A R&D report
on

Working of TCP & UDP Protocols, HTTP, HTTPS & ICMP Protocols

Submitted to **Celebal Technologies** in partial fulfilment of the internship task

Week 1

in

Cloud Infra and Security

By

Mr. Ganesh Ghadge

StudentId: CT_CSI_CI_6124

Objective

This document is intended to offer a thorough understanding of the operation of the core TCP/IP protocols that underpin modern networking. By breaking down the TCP, UDP, HTTP, HTTPS, and ICMP protocols, we aim to simplify their functions, key features, and real-world applications, making the concepts more approachable for individuals at various levels of networking expertise.

The document's objectives are as follows:

- Explain the key characteristics, differences, and use cases of Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
- Explain the HyperText Transfer Protocol (HTTP) and the secure version of HTTP (or HTTPS), and how web browsers communicate with servers to access resources over the internet is important.
- Discuss how Internet Control Message Protocol (ICMP) is used for diagnostics, error reporting, and the role it plays in everyday tools, such as ping and traceroute.
- Use relatable examples of everyday network interactions, such as web browsers, file transfer, streaming video, and online gaming, to illustrate how these protocols work in practice.
- Understanding how TCP provides reliable communications, or how UDP is utilised for rapid transmission in real-time applications, can help in diagnosing network failures and optimising the performance of systems.

Introduction

In modern networking and internet communications, several protocols work together to maintain efficient, secure, and reliable data communication. Different protocols run on different layers of the TCP/IP model. They provide critical functionality for everyday activities, such as browsing the internet, sending emails, streaming videos, and troubleshooting network problems.

Each protocol has a different purpose:

- TCP and UDP, as transport layer protocols, control the transfer of data between computers. TCP is a protocol that provides a reliable means of communication, while UDP is able to transfer data more quickly and with less reliability.
- HTTP and HTTPS are application-layer protocols that control client-server communication for web browsing. HTTPS adds another layer of security through encryption.
- ICMP is an application layer protocol that is often used for diagnostics and error reporting. If a device on the network can't be reached for some reason, ICMP allows a distant device to communicate that information back to the person or algorithm causing the transmission with a type 3 ICMP code.

Knowing how these protocols really work at a technical level allows professionals of all different shapes and sizes to resolve issues in the network, optimise performance on the network, and design applications that are more secure and efficient. Whether you are a network engineer, a systems administrator, or someone just getting into networking, understanding how these protocols operate is foundational to being able to manage, navigate and troubleshoot the vast web of communication that is the internet.

Working of TCP Protocol

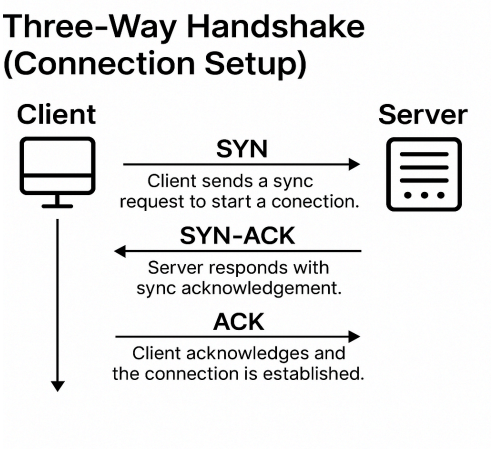
Transmission Control Protocol (TCP) is a transport layer protocol that is both connection-oriented and reliable. TCP is often a good choice for those applications where accurate delivery is important to the user, such as web browsing or email. TCP will deliver data in order without loss.

Characteristics of TCP

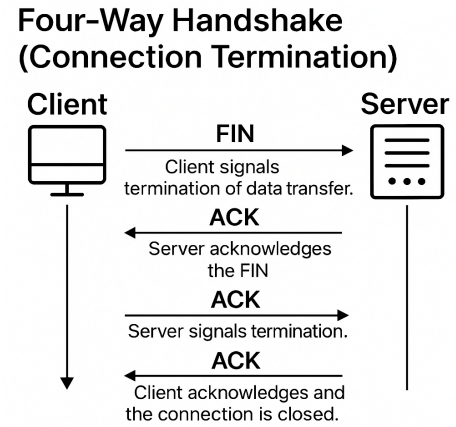
- Connection-Oriented: Before data transfer, a connection must be established through a mechanism known as the three-way handshake (SYN, SYN-ACK, ACK).
- Reliability: TCP guarantees that data is delivered without error and in sequence. If packets are lost or corrupted, TCP will retransmit them.
- Flow Control: TCP employs a sliding window mechanism to control the rate of delivery of data from sender to receiver, the intention being to avoid congestion on the network.
- Error Detection: TCP implements error detection and recovery through a checksum and an acknowledgement (ACK) that the data has been successfully received.

Working

1. Three-Way Handshake (connection setup)



2. Four-Way Handshake (Connection Termination)



Use Cases

- **Web Browsing** (HTTP/HTTPS)
- **Email** (SMTP/IMAP)
- **File Transfers** (FTP)
- **Remote Access** (SSH)

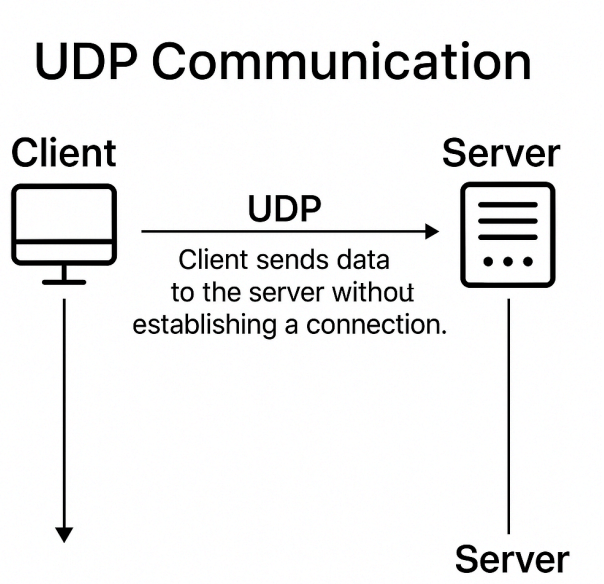
Working of UDP

User Datagram Protocol (UDP) is a simple, fast transportation layer protocol that is connectionless. Unlike TCP, UDP does not provide reliability or ordering, which makes it faster, but overall, not as reliable. It is useful for services that prioritise speed over reliability, such as streaming video or online gaming.

Important Properties of UDP

- Connectionless: There is no need to establish a connection before beginning data transfer, thus, the packets (datagrams) are sent as independent packets.
- Unreliable: UDP provides absolutely no guarantees on delivery, ordering, or error checks. If a packet is lost or corrupted, it is simply dropped, and not resent.
- Low Overhead: Because there are no "connection" setup or teardown procedures, UDP has much lower overhead than TCP, and is therefore faster.
- No Flow Control: Nothing is stopping the sender from overwhelming the receiver with data.

Working



Use Cases:

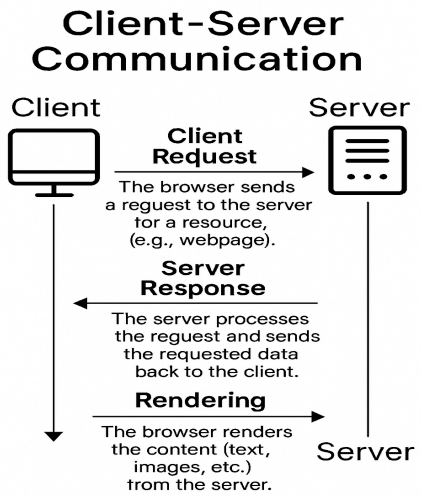
- Video Streaming (YouTube, Netflix)
- Voice over IP (VoIP) (Skype, WhatsApp)
- Online Gaming (Real-time multiplayer games)
- DNS Queries: DNS relies on UDP for fast query-response cycles.

Working of HTTP/ HTTPS

HyperText Transfer Protocol (HTTP) and its secure counterpart, HyperText Transfer Protocol Secure (HTTPS), are application layer protocols for communication between web browsers and web servers. While HTTP is the protocol for data transport on the web, HTTPS is the secure version of HTTP with encryption.

1. HTTP (HyperText Transfer Protocol)
    - Stateless: Each HTTP request and response is self-contained; there is no memory of previous requests/responses.
    - Request-Response Model: A client (usually a browser) sends a request to a server, and the server sends back the requested resource (HTML page, image, etc.).
    - Port: HTTP is usually available on port 80.

    Working:



2. HTTPS (Hypertext Transfer Protocol Secure)
    - Encryption: HTTPS employs SSL/TLS encryption to provide protection for the information exchanged from the client to the server.
    - Authentication: HTTPS provides assurance that the server is authentic and that the data cannot be intercepted or modified during transmission.
    - Port: HTTPS operates by default on port 443.

    Working:
    - SSL/TLS Handshake: The handshake occurs before any HTTP communication begins, at which time the SSL/TLS encryption is established between the client and the server.
    - Encrypted Communication: Once the handshake is completed, the client and server exchange the data securely, preventing eavesdropping or tampering.

Use cases:

- Web Browsing: Accessing websites (e.g., www.google.com, www.amazon.com).
- Online Banking: Secure transactions over the web.
- E-Commerce: Protecting sensitive customer data like credit card information.

Working of ICMP

The Internet Control Message Protocol (ICMP) is an application layer protocol that is primarily designed for error messaging and network diagnostics. ICMP is useful for relaying certain network issues between devices, such as an unreachable host or a timeout.

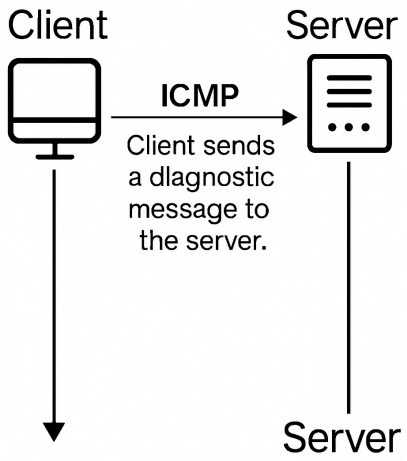
Key Features of ICMP

- Error Reporting: ICMP will report error messages pertaining to problems encountered in packet delivery, such as a destination host being unreachable or a timeout.
- Diagnostics: ICMP is useful for diagnostics and is used by applications such as ping and traceroute to determine connectivity and packet paths across networks.
- No User Data Exchange: ICMP does not provide a means for the exchange of user data, but only provides control messages to assist with managing the network.

Types of ICMP Messages

- Echo Request / Echo Reply (Ping): The ping command uses this to see if a host is reachable on the network.
- Echo Request: Message sent to the destination host.
- Echo Reply: Message received back from the destination host. This indicates that the host is up and reachable.
- Destination Unreachable: Sent when a packet cannot be delivered to the destination (e.g., the destination is down, or there is no route available).
- Time Exceeded: Indicates that a packet's time-to-live (TTL) has expired (used by traceroute to map a packet's path).

Working



Use Cases:

- Network Troubleshooting: ICMP helps in identifying connectivity issues, such as unreachable devices or routing problems.
- Path Tracing: Tools like traceroute use ICMP to trace the route packets take across networks.
- Ping Tests: Checking whether a device or server is available on the network.

References

1. TCP vs UDP - Difference and Comparison :
   https://www.diffen.com/difference/TCP_vs_UDP

2. GeeksforGeeks – Differences between TCP and UDP
   https://www.geeksforgeeks.org/differences-between-tcp-and-udp/