Internet Protocol (IP) :-

→ The Internet Protocol is the method or Protocol by which data is sent from one Computer to another on the internet.

→ Each computer (Host) on the internet has atleast one IP address that uniquely identifies it from all other computers on the Internet.

→ Internet Protocol is connectionless and unreliable.

→ It ensure no guarantee of successfully transmission of data.

→ in order to make it reliable, it must be Paired with reliable Protocol such as TCP at the transport Layer.

→ Internet Protocol transmits the data in form of a datagram.

↳ Datagram is a block of data; and it is synonym for Packets and used in UDP, connection less.

→ The length of datagram is Variable.

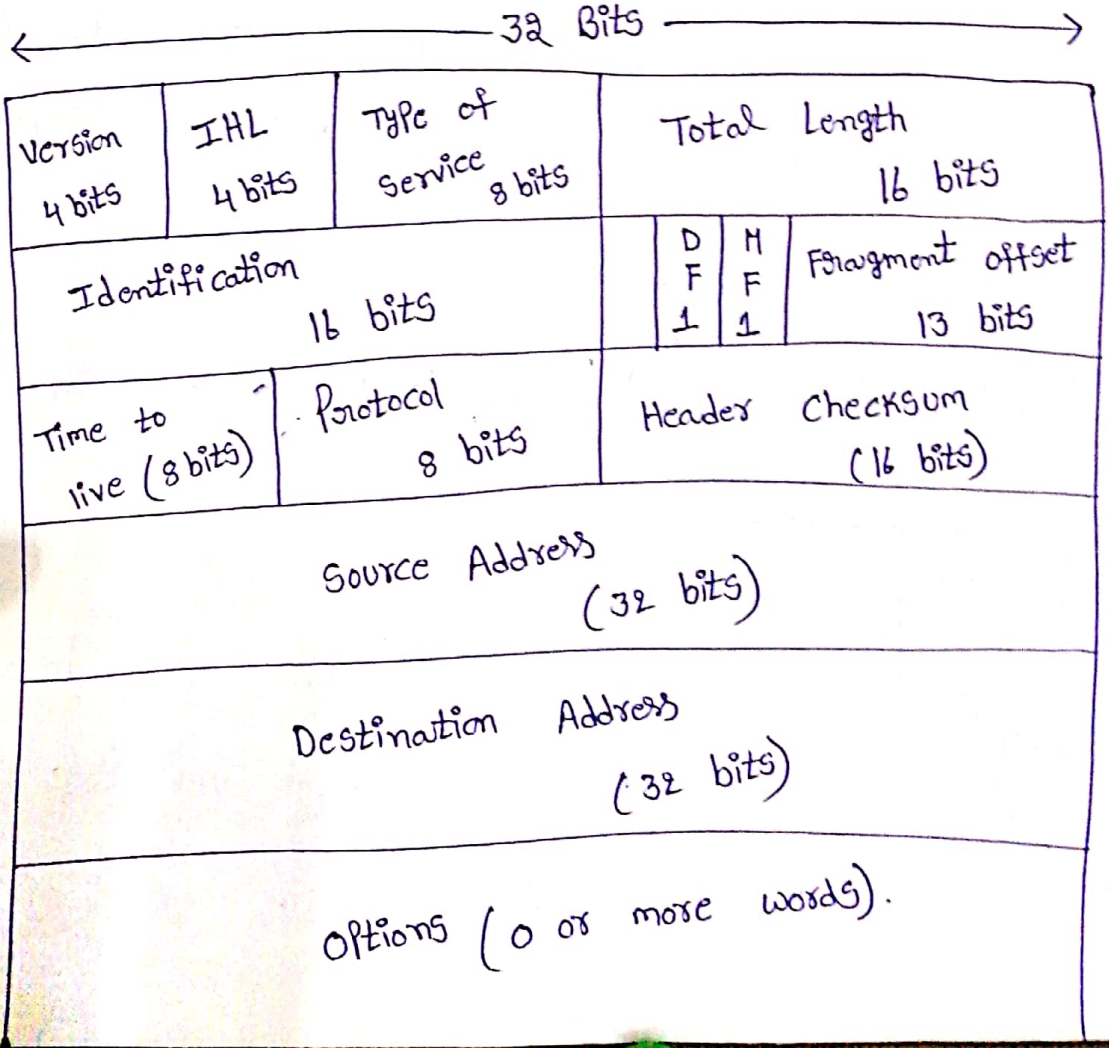
→ The Datagram is divided into 2 Parts; Header and Data/Payload.

IP Header :-

→ The IP Header consists of various Parameter.

→ The Header has a 20 byte fixed Part and a Variable length optional Part.

→ The Header Contains information for Routing and delivery of the Packet.



1. Version :- Version field contains the version of protocol the datagram belongs to.

eg:- IPv_4, IPv_5, IPv_6 ....

2. IHL :- This field provides the size of the Header, header length is not constant. without option the size of header field is 5.

3. Type of Service :- This is also called as Differentiated service field. it contains information about service and host uses this field. using this field host to tell the subnet what kind of service it wants. speed and reliability of service is possible.

4. Total Length :- it includes both header and datas. The Max length is 65,535 bytes

5. Identification Field :- it is needed to allow the destination host to determine which datagram a newly arrived fragment belongs to. All the fragments of a datagram contain the same identification no

6. DF :- it is 1 bit field. DF stands for do not fragment. if destination is in capable of putting the pieces back together, the order is given to router do not fragment the datagram.

7. MF :- it is 1 bit field. MF stands for more fragment. All fragment except the last one have this bit set. it is needed to know when all fragments of a datagram have arrived.

8. Fragment offset :- it tells where in the current datagram this fragment belongs. The Max. of 8192 fragments per datagram, giving a Max datagram length of 65,536 bytes.

9. Time to live :- it is used as a counter used to limit Packet lifetimes. The max. lifetime is 255 second. The counter is decrement on each hop. when it counter becomes zero, the Packet is discarded and a

warning Packet is sent back to the source host.

10. Protocol :- Protocol field tells it which transport Process to give it to TCP, UDP and other Protocol are the example of the field.

11. Header Checksum :- This field verifies the header only. This field is used to detect the error.

12. Source Address & Destination Address :- These fields indicate the n/w number and host number.

Network Address Translation (NAT) :-

→ IP Addresses are Scarce. An ISP might have a 16 address, giving it 65,534 usable host numbers. if it has more customers than that, it has a Problem.

→ To access Internet, one public IP address is needed but as you use private IP address in our private n/w, translation of private IP address to a public IP address is required.

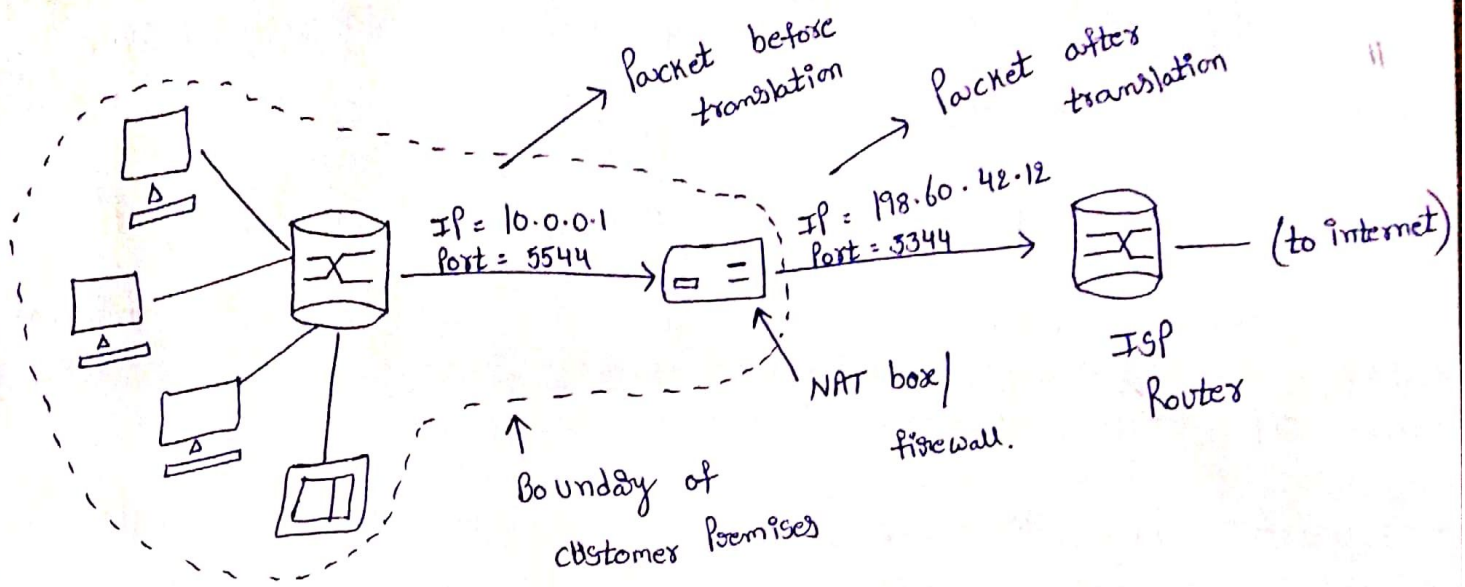
→ "NAT" is a process in which one or more local IP Address is translated into one or more Global IP Address and vice versa in order to provide Internet access to the local hosts.

→ NAT generally operates on routers / firewall.

→ The border router is configured for NAT i.e the routers which have one interface in local n/w and one interface in global n/w.

→ When a packet traverse outside the local n/w, then NAT converts that local IP address to a global IP address.

→ When a packet enters the local n/w; the global IP address is converted to local IP Address.



Public IP Address:- A Public IP Address is an IP Address that can be accessed over the internet. a Public IP Address is the globally unique ip address assigned to a computing device.

Private IP Address :- A Private IP Address is an IP Address that can be used with the LAN or within the organization. and not recognized on Internet.

Class	Starts from	Ends ~~from~~
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

→ within the company, every Machine has a unique address of the from 10.x.y.z.

→ When a packet leaves the company premises, it passes through the NAT box that convert the internal IP source Address 10.0.0.1.

→ NAT box ~~that~~ is often combined in a single device with a fire wall. it is also possible to integrate the NAT box into the company router.

→ whenever an outgoing packet enters the NAT box, the 10.x.y.z. source Address is replaced by the company true IP address.

→ In addition, TCP source port field is replaced by an index into the NAT box 65,536 entry translation table.

→ This table entry contains the original IP address and original source port.

→ finally both the IP and TCP header checksums are recomputed and inserted into the packet.

Types of NAT :-

- Static NAT
- Dynamic NAT
- Port Address Translation.

Static NAT :- A Single Private IP Address is mapped with Single Public IP Address.

Dynamic NAT :- multiple IP Address are mapped to a Pool of Public IP address.

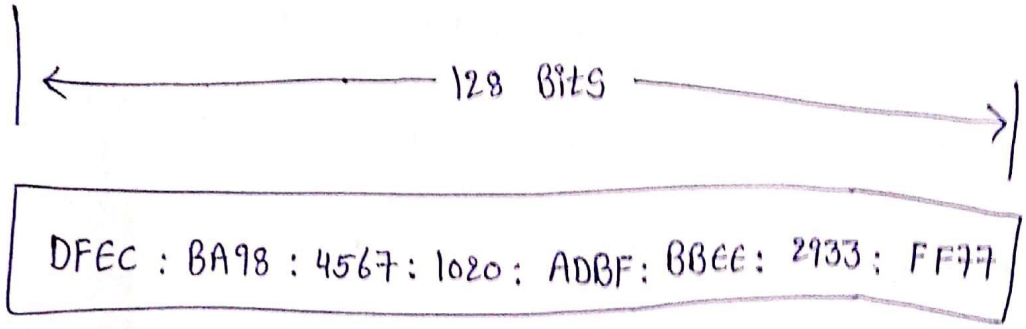
PAT :- This is also known as NAT overload. many Private IP addresses can be translated to Single Public IP Address. Port numbers are used to distinguish the traffic; i.e which traffic belongs to which IP Address.

IPv6 :- IPv6 includes the following enhancements over IPv4:

- Expanded address space
- Improved option mechanism
- Address auto configuration
- Increased addressing flexibility
- Support for resource allocation
- Security capabilities.

→ IPv6 uses 128 bits addresses.

→



→ IPv6 is redesigned Entirely; it offers the following features:

i) **Larger Address Space:-** In contrast to IPv4, IPv6 uses 4 times more bits to address a device on the Internet.

→ This much extra bits can provide approximately 3.4×10^{38} diff combinations of addresses.

14

IPV6 Header :-

→ The IPV6 header has a fixed length of 40 octets, consisting of the following field.

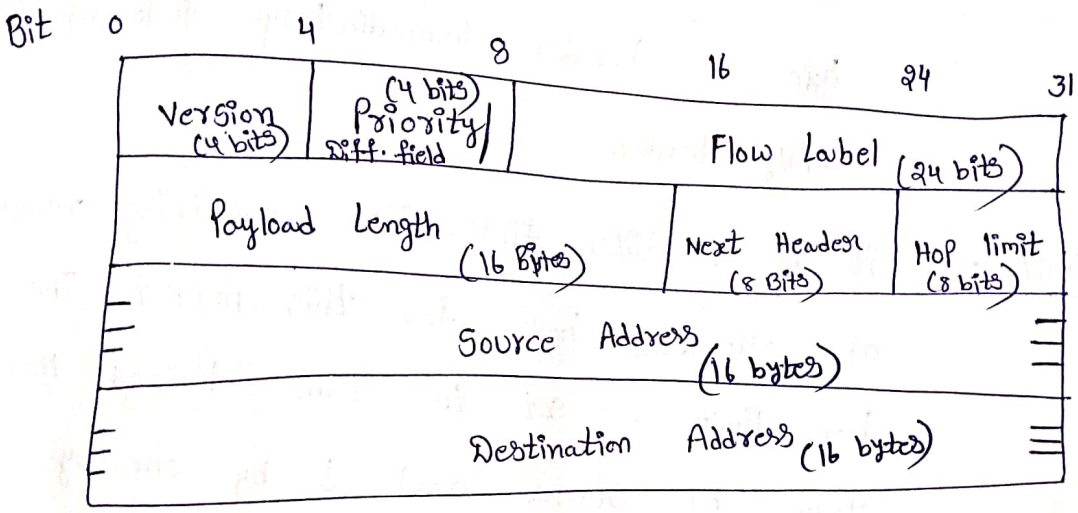


Fig:- IPV6 Header Format

Version:- it is 4 bit in size. it specifies the Internet Protocol version number.

Priority:- it is 4 bits field enables a source to identify the desired transmit.

flow Label :- flow Label is 24 bits. it may be used by a host to label those packets for which it is requesting special handling by routers within a network.

Payload Length:- It is 16 bits fields. This is the total length of all of the extension header plus the transport level PDU.

Next Header:- it is 8 bits field. it identifies the type of header immediately following the IPV6 Header.

Hop Limit :- it is 8 bits field. The remaining number of allowable hops for this packet. The hop limit is set to some desired Max. value by source and ↓ by one by each node. that forwards the packet. The packet is discarded if hop limit is ↓ to zero.

Source Address:- SA is 128 bits (32 x4). The address of the originator of the packet.

Destination Address:- DA is also 128 bits (32 x4).

→ IPV6 allows 3 types of addresses.

i) Unicast ii) Anycast iii) Multicast