IP Header

A router or computer cannot determine the size of a packet without additional information. Individuals can tick a letter or box and tell how big it is, but the router cannot. Therefore, the IP layer needs other information in addition to the source and destination IP addresses. It is a logical representation of knowledge that is used at the IP layer to achieve the delivery of data. This information is a header and is similar to the addressing information on the envelope. The title contains the knowledge required to route data on the web and has an equivalent format regardless of the type of knowledge sent. This is usually the same as an envelope, and the address format is the same irrespective of the letter. The IPV4 header format is 20 to 60 bytes long. It contains the information necessary for routing and delivery. The IP header can be the prefix of an IP packet that includes information on the IP version, packet length, source and destination IP addresses, etc. It consists of the following fields:

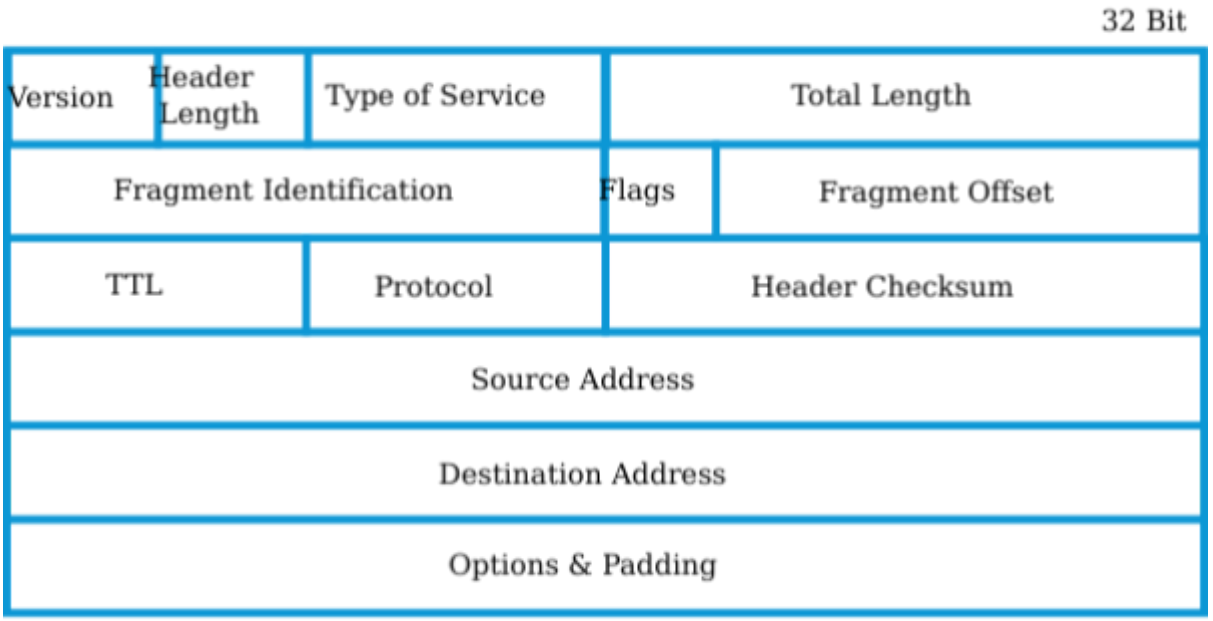

Figure 1: IPv4 Header

- **Version**: The primary field tells us which IP version we are using; only IPv4 uses this header, so you will always find the decimal value 4.
- **Header Length:** These 4th Fields tell us the length of the IP header in 32-bit steps. The size of an IP header is twenty bytes, so in 32-bit steps, you will see the value 5. The maximum value that we create with 4 bits is 15, so with 32-bit increments, this can result in a header- Length of 60 bytes. This field is also known as the length of the web header (IHL).
- **Service Type:** This is typically used for Quality of Service (QoS). We use 8 bits to mark the packet, and we use these bits to provide specific processing for the packet. You will read more about this field in my IP Precedence and DSCP course.
- **Total Length:** This 16-bit field indicates the full size (in bytes) of the IP packet (header and data). The minimum size is twenty bytes (if you have no data), so the maximum length is 65,535 bytes which is the best value you can get with 16 bits.
- **Fragment Identification:** If the IP data packet is segmented, each segmented data packet uses the corresponding 16-bit number to identify which IP data packet in which it belongs to.
- **IP Flags:** These three bits are used for fragmentation:
    - The first bit is usually set to 0.
    - The second bit is called the DF (Don't Fragment) bit, which means the packet should not be fragmented.
    - The third bit is called the MF bit (More Fragment) and is found on roughly all fragmented packets except the last one.
- **Fragment Offset:** These 13 fields indicate the position of the fragment in the original fragmented IP packet.
- **Time to live:** Every time an IP packet passes the router, the measurement time field is reduced by 1. As soon as it reaches 0, the router discards the packet and sends an ICMP timeout message to the sender. The timing field is 8 bits and is used to prevent the box from looping forever (if you have a routing loop).
- **Protocol:** These eight fields tell us which protocol is encapsulated in the IP packet. For example, the value of TCP is 6, and the importance of UDP is 17.
- **Header Checksum:** The checksum of the header is stored in these 16 fields. The recipient can use the checksum to see if the title contains any errors.
- **Source Address:** Here, you will find the 32-bit source IP address.
- **Destination address:** here is the 32-bit destination IP address.
- **Options & Padding:** This field is not commonly used, is optional, and has a variable length to support the options used. Once this field is used, the value in the header length field will increase. A possible option is "source routing," where the sender requests a specific routing path.