Name: Divij Shukla

Institute Name: Chandigarh University

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

DOMAIN: Cloud Infra. & Security

Submission Date: 05-06-2025

Assignment Title 2: Prepare R&D Document on working & functionality of TCP/IP Model

#INTRODUCTION

The TCP/IP Model (Transmission Control Protocol/Internet Protocol) is a set of networking protocols that allows computers to communicate over the internet. Unlike the OSI model, which is theoretical, the TCP/IP model is practical and widely used in real-world networks, including the Internet.

#OBJECTIVE

This R&D document aims to explain the architecture and functionality of the TCP/IP Model, analyze each layer's working mechanism and provide real-world examples of how it is used in data transmission.

#OVERVIEW OF TCP/IP MODEL

The TCP/IP model is a four-layer networking model developed by the U.S. Department of Defense to ensure end-to-end data communication. It forms the foundation of the modern Internet protocol suite, governing how data packets are addressed, transmitted, routed, and received.

Layer No.	Layer Name	Corresponds to OSI Layer
4	Application Layer	Application, Presentation, Session
3	Transport Layer	Transport
2	Internet Layer	Network
1	Network Access Layer	Data Link + Physical

#WORKING

1. **NETWORK ACCESS LAYER ---------- (LAYER 1)**

Role:

- Handles hardware-level communication and physical data transfer over the medium (cable, Wi-Fi, etc.)
- Combines the OSI model's Data Link and Physical layers.

Working:

- Converts packets into frames, adds MAC address, and sends it as electrical/optical signals over the network.
- Responsible for error detection (CRC) and media access (who sends first in shared media).

Technologies:

- Ethernet**,** Wi-Fi, Bluetooth, PPP

FUNCTIONALITY:

To prepare data for transmission over the physical media (like cables or wireless signals) and deliver it to the next-hop device (usually a switch or router) using MAC addressing.

- **Key Responsibilities:**

1. **Framing:**
    - Divides the network-layer packets into frames.
    - Adds a frame header and trailer (e.g., MAC addresses, CRC).
2. **Physical Addressing:**
    - Uses MAC (Media Access Control) addresses to identify the source and destination devices on the local network (LAN).
3. **Access to Physical Media:**
    - Controls how devices access and use the transmission medium (Ethernet, Wi-Fi, etc.).
    - Examples: CSMA/CD (Ethernet), CSMA/CA (Wi-Fi).
4. **Error Detection:**
    - Detects errors in frames using Cyclic Redundancy Check (CRC) or checksums.
    - If a frame is corrupted, it's discarded (not corrected here).
5. **Hardware Communication:**
    - Manages the actual electrical/optical/radio signal transmission of bits over cables or air.

- **Working Example:**

For example, you're sending a file to another computer on your LAN:

1. The Transport and Internet layers process the data and add headers.
2. The Network Access Layer takes this packet and:
    - Creates a frame
    - Adds MAC addresses (source and destination)
    - Sends it via Ethernet or Wi-Fi
3. The destination NIC receives the signal and processes the frame if the MAC address matches.

2. INTERNET LAYER ---------- (LAYER 2)

Role:

- Responsible for logical addressing (IP) and routing.
- Ensures packets reach the correct destination across networks.

Working:

- Takes segments from the Transport Layer, forms packets, and adds an IP header.
- IP header includes source and destination IP addresses.
- This layer uses routing algorithms to send packets across routers to reach the destination.

Protocols:

- IP (IPv4/IPv6) – addressing and routing
- ICMP – error messages (used by ping, traceroute)
- ARP – resolves IP to MAC address

FUNCTIONALITY:

1. **Logical Addressing (IP Addressing):**

    - Assigns a unique IP address to every device on the network.
    - Helps identify the source and destination of the data packet.

2. **Packet Routing and Forwarding:**

    - Determines the best path for data to travel through multiple routers and networks to reach its destination.
    - Uses routing tables maintained by routers**.**

3. **Packet Encapsulation:**

- Takes data from the Transport Layer and wraps it in an IP packet by adding an IP header.
- The IP header contains:
    - Source and destination IP addresses
    - Time to Live (TTL)
    - Protocol type (TCP/UDP)

4. **Error Handling and Diagnostics:**

- Protocols like ICMP provide error reporting (e.g., "Destination Unreachable").
- Used by tools like ping and traceroute to check connectivity.

- **WORKING EXAMPLE:**

You open www.example.com in a browser. The IP layer on your device:

1. Gets the destination IP address (e.g., 93.184.216.34).
2. Creates an IP packet with source and destination IPs.
3. Sends it to the router.
    - Routers in between examine the IP header and forward the packet until it reaches the destination network.
    - The destination host uses the IP header to determine if it's the intended recipient**.**

3. TRANSPORT LAYER ---------- (LAYER 3)

Role:

- Manages end-to-end connections between source and destination.
- Ensures reliable data delivery, segmentation, and error control.

Working:

- Breaks data from the Application Layer into segments**.**
- Adds a TCP or UDP header:
    - TCP ensures reliability with acknowledgments and retransmissions.
    - UDP provides faster, connectionless delivery without guarantee.
- Adds port numbers to identify specific services (e.g., port 80 for HTTP, port 443 for HTTPS).

Protocols:

- TCP – for reliable transmission (used in emails, web, etc.)
- UDP – for fast transmission (used in video streaming, VoIP, games)

FUNCTIONALITY:

1. **Reliable Data Transfer (using TCP):**
   - Ensures that all segments of data are delivered completely and in the correct order.
   - If any segment is lost or damaged, it will be retransmitted.

2. **Segmentation and Reassembly:**
   - Breaks large messages from the Application Layer into smaller units called segments.
   - Each segment is numbered and transmitted.
   - At the destination, the segments are reassembled into the original message.

3. **Connection Establishment and Termination:**
   - For TCP, a connection is established before data transfer using the 3-way handshake.
   - After data transfer, the connection is properly closed.

4. **Port Addressing:**
   - Uses port numbers to identify specific applications/services on the sending and receiving hosts.
   - Example:
     - Port 80: HTTP
     - Port 443: HTTPS
     - Port 25: SMTP

   Port numbers help the Transport Layer deliver the data to the correct app (like browser etc.).

5. **Flow Control:**
   - Prevents the sender from overwhelming the receiver with too much data at once.

- Uses mechanisms like sliding window protocol to manage this.

7. Congestion Control:

- Monitors network traffic and adjust the rate of data transmission to avoid network congestion (TCP).

- **WORKING EXAMPLE:**

  We send a message via WhatsApp:

1. WhatsApp (Application Layer) generates the message.
2. The Transport Layer breaks it into segments.
3. Adds port numbers and sequence numbers.
4. TCP ensures all segments reach the other phone in order and without loss.
5. At the receiving end, TCP reassembles the segments for WhatsApp to display.

4. APPLICATION LAYER ---------- (LAYER 4)

Role:

- The topmost layer that interfaces with user applications (like web browsers, email clients, etc.)
- Provides network services directly to the user.

Working:

- When you type www.google.com, the browser (an Application Layer client) creates an HTTP request.
- This data is passed down to the Transport Layer.

Common Protocols:

- HTTP/HTTPS – for web browsing
- FTP – file transfer
- SMTP/POP3/IMAP – email
- DNS – domain name resolution

FUNCTIONALITY:

1. **Provides User Services:**
    - Delivers network services directly to end-user applications.
    - Examples: web browsing, email, file transfer, chatting, remote login.

2. **Network Virtual Terminal:**
    - Enables a user to log in remotely to another computer as if it were local.
    - Protocol Example: Telnet

3. **Email Services:**
    - Supports sending, receiving, and managing emails over networks.
    - Protocols:
        - SMTP (Simple Mail Transfer Protocol) – sending emails
        - POP3 / IMAP – receiving emails

4. **File Transfer and Access:**
    - Allows users to transfer files between devices over a network.
    - Protocol Example: FTP (File Transfer Protocol)

5. **Name Resolution (DNS):**
    - Converts human-readable domain names (like www.google.com) into IP addresses (like 142.250.182.4).
    - Protocol: DNS (Domain Name System)

6. **Directory Services:**
    - Helps in managing user information and network resources.
    - Used in Active Directory, LDAP (Lightweight Directory Access Protocol)

7. **Authentication and Data Security (Optional):**
    - Some application-layer protocols also include authentication, encryption, or compression.
    - Example: HTTPS (HTTP with SSL/TLS for secure browsing)

#WORKING EXAMPLE:

We open Chrome and go to www.youtube.com:

1. Chrome (your app) makes an HTTP request (Application Layer).
2. The request is passed down through the TCP/IP layers and sent to YouTube's server.
3. YouTube sends back a response with the website content using the same protocol.
4. Your browser displays the website content to you.