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

Assignment 1.2 for Celebal Technologies Internship

June 8, 2025

1. Introduction

This document presents a detailed comparison and working overview of TCP, UDP, HTTP, HTTPS, and ICMP protocols. These core protocols are fundamental to modern internet communication and have different features, use cases, and implementation methods.

2. TCP vs. UDP

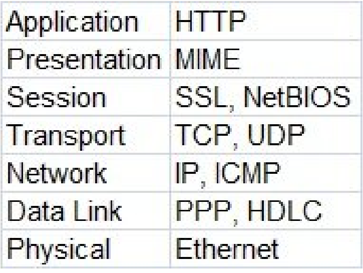
Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are two of the primary protocols operating at the Transport Layer of the OSI Model.

2.1. TCP - Transmission Control Protocol

TCP is a connection-oriented protocol. It ensures reliable and ordered delivery of a stream of bytes between applications. It uses mechanisms like three-way handshake, flow control, and error recovery. **Examples:** HTTP, HTTPS, FTP, Telnet

2.2. UDP - User Datagram Protocol

UDP is a connectionless protocol. It sends messages, called datagrams, without establishing a prior connection. It offers speed but not reliability. **Examples:** DNS, DHCP, TFTP, VoIP



Application	HTTP
Presentation	MIME
Session	SSL, NetBIOS
Transport	TCP, UDP
Network	IP, ICMP
Data Link	PPP, HDLC
Physical	Ethernet

Figure 1: OSI layer Protocols

3. Working of HTTP and HTTPS

3.1. HTTP - HyperText Transfer Protocol

HTTP is an application-layer protocol used for transmitting hypermedia documents, such as HTML. It is a stateless protocol that operates over TCP and uses port 80 by default.

Working Process:

1. The client (browser) initiates a TCP connection to the server
2. Client sends an HTTP request (GET, POST, PUT, DELETE, etc.)
3. Server processes the request and sends an HTTP response
4. Connection may be closed or kept alive for subsequent requests

Key Characteristics:

- Stateless protocol
- Request-response model
- Human-readable format
- Supports various methods and status codes

3.2. HTTPS - HTTP Secure

HTTPS is the secure version of HTTP that uses SSL/TLS protocols for encryption. It operates over port 443 and provides confidentiality, integrity, and authentication.

Working Process:

1. Client initiates connection and requests SSL/TLS handshake
2. Server presents its digital certificate
3. Client verifies the certificate and establishes encrypted session
4. Encrypted HTTP communication begins

Security Features:

- Data encryption using SSL/TLS
- Server authentication via certificates
- Data integrity protection
- Protection against man-in-the-middle attacks

4. ICMP - Internet Control Message Protocol

ICMP is a network layer protocol used by network devices to diagnose network communication issues and report errors. Unlike TCP or UDP, it is not used to exchange application data between systems but rather for network management and troubleshooting.

Primary Functions:

- Error reporting and diagnostics
- Network reachability testing
- Path discovery and troubleshooting
- Network congestion notification

Usage Examples: Network tools like `ping` and `traceroute` utilize ICMP to test connectivity and trace network paths.

Common ICMP Message Types:

- Echo Request and Echo Reply (used by ping command)
- Destination Unreachable (network/host/port unreachable)
- Time Exceeded (TTL expired, used by traceroute)
- Redirect (route optimization)
- Parameter Problem (malformed packets)

Working Process:

1. Network device encounters an error or needs to send diagnostic information
2. ICMP message is generated with appropriate type and code
3. Message is encapsulated in IP packet and sent to source
4. Receiving device processes ICMP message and takes appropriate action

References

- https://www.diffen.com/difference/TCP_vs_UDP
- Wikipedia: User Datagram Protocol
- Wikipedia: ICMP Protocol
- Wikipedia: HTTP & HTTPS