TCP & UDP

TCP

Transmission Control Protocol (TCP) can be a transmission protocol used in addition to IP to ensure reliable data packets. TCP includes mechanisms that can solve many problems caused by packet-based messaging, such as lost packets, out-of-order packets, duplicate packets, and corrupted packets. Since TCP is the most commonly used protocol besides IP, the Web protocol stack is usually called TCP/IP. It is a typical method; it defines how to establish and maintain a network session, applications can exchange data through it. TCP is used with the Web Protocol (IP), which describes how computers send knowledge packets to each other. Together, TCP and IP are the basic rules that define the Web. TCP organizes data so that it is often transferred between the server and the client. It guarantees the integrity of the information transmitted over the network. Before sending data, TCP establishes a connection between the source and the target and keeps it until the communication starts. Then a large amount of knowledge is broken down into smaller packages while ensuring data integrity throughout the process.

Therefore, all high-level protocols that need to transmit data use the TCP protocol. Examples include peer-to-peer sharing methods such as File Transfer Protocol (FTP), Secure Shell (SSH), and Telnet. It is also common to send and receive e-mail using the Internet Message Access Protocol (IMAP), Post Office Protocol (POP), and Simple Mail Transfer Protocol (SMTP), as well as the Hypertext Transfer Protocol (HTTP) for Web access.

TCP connection

Establishing a connection requires that both the client and the server participate in the so-called three-way handshake. This method is usually weakened as follows:

- The client sends an SYN packet to the server- a connection request from its source port to its destination port.
- The server replies with an SYN/ACK packet to confirm receipt of the connection request.
- The client receives the SYN and ACK packet and replies with its ACK packet.

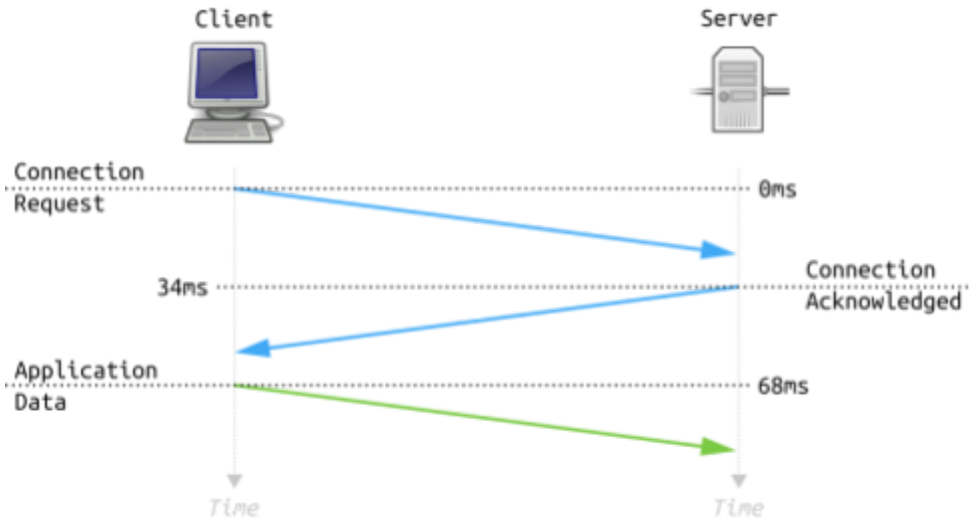

Figure 1: Three-Way Handshake

TCP Header

TCP surrounds each data packet with a header, which contains ten required fields for a total of 20 bytes (or octets). Each title includes information on the connection and the data currently being sent.

- **Source Port** -The port of the sending device.
- **Destination port** - The port of the receiving device.
- **Sequence Number** - The tool that initiates the TCP connection must choose a random initial sequence number, which is then incremented according to the number of bytes transmitted.
- **Confirmation Number** - The receiving device has a zero-based confirmation number. The number is incremented according to the number of bytes received.
- **TCP Data Offset** - This represents the size of the TCP header, expressed in 32-bit words. One word means four bytes.
- **Reserved data** - reserved fields are usually set to zero.
- **Control flags** - TCP uses nine control flags to manage the data flow in certain situations, such as B. When resetting is initiated.
- **TCP checksum window size** - The sender generates a checksum and transmits it in the header of each packet. The receiving device can use the checksum to detect errors in the received header and payload.
- **Urgent pointer** - When the URG control flag is an approximate value, this value indicates the offset of the sequence number indicating the last binding data byte.

- TCP optional data These are optional fields used to set the maximum segment size, selective acknowledgment, and activate window scaling for more efficient use of high-bandwidth networks.

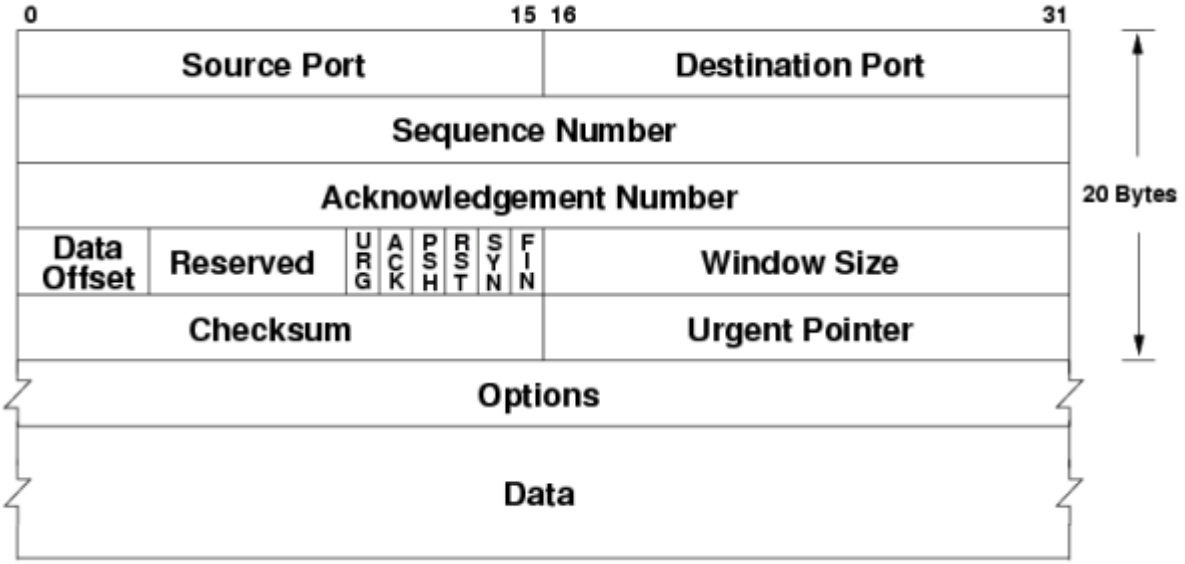

Figure 2: TCP Header

UDP

User Datagram Protocol (UDP) is mainly used to establish low-latency and fault-tolerant connections between applications on the Web. It speeds up the transfer by enabling knowledge transfer before the recipient reaches an agreement. Therefore, UDP is beneficial in time-sensitive communications, including Voice Internet Protocol (VoIP), naming systems DNS; to find and play video or audio. Like all network protocols, UDP can be a standardized method for transferring data between two computers on the network. Compared with other protocols, UDP accomplishes this process in a simple way: it sends data packets (knowledge transfer unit) to the target computer without first establishing a connection, specifying the order of the data packets or checking whether they arrive in this way (UDP packets are called "datagrams.")

UDP is faster than TCP, another popular transport protocol, but has lower reliability. The two computers begin to establish a connection during TCP communication using an automatic process called "handshake." When this handshake is completed, only once does one computer transmit the data packet to another computer.

UDP communication does not go through this process. Instead, one computer can start sending data to another computer:

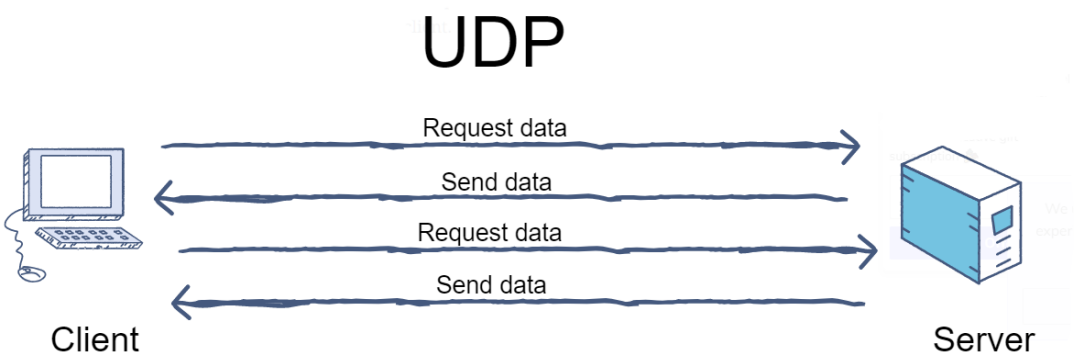

Figure 3: UDP Connection

UDP Header

- **Source port** - It is the port of the device sending the information. When the target computer does not need to reply to the sender, this field is usually set to zero.
- **Destination port** - It is the port of the device that is receiving the message. The UDP port number is usually between 0 and 65,535.
- **Length** - Represents the number of bytes, including the UDP header and UDP payload. The limit of the UDP length field is determined by the underlying IP protocol that does not transmit information.
- **Checksum** - The checksum enables the receiving device to check the integrity of the packet header and user data. It is optional in IPv4 but mandatory in IPv6.

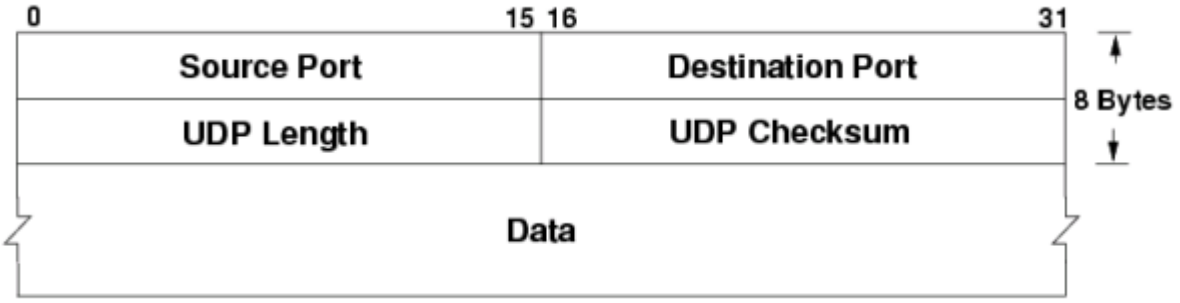

Figure 4: UDP Header