IPv4 Protocol

IP stands for **Internet Protocol** and **v4** stands for **Version Four** (IPv4). IPv4 was the primary version brought into action for production within the ARPANET in 1983.

IP version four addresses are 32-bit integers which will be expressed in decimal notation. Example- 192.0.2.126 could be an IPv4 address.

Parts of IPv4

- **Network part:**
- The network part indicates the distinctive variety that's appointed to the network. The network part conjointly identifies the category of the network that's assigned.
- **Host Part:**
- The host part uniquely identifies the machine on your network. This part of the IPv4 address is assigned to every host.
  For each host on the network, the network part is the same, however, the host half must vary.
- **Subnet number:**
  This is the nonobligatory part of IPv4. Local networks that have massive numbers of hosts are divided into subnets and subnet numbers are appointed to that.

Characteristics of IPv4

- IPv4 could be a 32-Bit IP Address.
- IPv4 could be a numeric address, and its bits are separated by a dot.
- The number of header fields is twelve and the length of the header field is twenty.
- It has Unicast, broadcast, and multicast style of addresses.
- IPv4 supports VLSM (Virtual Length Subnet Mask).
- IPv4 uses the Post Address Resolution Protocol to map to the MAC address.
- RIP may be a routing protocol supported by the routed daemon.
- Networks ought to be designed either manually or with DHCP.
- Packet fragmentation permits from routers and causing host.

Advantages of IPv4

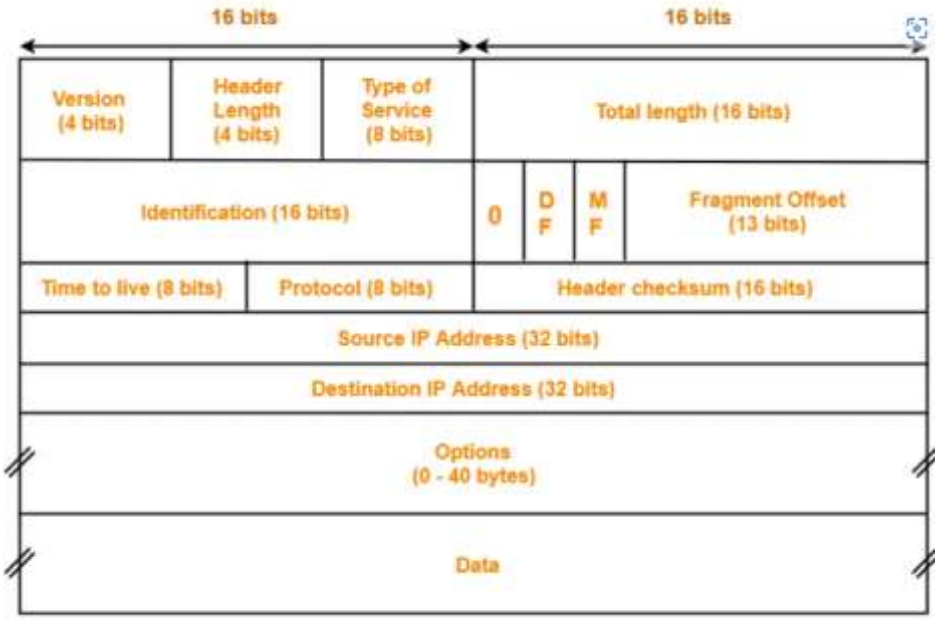
- IPv4 security permits encryption to keep up privacy and security.
- IPV4 network allocation is significant and presently has quite 85000 practical routers.
- It becomes easy to attach multiple devices across an outsized network while not NAT.
- This is a model of communication so provides quality service also as economical knowledge transfer.
- IPV4 addresses are redefined and permit flawless encoding.
- Routing is a lot of scalable and economical as a result of addressing is collective more effectively.
- Data communication across the network becomes a lot of specific in multicast organizations.
    - Limits net growth for existing users and hinders the use of the net for brand new users.
    - Internet Routing is inefficient in IPv4.
    - IPv4 has high System Management prices and it's labor-intensive, complex, slow & frequent to errors.
    - Security features are nonobligatory.
    - Difficult to feature support for future desires as a result of adding it on is extremely high overhead since it hinders the flexibility to attach everything over IP.

Limitations of IPv4

- IP relies on network layer addresses to identify end-points on network, and each network has a unique IP address.

- The world's supply of unique IP addresses is dwindling, and they might eventually run out theoretically.
- If there are multiple host, we need IP addresses of next class.
- Complex host and routing configuration, non-hierarchical addressing, difficult to re-numbering addresses, large routing tables, non-trivial implementations in providing security, QoS (Quality of Service), mobility and multi-homing, multicasting etc. are the big limitation of IPv4 so that's why IPv6 came into the picture.
-

IPV4 Header Format



IPv4 Header

- 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**.

1.**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

2.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

Minimum And Maximum Header Length

- 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.

In general,

Header length = Header length field value x 4 bytes

3. 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

3. **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

4. **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.

5. 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

6. 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.

8.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

9.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.

10. 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.

11. 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-

1. TTL

2. Options
3. Datagram Length
4. Header Length
5. Fragment Offset

12. Source IP Address-

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

13. Destination IP Address-

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

14. Options-

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

1. Record route
2. Source routing
3. Padding