

R&D DOCUMENT ON WORKING OF TCP & UDP PROTOCOLS, WORKING OF HTTP, HTTPS & ICMP PROTOCOL

TITLE :

Working of TCP, UDP, HTTP, HTTPS, and ICMP Protocols.

PREPARED BY :

Richa Budhori

PURPOSE :

To explore the functionalities and working of various communication protocols used in network communication.

INTRODUCTION







The Internet relies on various communication protocols such as TCP, UDP, HTTP, HTTPS, and ICMP to enable data exchange between devices. These protocols play crucial roles in ensuring data is transmitted accurately, securely, and efficiently.

♦TCP (TRANSMISSION CONTROL PROTOCOL)

Type: Connection-oriented protocol

Layer: Transport Layer

Working:

-  Establishes connection by using a three-way handshake to establish reliable connection.
-  Breaks data into segments, which are then numbered sequentially.
-  Receiver sends ACK for received data. If ACK is not received, data is retransmitted.
-  Uses a sliding window mechanism for flow control.
-  Monitoring network traffic and adjusting data flow to prevent any congestion.
-  Connection ends with a four-way termination.

Use Cases: Web Browsing(HTTP, HTTPS), File Transfer(FTP), Emails(SMTP).

♦UDP (USER DATAGRAM PROTOCOL)

Type: Connectionless protocol

Layer: Transport Layer

Features:

- ☞ No connection setup required before sending data.
- ☞ Data is sent as individual datagrams.
- ☞ No acknowledgement or retransmission required.
- ☞ Faster, but less reliable than TCP.
- ☞ Header is minimal with only essential fields.

Use Cases: Online Gaming, DNS Queries, Live broadcasts.

TCP VS UDP

TCP	UDP
Connection-oriented protocol	Connectionless protocol
suited for applications that require high reliability	suitable for applications that need fast, efficient transmission
The speed of transfer for TCP is slower than UDP.	UDP is faster because error recovery is not attempted.
Data is sent sequentially.	UDP does not follow any order for sending data packets.
There is absolute guarantee that the data transferred remains intact and arrives in the same order in which it was sent.	There is no guarantee that the messages or packets sent would reach at all.
TCP header size is 20 bytes	UDP Header size is 8 bytes.
Performs flow control.	Does not perform flow control.
Acknowledgements are sent.	No acknowledgements are sent.

◆HTTP (HYPERTEXT TRANSFER PROTOCOL)

Type: Application layer protocol

Default Port: 80

Working:

- ☞ HTTP is a stateless, request-response protocol.

- ☞ A client sends an HTTP request to the server.
- ☞ The server processes the request and sends an HTTP response.
- ☞ Operates over TCP, hence it inherits TCP's reliability property.

Common Methods: GET (retrieve data), POST (submit data), PUT (update data), DELETE (remove data)

◆HTTPS (HYPERTEXT TRANSFER PROTOCOL SECURE)

Type: secure version of HTTP

Default port: 443

Features:

All HTTP requests/responses are encrypted to ensure:

- **Confidentiality**
- **Integrity**
- **Authentication**

☞ HTTPS = HTTP + SSL/TLS encryption.

☞ Establishes a secure connection using TLS handshake:

- 1) Client and server exchange certificates.
- 2) A shared encryption key is generated.

☞ All HTTP requests and responses are encrypted to ensure confidentiality, integrity and availability.

Use Cases: Online banking, E-commerce, Secure login pages.

◆ICMP (INTERNET CONTROL MESSAGE PROTOCOL)

Type: Not a transport protocol but supports network layer operations.

Layer: Network Layer

Features:

☞ ICMP is used by network devices to send error messages or diagnostic information.

☞ Common use: ping and traceroute.

☞ It does not carry application data, only controls messages.

☞ Vulnerable to misuse in attacks.

Use Cases: Diagnostics and error reporting.

CONCLUSION

Each protocol plays a specific role in enabling internet communication. Understanding their working helps in network design, enhancing performance, and securing communication systems.
