R&D Document: Working and Functionality of TCP, UDP, HTTP, HTTPS, and ICMP Protocols

Tushar Bhosale

June 2025

Contents

1 Introduction

Modern computer networks rely on a suite of protocols for reliable and structured communication. Among these, the Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Hypertext Transfer Protocol (HTTP), its secure version HTTPS, and the Internet Control Message Protocol (ICMP) are foundational. This document explores their working, purpose, and relevance in depth.

2 Working and Functionality of TCP UDP, HTTP, HTTPS, and ICMP Protocols

2.1 Transmission Control Protocol (TCP)

Transmission Control Protocol (TCP) is a connection-oriented protocol that ensures reliable data transmission across networked devices. It uses error checking, acknowledgment, retransmission of lost packets, and flow control mechanisms to provide robust communication.

TCP uses a three-way handshake to establish a connection:

- Sender sends a SYN (synchronize) packet.
- Receiver replies with SYN-ACK.
- Sender responds with ACK, establishing the connection.

Once the connection is established, data is broken into segments, each tagged with a sequence number. The receiver acknowledges received segments and requests retransmission if any are missing.

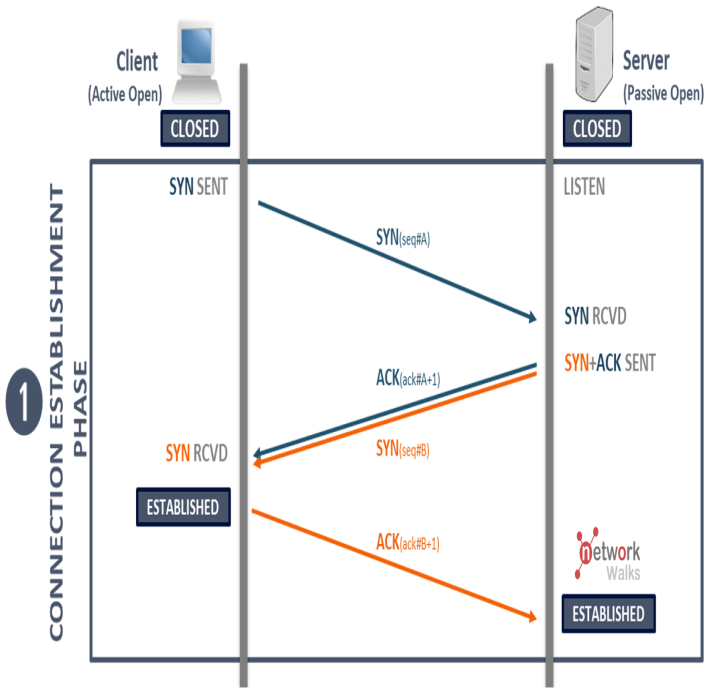

Figure 1: Three-way Handshake in TCP

2.2 User Datagram Protocol (UDP)

UDP is a connectionless protocol offering faster communication by eliminating the overhead of error checking and acknowledgments. It is often used in real-time applications like video streaming, gaming, or voice over IP.

Each UDP segment (datagram) consists of a header with port information and a payload. There is no guarantee of delivery, order, or error-free data transfer.

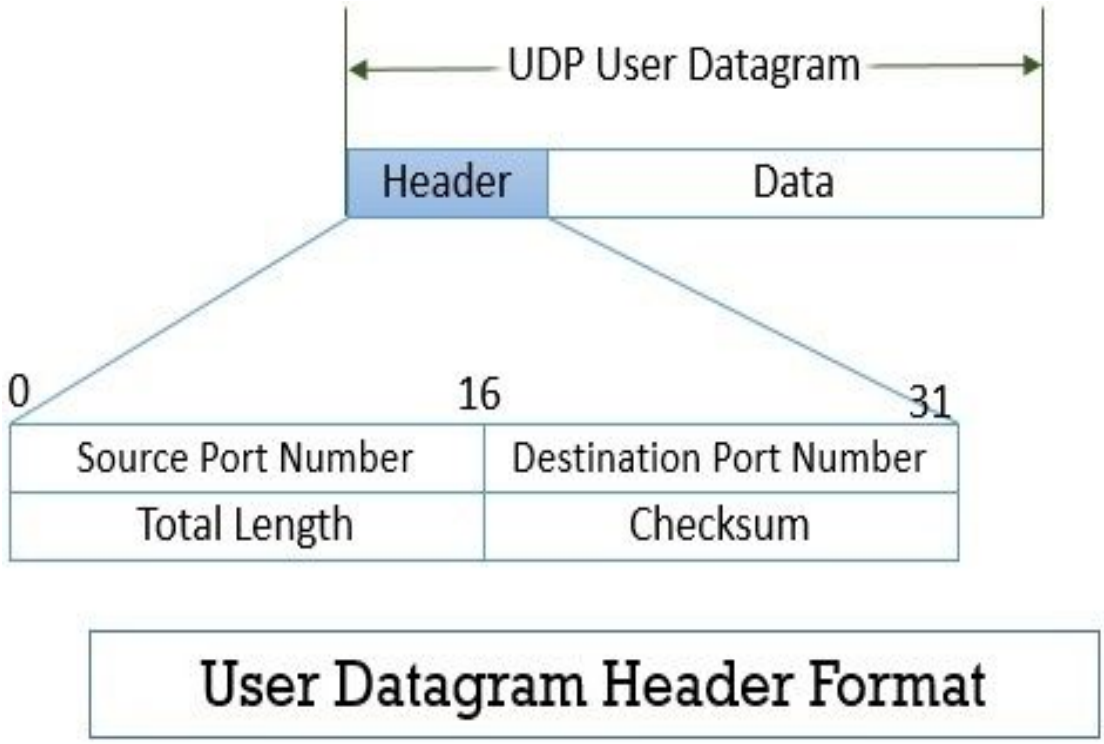

Figure 2: Three-way Handshake in TCP

2.3 HyperText Transfer Protocol (HTTP)

HTTP is an application-layer protocol used for transferring web pages on the internet. It follows a request-response model where a client sends a request and the server returns a response. It is stateless, meaning each request is independent.

Key characteristics:

- Uses TCP as transport.
- Default port: 80
- Lacks encryption.

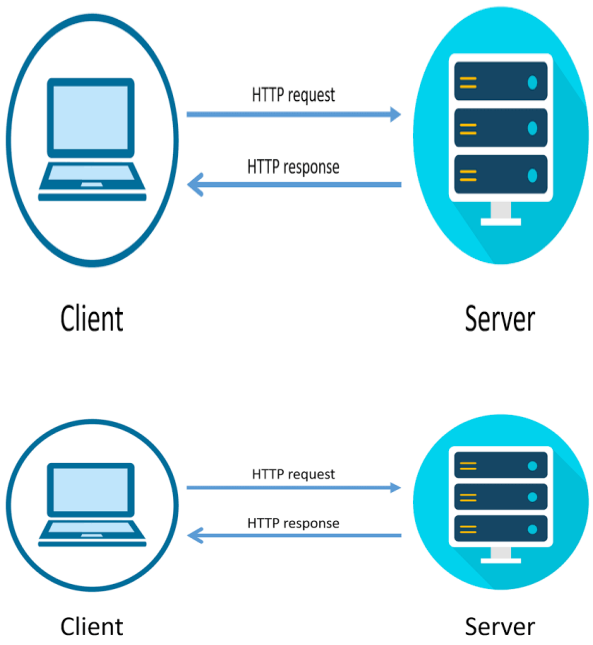

Figure 3: Enter Caption

Figure 4: HTTP Request-Response Model

2.4 HyperText Transfer Protocol Secure (HTTPS)

HTTPS is a secure version of HTTP. It uses SSL/TLS to encrypt communications between the client and server. This prevents eavesdropping and ensures data integrity.

Key characteristics:

- Uses TCP and encryption layer (SSL/TLS).
- Default port: 443
- Provides authentication, confidentiality, and integrity.

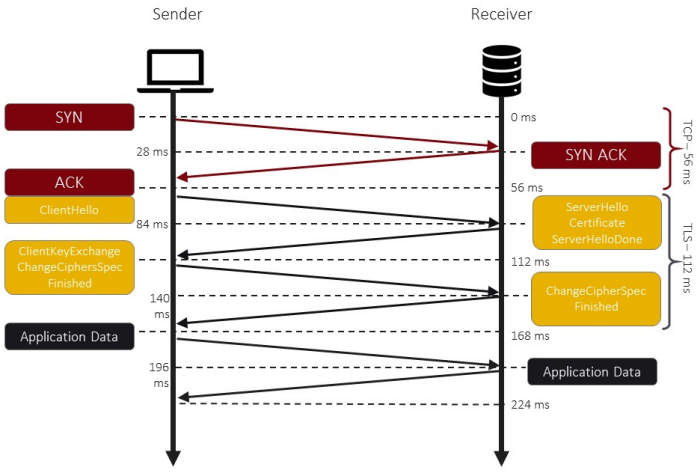

Figure 5: HTTPS Secure Communication Process

2.5 Internet Control Message Protocol (ICMP)

ICMP is a network-layer protocol used for diagnostics and control. It sends error messages and operational information such as destination unreachable or time exceeded.

Common tools using ICMP:

- `ping`: Tests reachability of a host.
- `traceroute`: Traces route from source to destination.

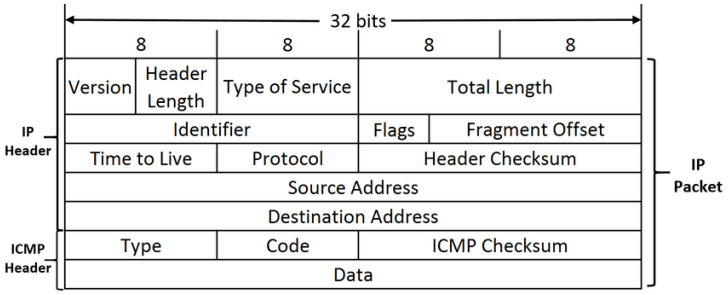

Figure 6: ICMP Packet Structure

3 Conclusion

Understanding the working and functionality of key protocols like TCP, UDP, HTTP, HTTPS, and ICMP is vital for network engineers and developers. Each serves a unique purpose, from reliable data transfer (TCP) to efficient diagnostic messaging (ICMP). Together, they form the backbone of modern internet communication.

4 References

- `https://www.geeksforgeeks.org/tcp-ip-model/`
- `https://developer.mozilla.org/en-US/docs/Web/HTTP`
- `https://www.cloudflare.com/learning/ddos/glossary/internet-control-message-proto`
- `https://www.cloudflare.com/learning/ssl/what-is-https/`
- `https://www.ibm.com/docs/en/zos/2.1.0?topic=protocols-tcpudp`