IP Address in Networking

IPv4 Header Format

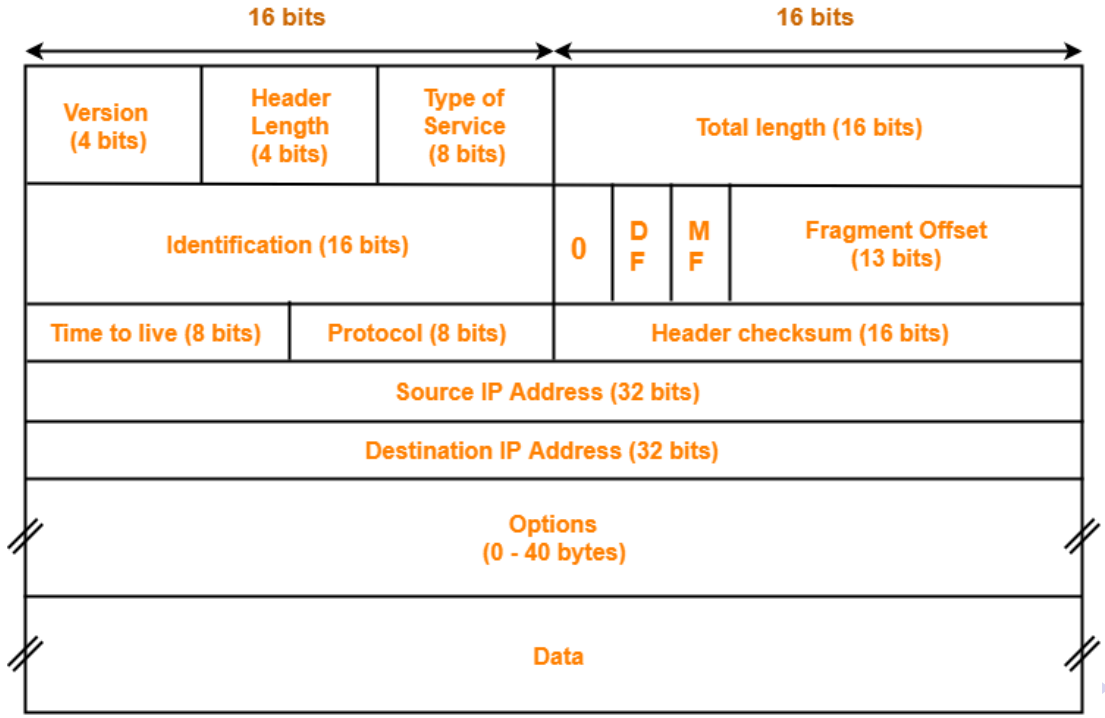
Munesh Singh

Indian Institute of Information Technology, Design and Manufacturing Kancheepuram,
Chennai, Tamil Nadu 600127

November 13, 2020

IPV4

- 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 a connectionless protocol for use on packet-switched networks.



Field of IPV4

- 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.
- It is important to note-
  - Datagrams belonging to different versions have different structures.
  - So, they are parsed differently.
  - IPv4 datagrams are parsed by version-4 parsers.
  - IPv6 datagrams are parsed by version-6 parsers.

Field of IPV4

- 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.
- **Minimum And Maximum Header Length**
  - The length of IP header always lies in the range- [20 bytes , 60 bytes]
- The initial 5 rows of the IP header are always used.
  - So, minimum length of IP header = 5 x 4 bytes = 20 bytes.
  - The size of the 6th row representing the Options field vary.
  - The size of Options field can go up to 40 bytes.
  - So, maximum length of IP header = 20 bytes + 40 bytes = 60 bytes.
- **Concept of Scaling Factor**
  - Header length is a 4 bit field.
  - So, the range of decimal values that can be represented is [0, 15].
  - But the range of header length is [20, 60].
  - So, to represent the header length, we use a scaling factor of 4.

- **Header length = Header length field value x 4 bytes**
  - If header length field contains decimal value 5 (represented as 0101), then-
    - Header length = 5 x 4 = 20 bytes
  - If header length field contains decimal value 10 (represented as 1010), then-
    - Header length = 10 x 4 = 40 bytes
  - If header length field contains decimal value 15 (represented as 1111), then-
    - Header length = 15 x 4 = 60 bytes
  - **NOTES**
    - Header length and Header length field value are two different things.
    - The range of header length field value is always [5, 15].
    - The range of header length is always [20, 60].
  - **While solving problem**
    - If the given value lies in the range [5, 15] then it must be the header length field value.
    - This is because the range of header length is always [20, 60].

Type Of Service

- Type of service is a 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.

    D=0
    - It grants the permission to the intermediate devices to fragment the datagram if required.

    D=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.

    MF=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.

    MF=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.
- **Fragment offset for a given fragmented datagram = Number of data bytes ahead of it in the original unfragmented datagram**

- **Concept Of Scaling Factor**
  - We use a scaling factor of 8 for the fragment offset.
  - Fragment offset field value = Fragment Offset / 8
- **Need Of Scaling Factor For Fragment Offset**
  - In IPv4 header, the total length field comprises of 16 bits.
  - Total length = Header length + Payload length. Minimum header length = 20 bytes.
  - So, maximum amount of data that can be sent in the payload field = 2^{16} - 20 bytes.
  - In worst case, a datagram containing 2^{16} - 20 bytes of data might be fragmented in such a way that the last fragmented datagram contains only 1 byte of data.
  - Then, fragment offset for the last fragmented datagram will be (2^{16} - 20) - 1 = 2^{16}-21 $\simeq$ 2^{16}
    (if no scaling factor is used)
  - Now, this fragment offset value of 2^{16} can not be represented.
  - This is because the fragment offset field consists of only 13 bits.
  - Using 13 bits, a maximum number of 2^{13} can be represented.
  - So, to represent 2^{16} we use the concept of scaling factor.
  - Scaling factor = $2^{16}/2^{13} = 2^3 = 8$.

- **Time To Live**
  - Time to live (TTL) is a 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.
  - Both intermediate devices having network layer and destination decrements the TTL value by 1.
  - If the value of TTL is found to be zero at any intermediate device, then the datagram is discarded.
  - So, at any intermediate device, the value of TTL must be greater than zero to proceed further.
  - If the value of TTL becomes zero at the destination, then the datagram is accepted.
  - So, at the destination, the value of TTL may be greater than or equal to zero.

- **Protocol**
  - Protocol is a 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.
- **Why Protocol Number Is A Part Of IP Header?**
  - An IP datagram is sent by the sender to the receiver.
  - When datagram reaches at the router, its buffer is already full.
    - Router does not discard the datagram directly.
    - Before discarding, router checks the next level protocol number mentioned in its IP header.
    - If the datagram belongs to TCP, then it tries to make room for the datagram in its buffer.
    - It creates a room by eliminating one of the datagrams having lower priority.
    - This is because it knows that TCP is a reliable protocol and if it discards the datagram, then it will be sent again by the sender.
    - The order in which router eliminate the datagrams from its buffer is- $ICMP > IGMP > UDP > TCP$

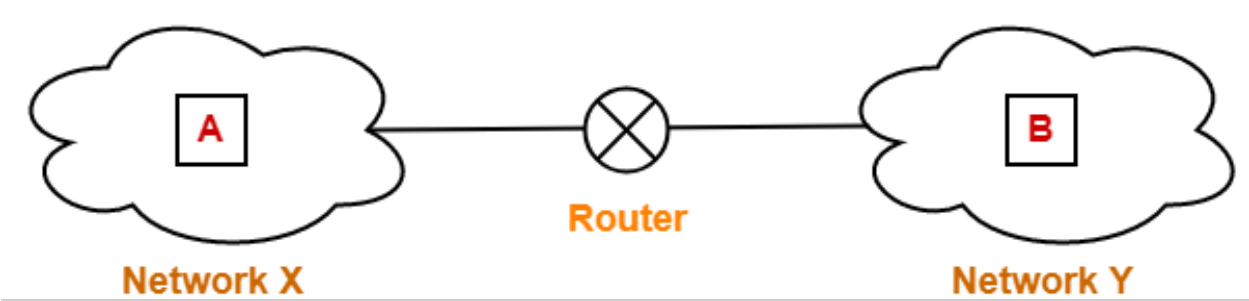
- If protocol number would have been inside the datagram, then-
  - Router could not look into it.
  - This is because router has only three layers- physical layer, data link layer and network layer.
- **Header Checksum**
  - Header checksum is a 16 bit field.
  - It contains the checksum value of the entire header.
  - The checksum value is used for error checking of the header.
- At each hop
  - The header checksum is compared with the value contained in this field.
  - If header checksum is found to be mismatched, then the datagram is discarded.
  - Router updates the checksum field whenever it modifies the datagram header.
- **The fields that may be modified are-**
  - TTL, Options, Datagram Length, Header Length, Fragment Offset

- **Source IP Address & Destination IP Address-**
  - Source IP Address is a 32 bit field.
  - It contains the logical address of the sender 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.
  - **The maximum number of IPv4 router addresses that can be recorded in the Record Route option field of an IPv4 header is 9.**
    - In IPv4, size of IP Addresses = 32 bits = 4 bytes.
    - Maximum size of Options field = 40 bytes. So, it seems maximum number of IP Addresses that can be recorded = 40 / 4 = 10.
    - But some space is required to indicate the type of option being used.
    - Also, some space is to be left between the IP Addresses.
    - So, the space of 4 bytes is left for this purpose.
    - Therefore, the maximum number of IP addresses that can be recorded = 9.

- **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.
    - When header length is not a multiple of 4, extra zeroes are padded in the Options field.
    - By doing so, header length becomes a multiple of 4.
    - If header length = 30 bytes, 2 bytes of dummy data is added to the header.
    - This makes header length = 32 bytes.
    - Then, the value 32 / 4 = 8 is put in the header length field.
    - In worst case, 3 bytes of dummy data might have to be padded to make the header length a multiple of 4.

Fragmentation in Networking

- IP Fragmentation is a process of dividing the datagram into fragments during its transmission.
- It is done by intermediary devices such as routers at the destination host at network layer.

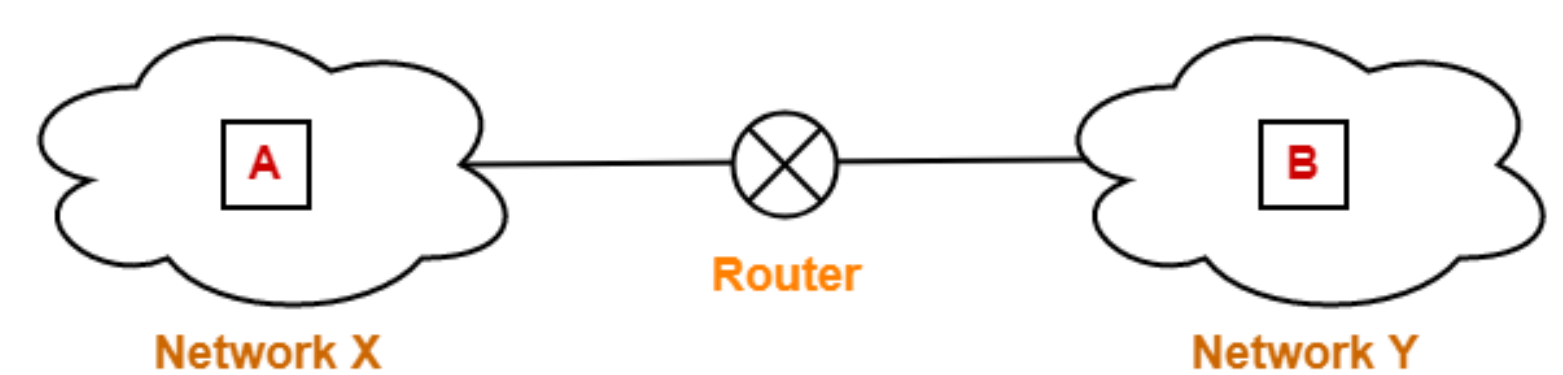


  - Each network has its maximum transmission unit (MTU).
  - It dictates the maximum size of the packet that can be transmitted through it.
  - Data packets of size greater than MTU can not be transmitted through the network.
  - So, datagrams are divided into fragments of size less than or equal to MTU.

- **Datagram Fragmentation**
  - When router receives a datagram to transmit further, it examines the following-
    - Size of the datagram
    - MTU of the destination network
    - DF bit value in the IP header
- **Case-01:**
  - Size of the datagram is found to be smaller than or equal to MTU.
  - In this case, router transmits the datagram without any fragmentation.
- **Case-02:**
  - Size of the datagram is found to be greater than MTU and DF bit set to 1.
  - In this case, router discards the datagram.
- **Case-03:**
  - Size of the datagram is found to be greater than MTU and DF bit set to 0.
  - In this case, router divides the datagram into fragments of size less than or equal to MTU.
  - Router attaches an IP header with each fragment making the following changes in it.
  - Then, router transmits all the fragments of the datagram.

Changes Made By Router

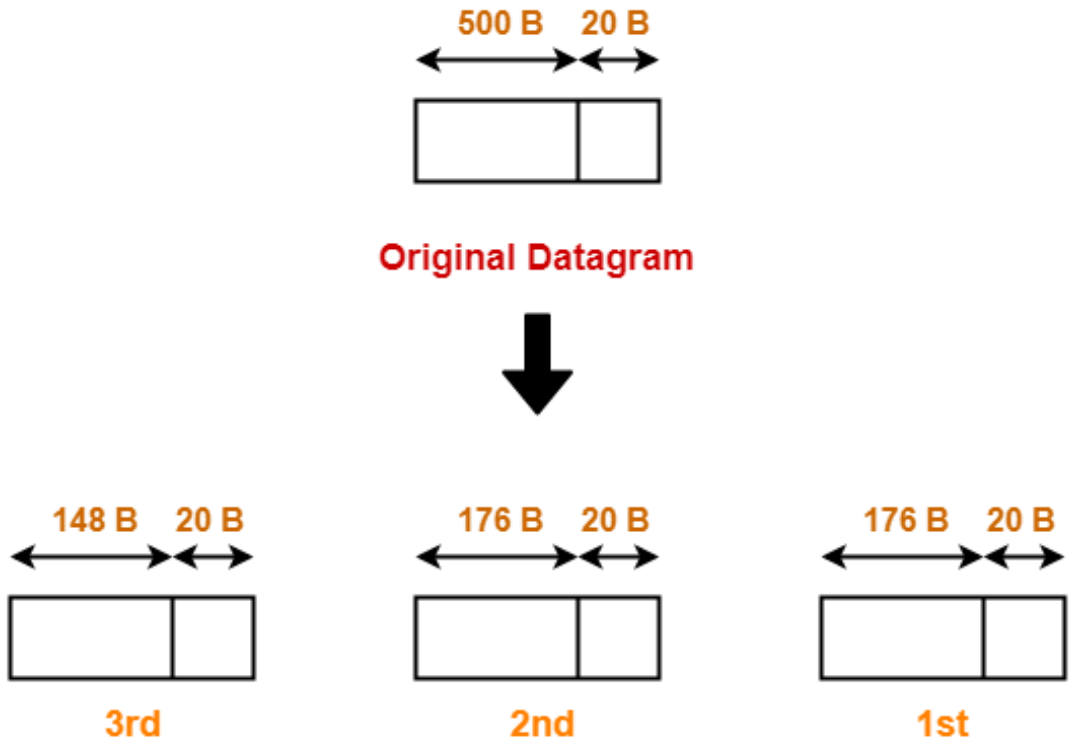
- Router makes the following changes in IP header of each fragment-
  - It changes the value of total length field to the size of fragment.
  - It sets the MF bit to 1 for all the fragments except the last one.
  - For the last fragment, it sets the MF bit to 0.
  - It sets the fragment offset field value.
  - It recalculates the header checksum.
- **IP Fragmentation Examples**
  - Consider-
  - There is a host A present in network X having MTU = 520 bytes.
  - There is a host B present in network Y having MTU = 200 bytes.
  - Host A wants to send a message to host B.



- Consider router receives a datagram from host A having-
  - Header length = 20 bytes
  - Payload length = 500 bytes
  - Total length = 520 bytes
  - DF bit set to 0
- Now, router works in the following steps
- **Step-01:Router examines the datagram and finds-**
  - Size of the datagram = 520 bytes
  - Destination is network Y having MTU = 200 bytes
  - DF bit is set to 0
- Router concludes-
  - Size of the datagram is greater than MTU.
  - So, it will have to divide the datagram into fragments.
  - DF bit is set to 0.
  - So, it is allowed to create fragments of the datagram.

- **Step-02:Router decides the amount of data that it should transmit in each fragment.**
  - MTU of the destination network = 200 bytes.
  - So, maximum total length of any fragment can be only 200 bytes.
  - Out of 200 bytes, 20 bytes will be taken by the header.
  - So, maximum amount of data that can be sent in any fragment = 180 bytes.
- Router uses the following rule to choose the amount of data that will be transmitted in one fragment-
  - The amount of data sent in one fragment is chosen such that-
    - It is as large as possible but less than or equal to MTU.
    - It is a multiple of 8 so that pure decimal value can be obtained for the fragment offset field.
- **Note**
  - It is not compulsory for the last fragment to contain the amount of data that is a multiple of 8.
  - This is because it does not have to decide the fragment offset value for any other fragment.

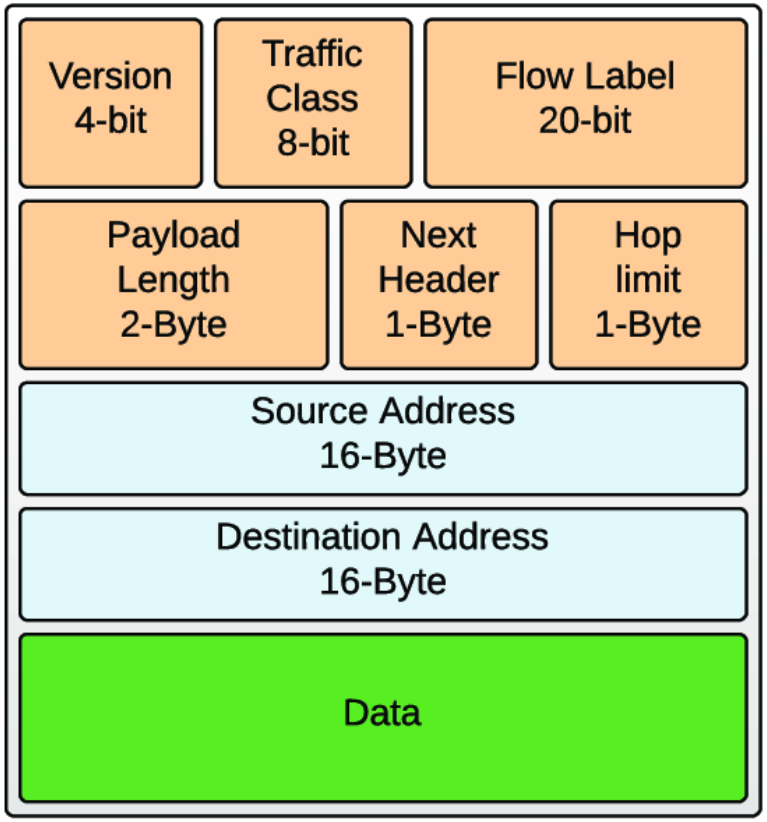
- Following the above rule,
  - Router decides to send maximum 176 bytes of data in one fragment.
  - This is because it is the greatest value that is a multiple of 8 and less than MTU.
- **Step-03: Router creates three fragments of the original datagram where-**
  - First fragment contains the data = 176 bytes
  - Second fragment contains the data = 176 byes
  - Third fragment contains the data = 148 bytes



- **Header Information Of 1st Fragment-**
  - Header length field value = 20 / 4 = 5
  - Total length field value = 176 + 20 = 196
  - MF bit = 1
  - Fragment offset field value = 0
  - Header checksum is recalculated.
  - Identification number is same as that of original datagram.
- **Header Information Of 2nd Fragment-**
  - Header length field value = 20 / 4 = 5
  - Total length field value = 176 + 20 = 196
  - MF bit = 1
  - Fragment offset field value = 176 / 8 = 22
  - Header checksum is recalculated.
  - Identification number is same as that of original datagram.

- **Header Information Of 3rd Fragment-**
  - Header length field value = 20 / 4 = 5
  - Total length field value = 148 + 20 = 168
  - MF bit = 0
  - Fragment offset field value = (176 + 176) / 8 = 44
  - Header checksum is recalculated.
  - Identification number is same as that of original datagram.
- Router transmits all the fragments.
- **Step-04:At destination side,**
  - Receiver receives 3 fragments of the datagram.
  - Reassembly algorithm is applied to combine all the fragments to obtain the original datagram.

IPv6



- Base header 40 bytes (320 bits) fixed
- Extension headers:
  - Routing Header(43)
  - Hop by Hop option (0)
  - Fragment Header (44)
  - Authentication Header (51)
  - Destination option (60)
  - Encapsulation security payload (50)

Thank You