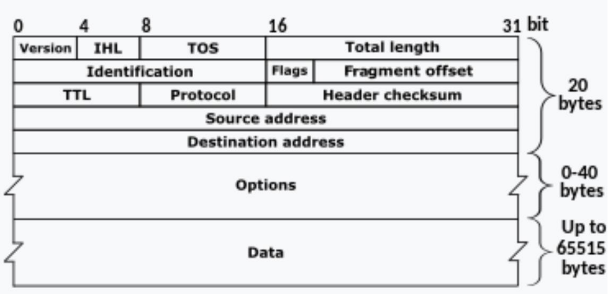
CN ASSIGNMENT

Q1. Discuss IPV4 Packet Structure in Detail?

Ans. IPv4 is a connectionless protocol used for packet-switched networks. It operates on a best effort delivery model, in which neither delivery is guaranteed, nor proper sequencing or avoidance of duplicate delivery is assured. Internet Protocol Version 4 (IPv4) is the fourth revision of the Internet Protocol and a widely used protocol in data communication over different kinds of networks. IPv4 is a connectionless protocol used in packet-switched layer networks, such as Ethernet. It provides a logical connection between network devices by providing identification for each device. There are many ways to configure IPv4 with all kinds of devices – including manual and automatic configurations – depending on the network type.

IPv4 uses 32-bit addresses for Ethernet communication in five classes: A, B, C, D and E. Classes A, B and C have a different bit length for addressing the network host. Class D addresses are reserved for military purposes, while class E addresses are reserved for future use. IPV4 uses 32-bit (4 byte) addressing, which gives 2^{32} addresses.

- **Version** − Version no. of Internet Protocol used (e.g. IPv4).
- **IHL** − Internet Header Length; Length of entire IP header.
- **DSCP** − Differentiated Services Code Point; this is Type of Service.
- **ECN** − Explicit Congestion Notification; It carries information about the congestion seen in the route.
- **Total Length** − Length of entire IP Packet (including IP header and IP Payload).
- **Identification** − If IP packet is fragmented during the transmission, all the fragments contain same identification number. to identify original IP packet they belong to.
- **Flags** − As required by the network resources, if IP Packet is too large to handle, these 'flags' tells if they can be fragmented or not. In this 3-bit flag, the MSB is always set to '0'.
- **Fragment Offset** − This offset tells the exact position of the fragment in the original IP Packet.
- **Time to Live** − To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross. At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded.
- **Protocol** − Tells the Network layer at the destination host, to which Protocol this packet belongs to, i.e. the next level Protocol. For eg. protocol number of ICMP is 1, TCP is 6 and UDP is 17.
- **Header Checksum** − This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free.
- **Source Address** − 32-bit address of the Sender (or source) of the packet.
- **Destination Address** − 32-bit address of the Receiver (or destination) of the packet.
- **Options** − This is optional field, which is used if the value of IHL is greater than 5. These options may contain values for options such as Security, Record Route, Time Stamp, etc.



IPv4 packet

Q2. Explain Working of DHCP?

Ans. DHCP (Dynamic Host Configuration Protocol) is a network management protocol used to dynamically assign an IP address to any device, or node, on a network so it can communicate using IP. DHCP automates and centrally manages these configurations rather than requiring network administrators to manually assign IP addresses to all network devices. DHCP can be implemented on small local networks, as well as large enterprise networks. DHCP is a client-server protocol in which servers manage a pool of unique IP addresses, as well as information about client configuration parameters. The servers then assign addresses out of those address pools. DHCP-enabled clients send a request to the DHCP server whenever they connect to a network.

Dynamic Host Configuration Protocol (DHCP) uses the **DORA.**

It consists of four-stage:

1. Discover
2. Offer
3. Request
4. Acknowledge

DHCP Discover Message

This is the first message in the DORA process which helps in finding the DHCP server of the network. DHCP client will find the server by sending DHCP discover message. The broadcast message is sent to the network.

DHCP Offer Message

DHCP server receives the discover message and it replays the DHCP client with the DHCP offer request. The server sends a DHCP offer message with filled information. It has information about the IP address and duration of time that a host can use.

DHCP Request Message

DHCP clients send the request message to the server when it receives a DHCP offer message from the server. This message tells the server that it accepts the IP address given by the server.

DHCP Acknowledge Message

This is the last step or message in the DORA process. The DHCP server sends Acknowledge Message to the client when it receives the request message from the DHCP client. This message will contain the IP address and subnet mask that the server assigns to the client. Source IP address will be the IP address of the server.

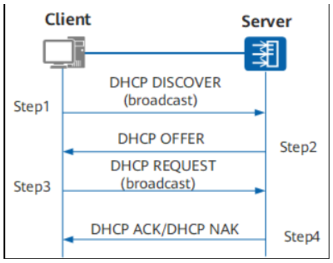
So, this is the DORA process and when this process is over DHCP client will get its IP address. Here things to remember is

DHCP Discover Message – Broadcast

DHCP Offer Message – Broadcast in the network layer and unicast in the data link layer

DHCP Request Message – Broadcast in the network layer and unicast in the data link layer

DHCP Acknowledge Message – Broadcast in the network layer and unicast in the data link layer


Client
Server
DHCP DISCOVER
(broadcast)
Step1
DHCP OFFER
Step2
DHCP REQUEST
(broadcast)
Step3
DHCP ACK/DHCP NAK
Step4