**TCP/IP MODEL :**

The **TCP/IP model** (Transmission Control Protocol/Internet Protocol) is a conceptual framework for understanding how data is transmitted over networks, including the internet. It defines a set of networking protocols used for communication between computers.

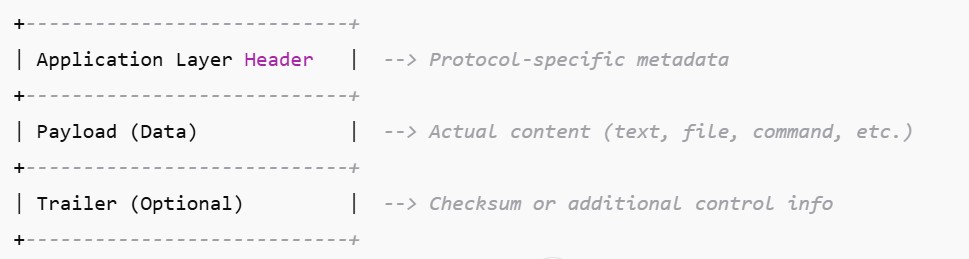
The model consists of **four layers**, each with specific functions:

1. **Application Layer :**

It Provides high-level services and interfaces for applications to communicate over the network.

Potocols : **HTTP, HTTPS, FTP, SMTP, DNS, Telnet, SSH, POP3, IMAP**.

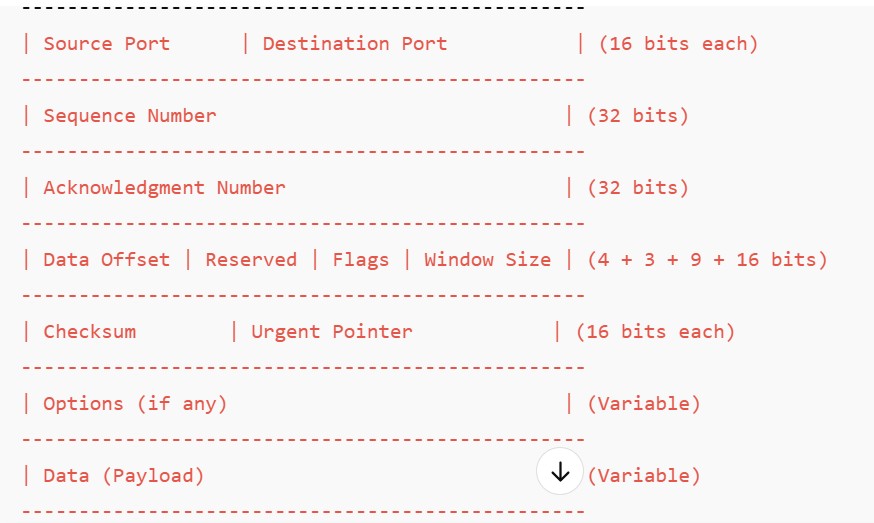
* General Packet Structure :



1. **Transport layer :**

The **Transport Layer** in the **TCP/IP model** is responsible for end-to-end communication between devices. It ensures reliable or fast delivery of data, depending on the protocol used (TCP or UDP). Here's a step-by-step breakdown of what happens at the Transport Layer:

* It assigns port number in packet so receiver can understand for which application the request has arrived for example we use 80 for web-request and 25 for SMTP etc.
* It also checks or assigns the protocol on which the data is gonna come or bind with so communication can happen in that way like TCP OR UDP.
* If TCP used then SYN, SYN-ACK, ACK id used to show the communication status.
* In this layer data packets are broken down into small segments (TCP) or Data-grams (UDP).
* Each segemnt get header which contain Source port, Destination port, Sequence Number, CheckSum.
* It also handles flow control by using window size which is estimated by getting maximum bandwidth which receiver can handle.
* It also do error checking and re-transmission by ACK and NACK .
* It use segment number in TCP to rearrange the segmented packets.
* In final step It uses FIN to finish the communication.
* General Packet Structure :

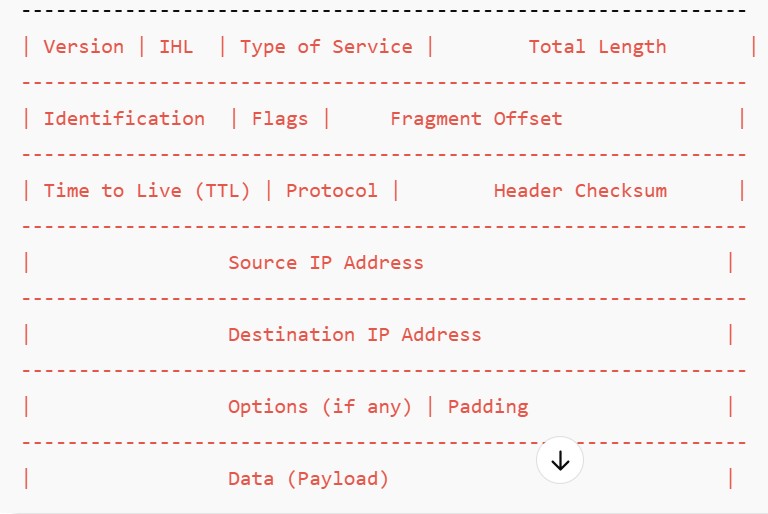


* Sequence Number is used to assemble the delivered segments into the correct order.
* Acknowledgment Number is sent to sender after receiver gets the data which contains the next byte number which is required by receiver.
* The **data offset** field (also known as the **header length**) is used in **TCP** (Transmission Control Protocol) headers. Its main purpose is to indicate where the actual data begins in the segment.
* Flag field tells that the data got by receiver or not by using ACK, FIN etc.
* Urgent pointer is used to tell that if data packet is needed to sent to receiver urgently or not.

1. **Network layer :**

The **Network Layer** in the TCP/IP model (equivalent to the **Internet Layer**) is responsible for **routing, addressing, and forwarding** data packets across different networks. It ensures that data moves from the source device to the destination device, even if they are on different networks.

* After getting data segments from Transport layer it converts the data into packets, it contains { Source and Destination IP, Protocol Information, Payload }.
* There are 2 IP options { IPV4 - 32 bits and IPV6 - 128 bits }.
* It also assigns a perfect path to data packets for data delivery using routing protocols { OSPF, BGP, RIP }.
* It also convert segments into fragments if data segments are too big.
* It also report error using ICMP if data is not delivered to receiver.
* General Packet Structure IPV4 :



* Version tells about the packet IP version so the receiver end can understand the packet.
* IHL tells about where the payload starts in packet so payload can be processed at receiver end.
* The **Type of Service (ToS)** field in the **IPv4 header** is used to specify how a packet should be handled in terms of priority and quality of service (QoS). It helps in **traffic prioritization, congestion control, and latency management**.

· **Traffic Prioritization** – Critical services like voice, video,and online gaming can get higher priority.

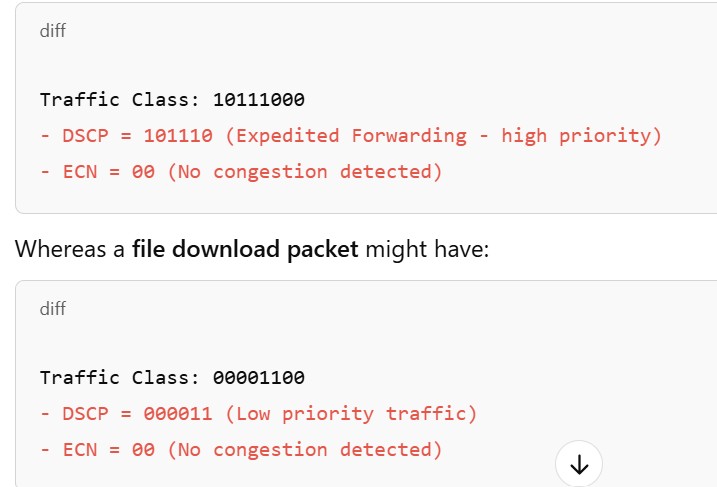
· **Quality of Service (QoS)** – Helps ISPs and enterprise networks manage bandwidth efficiently.

· **Congestion Control** – Prevents packet loss and improves network performance.

* Identification & Fragment Offset : When a single segment brakes into 2 fragments it contains same number which represents that the fragment belongs to same segment that is identification number at the same time the offset value tells that which fragment is 1st and which one is 2nd in order.
* Flags are used in this layer to do fragmentation of data, like the data is too big then the router set Data Flag = 0 that means need fragmented data.If the data is small the router set Data Flag = 1 means data is getting fragmented, At the same time More Flag = 1 when receiver is getting more fragments of data so it can wait for data before re-assembly of data start.If More Flag = 0 that means the coming fragment is the last fragment of the data so start re-assembly.
* Protocols tells about what prtocol is paylod is made of at transport layers.
* General Packet Structure of IPv6 Packet :



* Traffic class tells that which packet to be delivered first and is there any network congestion or not.

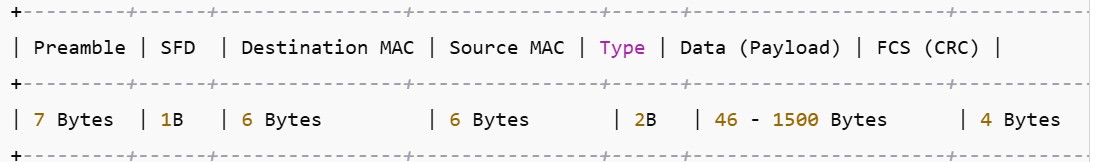


* Flow label used to label same type of ipv6 packets in a traffic so they can be treated equals in an operation.
* Hop limit tells that after how many hops the data packet can be discarded if it not delivered and Next header tells that which protocol the payload have for upper use like ( TCP, UDP, FTP )etc.

1. **Data link layer :**

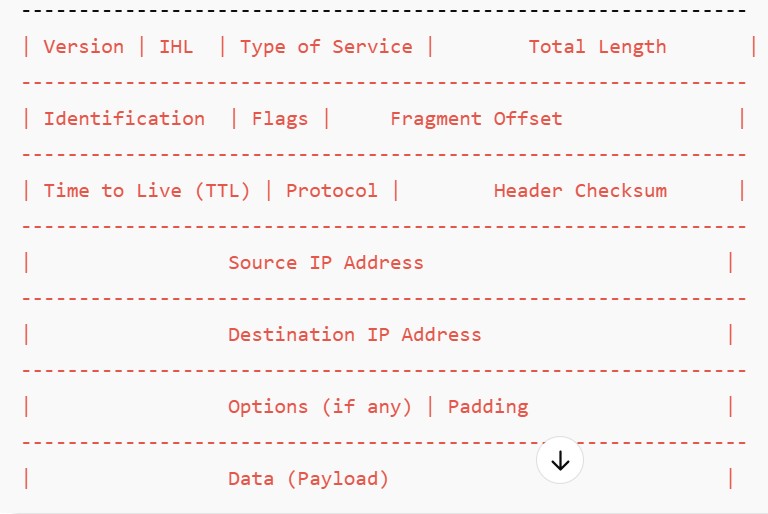
The **Data Link Layer (Layer 2)** is responsible for **framing, addressing, error detection, and physical transmission** of data over a specific medium.

* Data link layer converts the IP Packets in Frames which tells that from where the packet starts and ends.
* It also assign a MAC address to every frame so it can be delivered to the device in the internal network.
* It also do frame check sum at every hop or node while traveling to the receiver end for data integrity.
* It also do media access control for data transmission in the network.
* Basic packet structure at data link layer :



* SFD it tells about from where a frame is starting.
* Type tells about which protocol it is IPV4 or IPV6.
* Preamble is also used to find the start point of the frame but receiver use it to identify that I need to find this specific pattern of data so it locks the specific patter of data to get the packet.
* **Network Layer Protocols :**

1. **Ipv4 :**

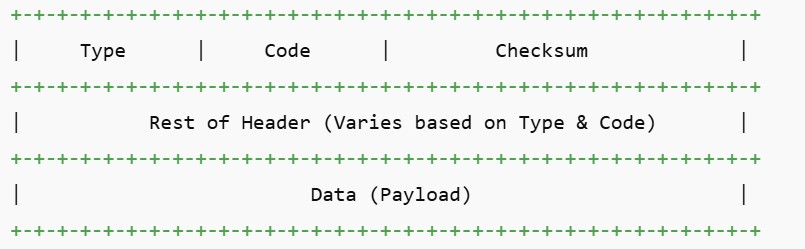
****

1. **Ipv6 :**

****

1. **ICMP :**

An **ICMP (Internet Control Message Protocol) packet** is used for sending error messages and operational queries, such as "ping" requests. ICMP is encapsulated inside an **IPv4 packet**, meaning it follows the IPv4 header.



* Type tells about the message.
* Code tells about from which the message come from like reciver or sender.
* Rest of Header containes :
  + Identifier : it tells about the which sender has sent the ping request.
  + Sequence number : Which ping request the user has sent like 1st or 2nd etc.

**4. UDP :**

UDP is a connection-less, lightweight transport protocol used in applications where **low latency** is more critical than reliability, such as **video streaming, VoIP, and online gaming**.

