(ii) Transport Layer

→ This layer support communication between devices across diverse network using port addressing

(iii) Network Layer

→ Its primary responsibility is to perform routing using IP address.

iv) Network Access Layer

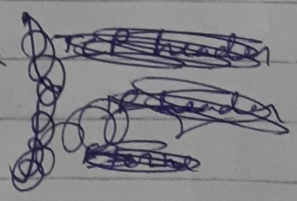
→ Also called as Link Layer / Network interface Layer.

→ It controls the hardware devices and media that help in message transmission.

→ In a 5-layer TCP architecture the Network access layer is divided into Datalink & Physical layer.

TCP/IP PDUs

5 Application → Data
4 Transport → segment → Port address
3 Network → Packet → IP "
2 Datalink → Frame → MAC "
1 Physical → Bits



There exist three classes of IP address in version 4, that is:

(i) Class A

In format a.b.c.d, the variation of the bits lies in between zero to 127. with the category of subnet mask 255.0.0.0 where a is indicating the network id and b,c,d are indicating the host id.

This class is utilised for larger network.

(ii) Class B

In format a.b.c.d, the values vary in between 128 to 191 with subnet mask format 255.255.0.0, where a,b are network id & c,d are host id.

This is used for medium sized network.

(iii) Class C

In format a.b.c.d, the first 24 bit are network id and last 8 bit is host id. (a,b,c → network id, d → host id), its subnet mask format is 255.255.255.0. The values vary from 192 to 255.

This is used for small network.

Concept of Data Encapsulation

→ While the message is transmitted from source to destination, at every layer a header is attached to the original message and the process is called as "Encapsulation".

→ Some of the important headers are :-

(i) Ethernet header (layer 1)

(ii) IP header (layer 2)

IPv4 (32 bits) IPv6 (128 bits)

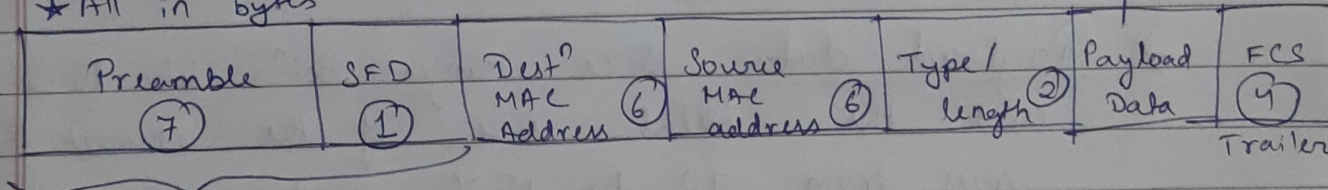
(iii) TCP protocol header (layer 3)

(iv) UDP protocol header (layer 3)

Ethernet Header

(Network Access)

★ All in bytes



Header for physical layer → Rest is the header corresponding to datalink layer

⇒ Preamble and SFD (Start frame delimiter)

(fields)

→ These two layers are attached by the physical layer and indicate the starting of the data frame between Sender and Receiver over a network.

→ Preamble is 7 bytes = 56 bits with value 1010... (upto 56 bits).

→ SFD is 1 byte = 8 bits with value 10101011.

⇒ The next two fields are Source & dest^n MAC address with size 48 bit each.

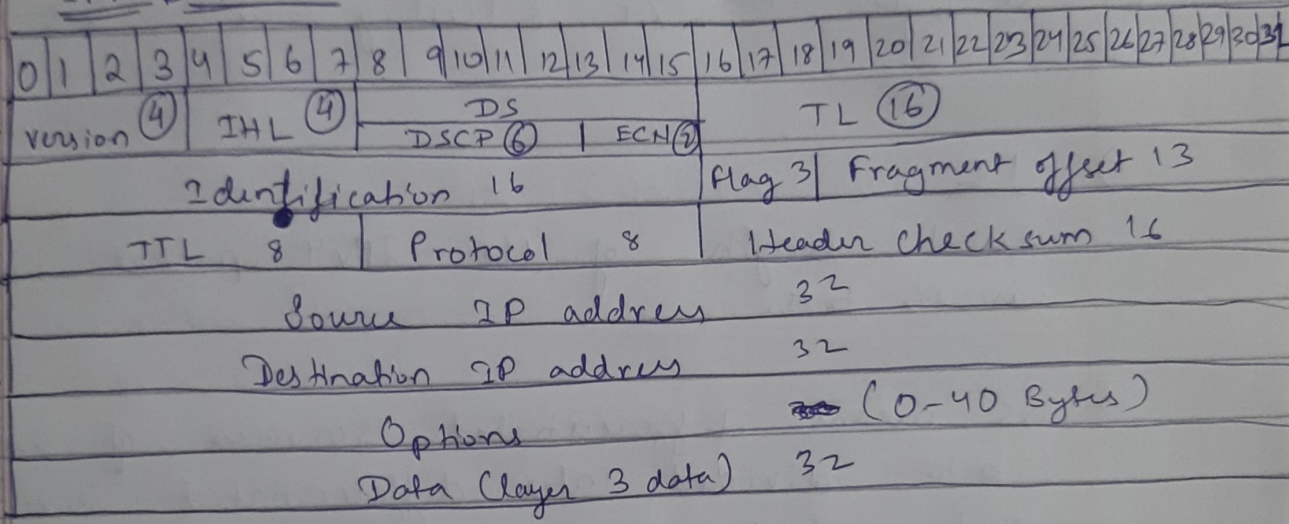
⇒ Type and length field is used to identify the type of upper layer protocol (Ipv4, Ipv6).

⇒ Payload data size ranges bet^n 46 to 1500 bytes and the total size of the ethernet header goes from 72 to 1526 and the minimum size of a ethernet frame should be 64 bytes. Frames lesser than 64 bytes are called "runts" and needs to be padded with zeroes. Frames greater than 64 bytes are called jumbo frames or giants.

⇒ FCS (Frame Check Sequence)

→ It is of 4 bytes which is used to verify the frame integrity and rectify the errors.

IPv4 Header



→ Starting header (20B)

★ So, full header will be 20-60 bytes.

⇒ The size of the static header is 20 B and full header is 20-60 bytes

→ IPv4 (0100) or IPv6 (0110)

⇒ IHL means Internet header length which goes from 20 to 60 bytes.

★ IHL ranges from 5-15, with a scaling factor 4.

Q) Calculate the IHL binary value if the total header size is :-

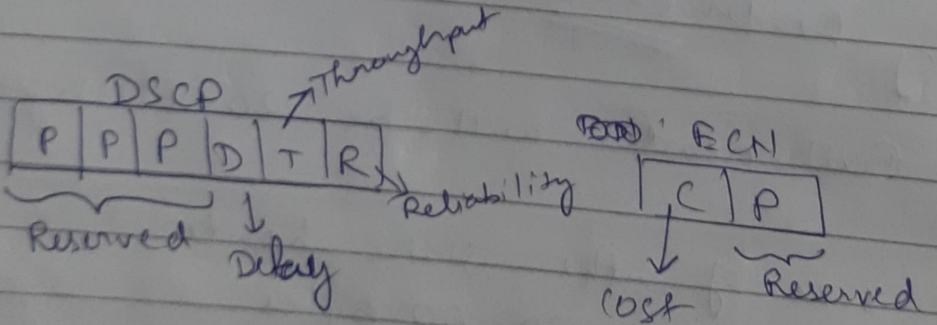
(i) 24 bytes → 24/4 = 6 = 0110

(ii) 31 bytes → 31/4 = 8 (ceiling value) = 1000

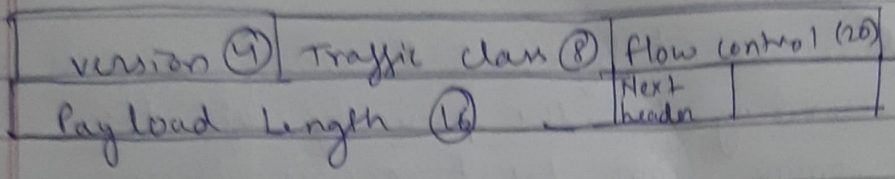
⇒ TL

Total length of the IPv4 packet which is 16 bits.

→ DS means differentiated services of size 8 bits divided into differentiated service code point and explicit ~~congestion~~ congestion notification.



IPv6 Header



TTL

→ Stands for Time To Live.

→ ~~Time to live~~

data ⟶ R1 ⟶ R2 ⟶ R3 ⟶ R1

let TTL = 3,

So, at R1, TTL = 3

at R2, TTL = 2 (it will decrement)

at R3, TTL = 1

at R1, TTL = 0 (Packet is discarded)

→ The range of TTL is 8 bit with value going from ~~0 to 255~~ 0 to 255.

→ It is Hop counter, and it is used to avoid infinite loop in system.

→ At every router, TTL is decremented and the network will discard the frame if TTL=0.

Protocol

→ Its size is 1 byte and its value is set according to the priority of the data coming from the transport layer.

* **Priority:-**

TCP > UDP > IGMP > ICMP

Header Check-Sum

→ Its size is 16 bit and it is used for determining any corruption inside the IPv4 header.

→ The size of option field is 0-40B and is not necessarily to be used.

Identification

→ Its size is two bytes and helps in providing a numbering to the fragmented packet in a network.

- **Flag**

→ It is 3 bits:-

- ~~Unused~~ Unused (X [redacted])
- Df (Don't Fragment)
- Mf (More Fragment)

Fragment offset

→ It is of 13 bits and it indicates the sequencing position of the fragmented packet.

IPv6 header

→ Version field is 4 bits indicating IPv4 or IPv6

→ Traffic class is of 1 byte having the same functionalities like DSCP & ECN.

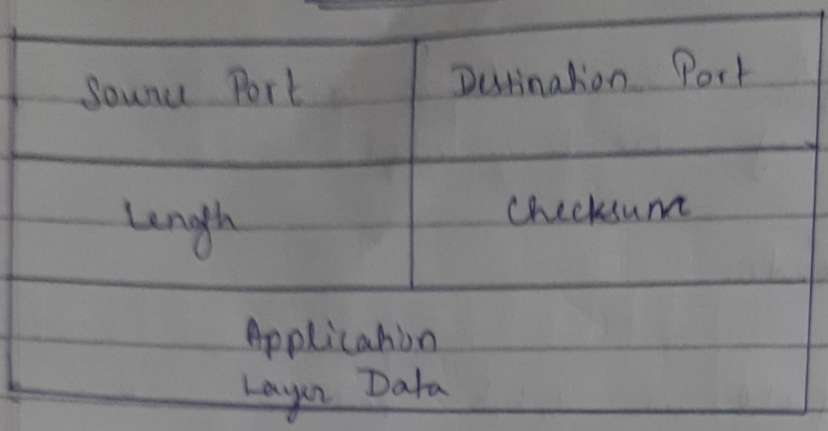
→ The flow control field is 20 bits and is used to inform the router about the labelled information of the IPv6 packet. Its work is same as the protocol field of IPv4.

→ Payload length is 16 bits representing length of the data packet. Next header is 1 byte explaining the type of transport layer protocol (TCP, UDP, IGMP, ICMP).

→ Hop limit is 1 byte having the same role as TTL of IPv4.

→ Source & Destination IP address is 128 bits each.

UDP Header



→ The header format of UDP is very small compared to TCP for which it is used in time sensitive applications like YouTube streaming.

→ It is a connection less protocol where data packets may be lost in the network.

→ Source and destination port address is of 16 bit each containing port number of the corresponding application.

→ The length of UDP header is 16 bit and the length of checksum used for detecting error is 16 bit.

→ UDP receives the layer 5 data that is application layer of TCP IP protocol.

TCP header

Source Port Address (16)	Destination Port Address (16)
Sequence Number (32)	
Acknowledgement Number (32)	
Header Length (4) | Reserved (6) | Control Bits (6)	Window (16)
Checksum (16)	Urgent (16)
Options (0-40 B)	
Application Layer Payload data	

→ TCP is a connection oriented protocol working in the transport layer having the same header format as that of IP.

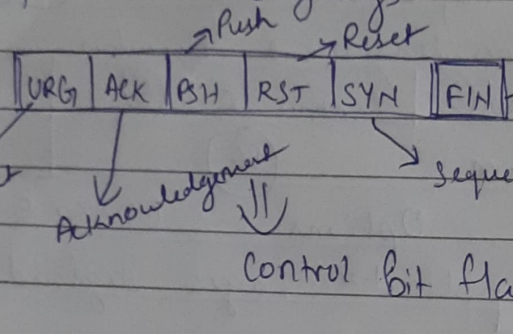
→ The header contains 16 bit source and destination port address each corresponding to the type of application.

→ The sequence number is a 32 bit field corresponding to the datagram fragmented from a single message.

→ For every sequence number a 32 bit acknowledgement number is generated whose value is sequence number +1.

→ The length of the header is 4 bit with a scaling factor 4 and value going from 5 to 15. There is a 6-bit reserve field for future advancement of the TCP header.

→ A 6 bit control field also called as flag is present in TCP header that controls the different operations of TCP. The 6 bits correspond to 6 flags



→ The Urgent flag indicates an emergency in the TCP header. Acknowledgement corresponds to the acknowledgement number.

→ The push flag helps in performing a pushing function in the event when payload data is absent.

→ The function of Reset is to initialize the TCP header to its original condition.

→ Syn corresponds to the synchronization sequence number generated by ~~trans~~ while transmitting the message.

→ FIN flag indicates the termination of a TCP session.

→ The window field is 16bit indicating the no. of bits or bytes accepted during data transmission bet^n sender & receiver.

→ Checksum is 16 bit that helps in identifying error within TCP header.

→ The size of options field is 0-40 bytes and the size of the starting header in TCP is 20B. and total header is 20 - 60 B.