Name: Divij Shukla

Institute Name: Chandigarh University

Department: BE-CSE(H) – INFO. SECURITY

DOMAIN: Cloud Infra. & Security

Submission Date: 05-06-2025

Assignment Title 3: Prepare R&D Document working of TCP & UDP Protocol, working of HTTP, HTTPs & ICMP Protocol

TCP:

#INTRODUCTION

TCP (Transmission Control Protocol) is a connection-oriented protocol used for reliable data transmission over IP networks. It ensures that data is delivered error-free, in sequence, and without duplication.

#OBJECTIVE

To provide reliable communication between sender and receiver and to ensure data integrity, retransmission of lost packet and flow control.

#OVERVIEW

TCP is used in applications where accuracy is critical, such as web browsing, emails, and file transfers. It operates at the Transport Layer (Layer 4) of the OSI model.

#WORKING

1. **Connection Establishment – Three-Way Handshake:**
    - SYN: Client sends a SYN (synchronize) message.
    - SYN-ACK: Server replies with SYN-ACK.

- ACK: Client sends ACK. Connection is established.

2. **Data Transfer:**
   - Data is divided into segments.
   - Each segment has a sequence number.
   - Receiver sends ACKs for received segments.
   - Window size controls how much data can be sent before requiring an ACK**.**
3. **Error Handling:**
   - If no ACK is received, the segment is retransmitted.
   - TCP uses checksums for error detection.
4. **Connection Termination:**
   - Uses a four-step FIN handshake to close the connection gracefully.

UDP:

#INTRODUCTION

UDP is a connectionless and lightweight protocol used for fast and efficient data transmission without ensuring reliability.

#OBJECTIVE

Provide low-latency, minimal overhead communication, suitable for real-time applications like gaming, and streaming.

#OVERVIEW

UDP works at the Transport Layer (Layer 4) but does not guarantee delivery, order, or error correction.

#WORKING

1. No Connection Setup:

- Data is sent as datagrams without prior connection.

2. Fast Transmission:

- No handshaking process.
- Sender does not wait for acknowledgment.

3. Packet Loss & Duplication:

- Packets can be lost or arrive out of order.
- No retransmission mechanism.

4. Use Cases:

- Online games, video conferencing, DNS, live streaming.

WORKING OF HTTP:

#INTRODUCTION

HTTP is a stateless, application-layer protocol used for transmitting web pages and data between clients (browsers) and servers.

#WORKING

1. **Client Request:**
   - Client sends an HTTP request (GET, POST, etc.) to the server.
2. **Server Response:**
   - Server returns an HTTP response containing the requested data (HTML, JSON, etc.).
3. **Stateless Protocol:**
   - Each request is independent; no memory of past requests.
4. **Operates on Port 80.**

WORKING OF HTTPs:

#INTRODUCTION

HTTPS is a secure version of HTTP that uses SSL/TLS encryption to protect data exchanged between client and server.

#WORKING

1. **TLS Handshake:**
    - Server sends its digital certificate.
    - Client verifies the certificate.
    - Both negotiate encryption keys.
2. **Encrypted Communication:**
    - All HTTP messages are encrypted using TLS.
    - Prevents eavesdropping, man-in-the-middle attacks, and data tampering.
3. **Uses Port 443.**

WORKING OF ICMP:

#INTRODUCTION

ICMP [Internet Control Message Protocol] is a network-layer protocol used for error reporting and diagnostics (not for data transfer).

#WORKING

1. **Error Reporting:**
    - If a router or destination is unreachable, ICMP sends an error message (e.g., Destination Unreachable).
2. **Diagnostics:**
    - Used by ping and traceroute commands to test connectivity and path.
3. **Message Types:**
    - Echo Request/Reply (used in ping)

- Destination Unreachable
- Time Exceeded

4. **Not used to transmit user data.**