transmission scheme is available
In IPv4 Encryption and Authentication facility not provided	In IPv6 Encryption and Authentication are provided