Internet Packets

IPv4 Fields

4 Bit: Protocol Version

Is always 0x4

4 Bit: IHL - Internet Header Length

Multiples of 4 Byte, minimum 0x5, greater than 0x5 signs that IPv4 Header Options are present

6 Bit: DSCP

Arbitrary identifier mostly used by QoS. Can mark specific types of payload.

2 Bit: ECN

Congestion control

16 Bit: Total Length

Length of IPv4 packet including header, size in Byte

16 Bit: Identification

Only used for fragmented packets. Ignore if not fragmented, set to 0x0000 or something. All packets with the same value belong to the same fragmented packet.

1 Bit: Reserved

Always 0x0

1 Bit: Don't fragment

If set to 0x1, don't fragment this packet (further). It might already be fragmented.

0x0, this packet is not fragmented.

1 Bit: More Fragments

If set to 0x0 this is the last fragment of the packet.

If set to 0x1, this is not the last fragment of the packet.

13 Bit: Fragment Offset

Is a multiple of 8 Bytes. This field specifies how much of the original packet has to be skipped, after that fragment must be placed. For the first fragment of a packet the value is 0x0.

8 Bit: Time To Live

Is decremented by each routing hop. If value is 0x0 packet is dropped.

8 Bit: Protocol

Type of data in the payload.

- 0x06: TCP
- 0x11: UDP

8 Bit: Header Checksum

Checksum of the IPv4 header.

32 Bit: Source Address

32 Bit: Destination Address

Variable length: IPv4 Options

Happy rabbit holing, if you encounter these x.x

Recognizing IPv6 packets

```
0000   xx xx xx xx xx xx xx xx xx xx xx xx 86 dd 60 xx
0010   xx xx xx xx xx xx XX XX XX XX XX XX XX XX XX XX
0020   XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
0030   XX XX XX XX XX XX ...
```

For IPv6 you only have the Ethernet Type 0x86dd for IPv6 as a distinguisher and the protocol constant 0x60 if the QoS fields aren't used.

XX marks where the addresses are placed.

Recognizing IPv4 packets

```
0000   xx xx xx xx xx xx xx xx xx xx xx xx 08 00 45 00
0010   xx xx 00 00 40 00 xx xx xx xx XX XX XX XX XX XX
0020   XX XX ...
```

IPv4 packets can be recognized by 0x0800 in the 13th and 14th Byte which is the Ethernet Type for IPv4. Also Byte 15 and 16 is usually 0x4500, as IPv4 Options and traffic control features are often not used.

Byte 21 and 22 are nearly always 0x4000 because fragmentation isn't really used these days anymore. Because of this Byte 19 and 20 can be 0x0000, but some implementations still set this to some other value despite no fragmentation is done.

XX marks where the addresses are placed.

Hex representation of IP addresses

For IPv6 it is very easy. It is just the IPv6 address, as one would write it without the double colons and the zeros filled in. So if you see 0x2a01 or 0x2001 or something like that, this is probably the beginning of an IPv6 address. If you encounter a lot of zeros six Bytes later, for example 0x0000000000000001, then this is an abbreviated IPv6 address, that is just the host ::1 in a /64.

For IPv4 it is not that easy. But you can watch out for widely used network prefixes like 0xc0a8, which is 192.168...

- 0xc0a800: 192.168.0...
- 0xc0a8b201: 192.168.178.1
- 0xc0a8b2: 192.168.178...
- 0xc0a8: 192.168...
- 0x0a: 10...
- 0xac: 172...

A word about IPv4 packet fragmentation

If More Fragments field is 0x0 and Fragment Offset is 0x0, then this packet is not fragmented.

A packet that is fragmented, must have the Don't Fragment field set to 0x1, as the packet can't be fragmented even further.