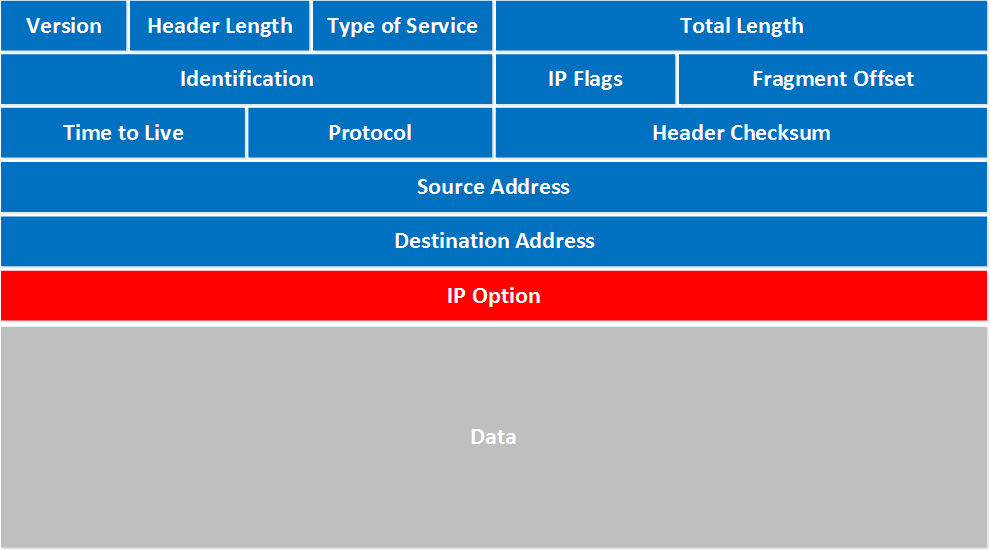
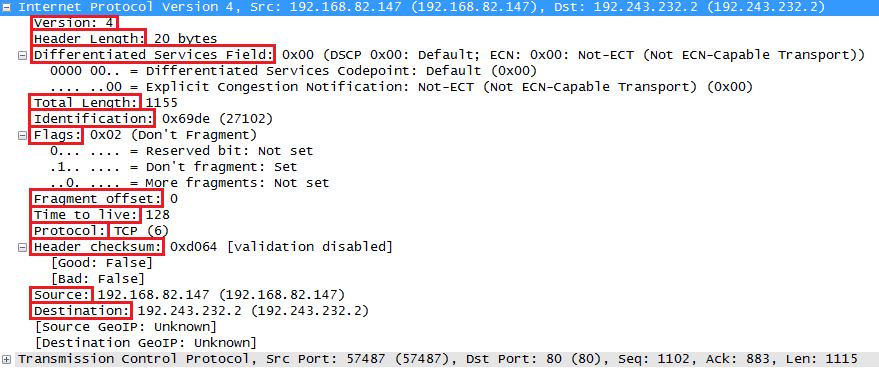
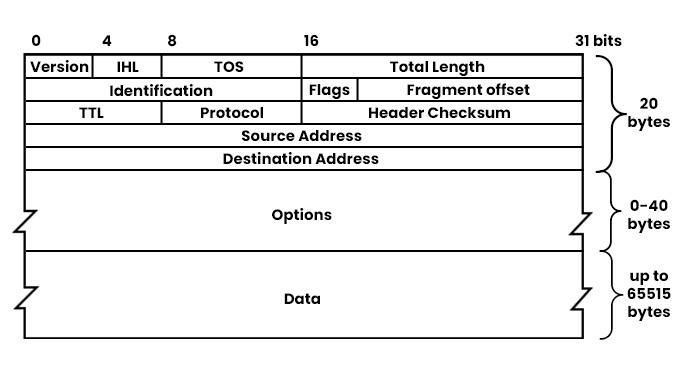
IPv4 Packet Header



* **Version**: the first field tells us which IP version we are using, only IPv4 uses this header so you will always find decimal value 4 here.
* **Header Length**: this 4 bit field tells us the length of the IP header in 32 bit increments. The minimum length of an IP header is 20 bytes so with 32 bit increments, you would see value of 5 here. The maximum value we can create with 4 bits is 15 so with 32 bit increments, that would be a header length of 60 bytes. This field is also called the **Internet Header Length (IHL)**.
* **Type of Service**: this is used for QoS (Quality of Service). There are 8 bits that we can use to mark the packet which we can use to give the packet a certain treatment. You can read more about this field in my [IP precedence and DSCP lesson](https://networklessons.com/quality-of-service/ip-precedence-dscp-values/).
* **Total Length**: this 16-bit field indicates the entire size of the IP packet (header and data) in bytes. The minimum size is 20 bytes (if you have no data) and the maximum size is 65.535 bytes, that’s the highest value you can create with 16 bits.
* **Identification**: If the IP packet is fragmented then each fragmented packet will use the same 16 bit identification number to identify to which IP packet they belong to.
* **IP Flags**: These 3 bits are used for fragmentation:
  + The first bit is always set to 0.
  + The second bit is called the **DF (Don’t Fragment) bit** and indicates that this packet should not be fragmented.
  + The third bit is called the **MF (More Fragments)** bit and is set on all fragmented packets except the last one.
* **Fragment Offset**: this 13 bit field specifies the position of the fragment in the original fragmented IP packet.
* **Time to Live**: Everytime an IP packet passes through a router, the time to live field is decremented by 1. Once it hits 0 the router will drop the packet and sends an ICMP time exceeded message to the sender. The time to live field has 8 bits and is used to prevent packets from looping around forever (if you have a routing loop).
* **Protocol**: this 8 bit field tells us which protocol is enapsulated in the IP packet, for example TCP has value 6 and UDP has value 17.
* **Header Checksum**: this 16 bit field is used to store a checksum of the header. The receiver can use the checksum to check if there are any errors in the header.
* **Source Address**: here you will find the 32 bit source IP address.
* **Destination Address**: and here’s the 32 bit destination IP address.
* **IP Option**: this field is not used often, is optional and has a variable length based on the options that were used. When you use this field, the value in the header length field will increase. An example of a possible option is “source route” where the sender requests for a certain routing path.

Here’s a real life example of an IP packet in Wireshark where you can see how these fields are used:





### Version

The version field is 4-bit, which indicates the version of the Internet protocol that is used in the packet. In this case, it is version 4, i.e., IPv4.

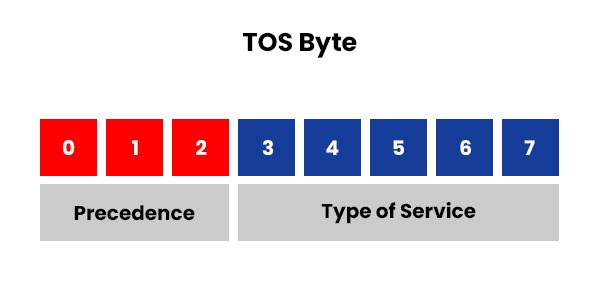
### IHL

IHL or Internet Header Length is also a 4-bit length that specifies the header’s length in 32-bit words. The minimum header length is 20 bytes, i.e., 5 words, and the maximum header length is 60 bytes, i.e., 15 words. Hence, this field can only have values between 5 and 15.

### TOS

TOS or type of service is 8-bit long, which indicates the [QoS (Quality of service)](https://www.pynetlabs.com/qos-in-networking/) that is requested for the packet. Further, it can be used to specify parameters such as priority, delay, throughput, reliability, or cost. TOS has been redefined several times; moreover, different standards use different interpretations of its bits.

* **Priority:**The precedence subfield specifies the packet’s priority among other packets, along with different QoS requirements.
* **Delay:**The delay subfield is to specify whether low delay is preferred or not.
* **Throughput:**Same as delay, in the throughput subfield, it specifies whether high throughput is preferred or not.
* **Reliability:**It specifies whether high reliability is preferred or not.



| Bit 3: | 0 = normal delay | 1 = low delay |
| --- | --- | --- |
| Bit 4: | 0 = normal throughput | 1 = high throughput |
| Bit 5: | 0 = normal reliability | 1 = high reliability |
| Bit 6-7: | Reserved for future use |  |

**Below we have shown these parameters along with their possible values in the form of the table.**

| **Precedence** | **Delay** | **Throughput** | **Reliability** |
| --- | --- | --- | --- |
| **Routine (000)** | Normal (0) | Normal (0) | Normal (0) |
| **Priority (001)** | Low (1) | Normal (0) | Normal (0) |
| **Immediate (010)** | Normal (0) | High (1) | Normal (0) |
| **Flash (011)** | Low (1) | High (1) | Normal (0) |
| **Flash Override (100)** | Normal (0) | Normal (0) | High (1) |
| **Critical/ECP (101)** | Low (1) | Normal (0) | High (1) |
| **Internetwork Control (110)** | Normal (0) | High (1) | High (1) |
| **Network Control (111)** | Low (1) | High (1) | High (1) |

### **Total Length**

The total length field is 16 bits long and specifies the length of the entire packet in bytes. This includes both the header and the payload. The minimum value can vary from 20 bytes, i.e., the minimum header length, to a maximum value of 65535 bytes, i.e., the maximum size of the packet. If the packet is larger than the provided maximum size, the packet will then be fragmented into smaller pieces by the routers or hosts.

### **Identification**

The identification field is 16 bits long and is mainly used to identify packets that belong to a fragment group. When we talk about fragment groups, it consists of all the packets that are fragmented from the original packet. The main work of the identification field is to assist in reassembling the fragments at the destination.

### Flags

The flag field is 3 bits long and controls as well as identifies fragments. It has three possible values. These are:

* **Bit 0:**Reserved and must be zero.
* **Bit 1:**DF or don’t fragment. If set to one, it usually indicates that the packet should not be fragmented by any device. If a device cannot forward the packet without fragmenting it, it should drop it and send an [ICMP](https://www.pynetlabs.com/what-is-icmp-protocol/) message to the sender.
* **Bit 2:**MF or more fragments. If set to one, it indicates that there are more fragments. On the other hand, if it is set to zero, it signifies that this is the last or only fragment in the group.

### **Fragment Offset**

The position of the packet in the original datagram is indicated by fragment offset. It is measured in units of 8 bytes. Fragment offset of zero belongs to the first packet of a datagram. The following other packets have a fragment offset that is equal to the sum of the lengths of the previous packets divided by 8. The fragment offset field further assists in reassembling the fragments at the destination.

### **TTL**

TTL, or time-to-live field, is 8 bits long, and with the help of TTL, one can easily know the maximum time that a packet can live in the network. It is measured in seconds, and it keeps on being decremented by one by every device that processes the packet. When the value reaches zero, the packet is discarded, and an ICMP message is sent back to the sender. With the help of TTL, it is now possible to prevent packets from looping endlessly in the network and consuming resources.

### **Protocol**

The protocol field indicates the type of protocol that is used in the payload. Furthermore, it identifies the next-level protocol that processes the data after the IP layer.

Below, we have shown some common values for this field for better understanding.

| **Protocol** | **Field** | **Description** |
| --- | --- | --- |
| **ICMP** | 1 | Internet Control Message Protocol |
| **TCP** | 6 | [Transmission Control Protocol](https://www.pynetlabs.com/udp-vs-tcp/) |
| **UDP** | 17 | User Datagram Protocol |

### **Header Checksum**

In order to verify the integrity of the header, header checksum field is utilized. It is calculated by adding all the 16-bit words in the header and taking one’s complement of the result. If there are any errors in the header, such as bit flips or corrupted fields, the checksum will not match, and the packet will be discarded.

### **Source Address**

This field signifies the IP address of the sender of the packet. The source address field is a 32-bit number used to identify a host or a network interface on the internet.

### **Destination Address**

Similar to the source address field, the destination address field indicates the IP address of the receiver of the packet. It is also a 32-bit number that uniquely identifies a host or a network interface on the internet.

### **Options**

The option field is variable in length and contains optional information that can be further used for different purposes. Some of these are security, routing, or timestamping. Each option has a format of:

* **Option Type:** It is of 8 bits and usually indicates what kind of option it is and whether it should be copied to all the fragments or not.
* **Option Length:**It is also 8 bits, and it simply signifies the length of the option in bytes. This includes option type and option length fields.
* **Option Data:**Variable – Contains the data for the option.

