Packet Structure:

A packet is a string of bits divided into three main sections:
- A set of headers
- The payload, the actual data being transmitted
- The trailer,
- sometimes called the footer
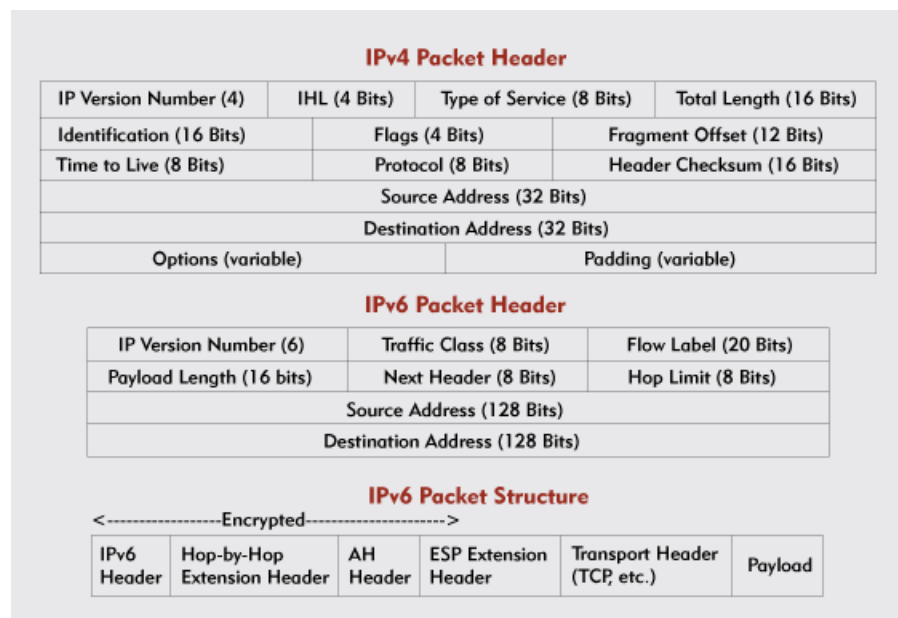
The headers consist of the following:
- **Internet Protocol (IP) version**
- **Header Length**
- **ToS (Type of Service):** Also called the Differentiated Services Code Point (rarely used)
- **Size of Datagram:** The size of the header plus the payload in bytes
- **Identification:** A 16-bit number. The destination computer combines the Identification with the source address to uniquely identify a packet, and uses these unique identifiers to reassemble data from packets.
- **Flags:** A bit used to let a router know whether it can fragment a packet or not. This is important, since many networks are restricted by the maximum size of packets they can forward.
- **Fragmentation Offset:** A value used to help reconstruct a fragmented packet
- **TTL (Time to Live):** The maximum number of hops a packet can take
- **Protocol:** The type of packet, i.e., TCP, UDP, ICMP, IGMP
- **Header Checksum:** A value used to detect errors, corruption
- **Source Address:** The IP address where the packet originated
- **Destination Address:** The IP address where the packet is going
- **Options:** Rarely used

The payload is the actual data being sent. This isn't normally read by routers en route like the headers and trailers are.
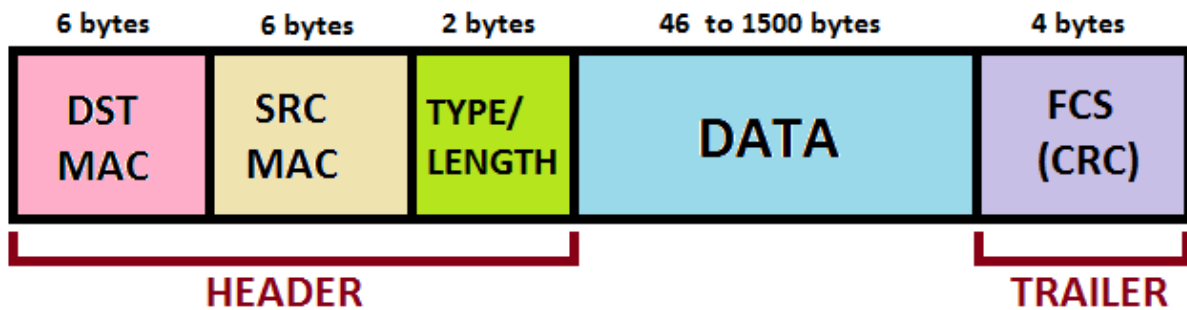
The trailer in most cases is nothing more than a pair of bits signaling the end of the packet. Occasionally, the trailer contains CRC (Cyclic Redundancy Check) error checking information.
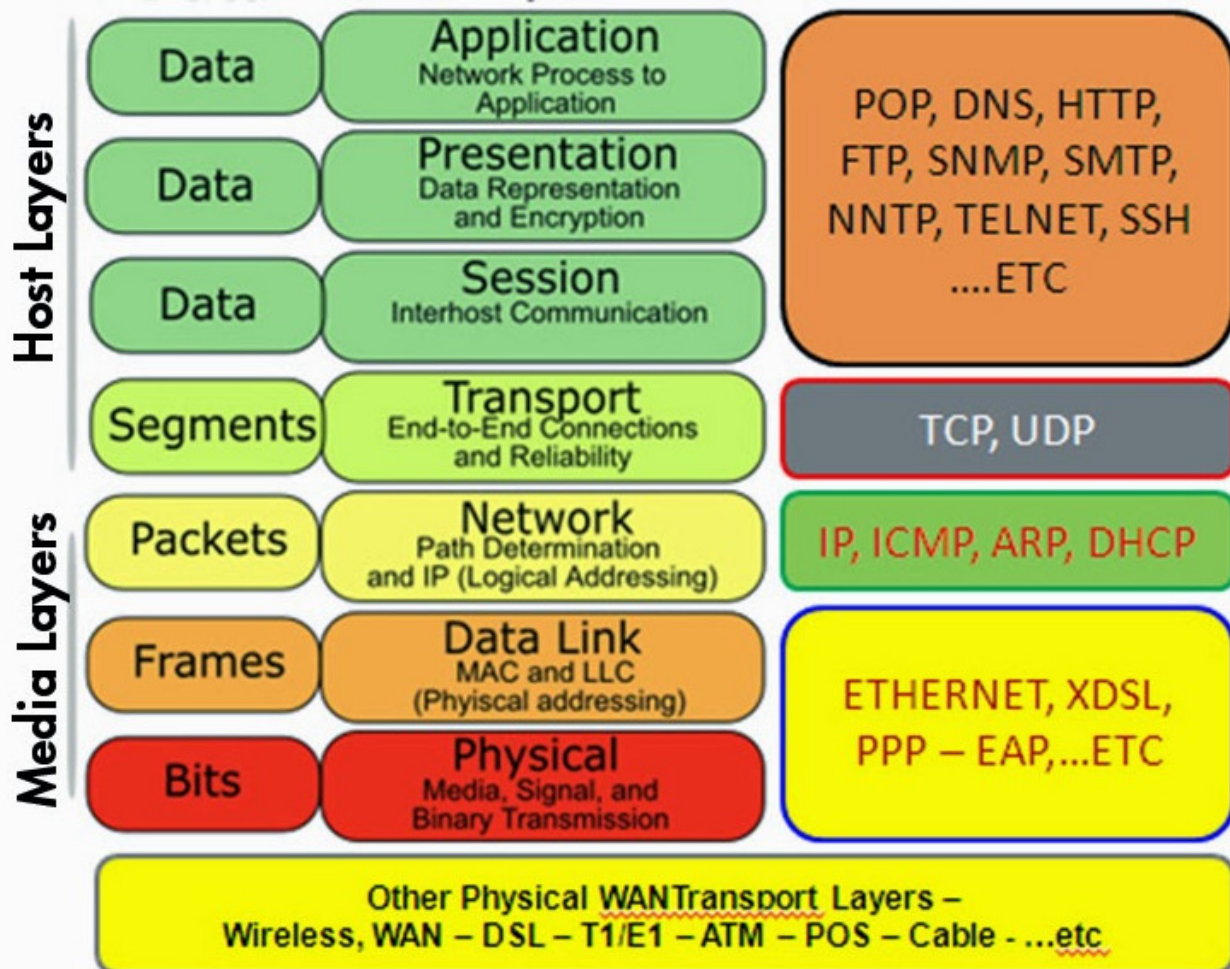
Structure Diagram:

IP,IPv6 Packets:

IPv4 Packet Header

IP Version Number (4)	IHL (4 Bits)	Type of Service (8 Bits)	Total Length (16 Bits)
Identification (16 Bits)		Flags (4 Bits)	Fragment Offset (12 Bits)
Time to Live (8 Bits)		Protocol (8 Bits)	Header Checksum (16 Bits)
Source Address (32 Bits)			
Destination Address (32 Bits)			
Options (variable)		Padding (variable)	

IPv6 Packet Header

IP Version Number (6)	Traffic Class (8 Bits)	Flow Label (20 Bits)
Payload Length (16 bits)	Next Header (8 Bits)	Hop Limit (8 Bits)
Source Address (128 Bits)		
Destination Address (128 Bits)		

IPv6 Packet Structure

<-----------------Encrypted---------------------->

IPv6 Header	Hop-by-Hop Extension Header	AH Header	ESP Extension Header	Transport Header (TCP, etc.)	Payload

ETHERNET II (DIX) FRAME

6 bytes	6 bytes	2 bytes	46 to 1500 bytes	4 bytes
DST MAC	SRC MAC	TYPE/ LENGTH	DATA	FCS (CRC)

HEADER | | | | **TRAILER**

OSI Example for Ethernet Media - TCP/IP STACK

Host Layers	Data	**Application** Network Process to Application	POP, DNS, HTTP, FTP, SNMP, SMTP, NNTP, TELNET, SSH ....ETC
	Data	**Presentation** Data Representation and Encryption	
	Data	**Session** Interhost Communication	
	Segments	**Transport** End-to-End Connections and Reliability	TCP, UDP
Media Layers	Packets	**Network** Path Determination and IP (Logical Addressing)	IP, ICMP, ARP, DHCP
	Frames	**Data Link** MAC and LLC (Phyiscal addressing)	ETHERNET, XDSL, PPP – EAP,...ETC
	Bits	**Physical** Media, Signal, and Binary Transmission	

Other Physical WAN Transport Layers –
Wireless, WAN – DSL – T1/E1 – ATM – POS – Cable - ...etc

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example	Central Device/Protocols		DOD4 Model

Application (7)
Serves as the window for users and application processes to access the network services.

End User layer Program that opens what was sent or creates what is to be sent
Resource sharing • Remote file access • Remote printer access • Directory services • Network management

User Applications

SMTP

Process

Presentation (6)
Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.

Syntax layer encrypt & decrypt (if needed)
Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**

JPEG/ASCII
EBDIC/TIFF/GIF
PICT

Session (5)
Allows session establishment between processes running on different stations.

Synch & send to ports (logical ports)
Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.

Logical Ports

RPC/SQL/NFS
NetBIOS names

Transport (4)
Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.

TCP Host to Host, Flow Control
Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing

P A C K E T — F I L T E R I N G

TCP/SPX/UDP

Host to Host

Network (3)
Controls the operations of the subnet, deciding which physical path the data takes.

Packets ("letter", contains IP address)
Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting

Routers

IP/IPX/ICMP

Internet

Data Link (2)
Provides error-free transfer of data frames from one node to another over the Physical layer.

Frames ("envelopes", contains MAC address)
[NIC card —— Switch —— NIC card]   (end to end)
Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control

Switch
Bridge
WAP
PPP/SLIP

Network

Physical (1)
Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.

Physical structure Cables, hubs, etc.
Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts

Hub

G A T E W A Y

Can be used on all layers

Land Based Layers