

29th of Dec 2025

## User Datagram Protocol (UDP)

User Datagram Protocol (UDP) is a communication protocol for time-sensitive applications like gaming, playing videos, or Domain Name System (DNS) lookups. UDP results in speedier communications because it does not spend time forming a firm connection with the destination before transferring the data. Because establishing the connection takes time, eliminating this step results in faster data transfer speeds.

However, UDP can also cause datagrams to get lost as they go from the source to the destination. It can also make it relatively easy for a hacker to execute a distributed denial-of-service (DDoS) attack.

### UDP Header (Layer 4)

Protocol Number : 17      Header Size : 8 bytes (fixed)

Field	Size	Description / Function
Source Port	16 bits	Identifies the sending application
Destination Port	16 bits	Identifies the receiving application
Length	16 bits	Total length of UDP header + data
CHECKSUM	16 bits	Error detection for header and data

Description: UDP provides connectionless, unreliable communication with low overhead and fast transmission, no retransmission or ordering.

## Transmission Control Protocol (TCP)

Transmission Control Protocol (TCP) is a core transport-layer protocol in the Internet Protocol (IP) suite that provides reliable, ordered, and error checked delivery of data between applications running on hosts connected to a network. TCP is connection-oriented, meaning it establishes a logical connection between sender and receiver through a three-way handshake before data transmission begins, ensuring both sides are ready and synchronized. It breaks application data into segments, assigns sequence numbers to each segment and uses acknowledgments (ACKs) to confirm successful receipt, allowing lost or corrupted segments to be detected and retransmitted. TCP also implements flow control through a sliding window mechanism, which prevents a fast sender from overwhelming a slow receiver, and congestion control algorithms (such as slow start and congestion avoidance) to adapt transmission rates based on network conditions.

and avoid congestion collapse. Additionally, TCP ensures in-order delivery by reassembling segments at the destination according to sequence numbers and discarding duplicates, while checksum verification provides basic error detection. Together, these mechanisms make TCP well suited for applications that require accuracy and completeness of data, such as web browsing, email, and file transfers.

Header size: minimum 20 bytes, Protocol number: 6, maximum 60 bytes

- minimum of 20 bytes (Protocol number + 5 fields)
- maximum of 60 bytes (Protocol number + 5 fields + checksum)

Field / Value	Size	Description / Function
Source Port	16 bits	Identifies the sending application
Destination Port	16 bits	Identifies the receiving application
Sequence Number	32 bits	Data ordering
Acknowledgment Number	32 bits	Confirms received data
Body offset	4 bits	TCP header length
Flags (SYN, ACK, FIN, RST, ...)	6 bits	Controls connection state
Window size	16 bits	Flow control
Checksum	16 bits	Error detection
Urgent Pointer	16 bits	Priority data
Options	Variable	Extra features (mss, window scaling)

Description: TCP provides reliable, ordered, and error-checked data delivery using acknowledgments and retransmissions.

IP Header: minimum 20 bytes, maximum 60 bytes

The IP header is a structured set of fields at the beginning of an Internet Protocol (IP) packet that provides information routers and hosts need to correctly deliver data across interconnected networks.

Header size: minimum 20 bytes, maximum 60 bytes

- minimum of 20 bytes
- maximum of 60 bytes

Field / Value	Size	Description & Function
Version	4 bits	IP version (IPv4 = 4)
Header length (HLEN)	4 bits	IP header size
Type of service (TOS/DSCP)	8 bits	Traffic prioritization
Total length	16 bits	Packet size
Identification	16 bits	Fragment Identification
Flags	3 bits	Fragment control
Fragment offset	13 bits	Fragment position
Time to Live (TTL)	8 bits	Limits packet lifetime
Protocol	8 bits	Identifies next layer (TCP=6, UDP=17)
Header Checksum	16 bits	Header error detection
Source IP address	32 bits	Sender's IP
Destination IP address	32 bits	Receiver's IP
Options (Optional)	Variable	Security, routing

Description : IP provides logical addressing and routing of packets across networks.

#### Ethernet Header :

The Ethernet header is the data structure that precedes the payload in an Ethernet frame and provides essential information for local network communication at the data link layer. It typically consists of the destination MAC address and source MAC address, each 48 bits long, which uniquely identify the receiving and sending network interfaces on the same physical network segment. Following these addresses is the EtherType (or length) field, which indicates the type of protocol encapsulated in the payload, such as IPv4, IPv6, or ARP, allowing the receiving device to hand the data to the correct upper-layer protocol. In some Ethernet variants, an optional IEEE 802.1Q VLAN tag may be inserted after the source MAC address to support virtual LANs and priority tagging. The Ethernet header enables switches to forward frames based on MAC addresses, supports protocol multiplexing through the EtherType field, and forms a crucial part of the overall Ethernet frame structure, ensuring efficient and accurate delivery of data within a local area network.

#### Header size :

• Ethernet header : 14 bytes • FCS (Trailer) : 4 bytes

- Total Ethernet frame overhead: 18 bytes

Field	Value	Size	Description / Function
Destination mac address	48 bits		Receiver hardware address
Source mac address	48 bits		Sender hardware address
Ether Type	16 bits		Identifies payload protocol (IPV4 = 0x0800, IPV6 = 0x86DD)
Frame Check Sequence (FCS)	32 bits		Error detection (CRC)

Description: Ethernet provides physical addressing and frame delivery within a local network.