**R&D Document: OSI Model – Working of All Layers**

**Overview:**

The **Open Systems Interconnection (OSI) Model** is a conceptual framework used to understand and implement standard protocols in network communication. It divides the networking process into **7 layers**, each responsible for specific functions.

**Layer 7: Application Layer**

* **Function:** Provides network services directly to user applications (like browsers, email clients).
* **Protocols:** HTTP, FTP, SMTP, DNS
* **Working:** Interfaces with user software and ensures communication with lower layers.

**Layer 6: Presentation Layer**

* **Function:** Translates data between application and network format; handles encryption, compression.
* **Example:** Converts .doc file to binary for transmission.
* **Working:** Maintains data syntax and encoding.

**Layer 5: Session Layer**

* **Function:** Establishes, maintains, and terminates sessions between applications.
* **Working:** Ensures data from different applications are properly separated and synchronized.

**Layer 4: Transport Layer**

* **Function:** Provides end-to-end communication control (segmentation, flow control, error control).
* **Protocols:** TCP, UDP
* **Working:** Breaks data into segments, tracks packets, retransmits lost packets (in TCP).

**Layer 3: Network Layer**

* **Function:** Handles logical addressing and routing (determining best path).
* **Protocols:** IP, ICMP
* **Working:** Adds source and destination IP addresses and routes packets.

**Layer 2: Data Link Layer**

* **Function:** Transmits frames over a physical medium, handles MAC addressing and error detection.
* **Sub-layers:** LLC (Logical Link Control) & MAC (Media Access Control)
* **Working:** Converts packets into frames and manages access to the physical medium.

**Layer 1: Physical Layer**

* **Function:** Transfers raw bits over the physical medium (cables, wireless).
* **Working:** Defines hardware specifications, voltage levels, timing.

**R&D Document: TCP/IP Model – Working & Functionality**

**Overview:**

The **TCP/IP Model**, or DoD Model, is a simplified 4-layer architecture used to structure all network communication.

**1. Application Layer**

* **Function:** Interfaces directly with user applications.
* **Protocols:** HTTP, HTTPS, SMTP, FTP, DNS, Telnet
* **Working:** Sends user data to transport layer for delivery.

**2. Transport Layer**

* **Function:** Provides logical communication between application processes.
* **Protocols:** TCP (connection-oriented), UDP (connectionless)
* **Working:** Handles segmentation, error detection, retransmission (TCP), or fast delivery (UDP).

**3. Internet Layer**

* **Function:** Handles logical addressing and routing.
* **Protocols:** IP, ICMP, ARP
* **Working:** Determines packet paths and ensures packets reach destination networks.

**4. Network Access Layer**

* **Function:** Interfaces with physical network for actual data transmission.
* **Includes:** Ethernet, Wi-Fi, ARP
* **Working:** Converts packets to frames, transmits bits over hardware.

**R&D Document: TCP & UDP Protocols – Working**

**TCP (Transmission Control Protocol)**

* **Type:** Connection-oriented
* **Functions:**
  + Reliable delivery (ACKs, retransmission)
  + Flow control (Windowing)
  + Congestion control (e.g., Slow Start)
* **Working:**
  + Three-way handshake to establish a connection.
  + Data transfer with sequence and acknowledgment numbers.
  + Graceful connection termination.

**UDP (User Datagram Protocol)**

* **Type:** Connectionless
* **Functions:**
  + Unreliable delivery (no ACKs)
  + Minimal overhead, faster transmission
* **Working:**
  + Sends datagrams directly to destination without prior connection.
  + Common in video streaming, DNS, VoIP.

**📄 R&D Document: HTTP, HTTPS & ICMP Protocols – Working**

**HTTP (HyperText Transfer Protocol)**

* **Port:** 80
* **Working:**
  + Stateless, client-server protocol
  + Client sends GET/POST request; server responds with resources (HTML, JSON, etc.)

**HTTPS (HTTP Secure)**

* **Port:** 443
* **Working:**
  + HTTP over SSL/TLS encryption
  + Ensures confidentiality, integrity, and authenticity using certificates
  + Handshake includes exchanging public keys and generating session keys.

**ICMP (Internet Control Message Protocol)**

* **Use:** Error reporting and diagnostics
* **Working:**
  + Used by tools like ping and traceroute
  + Sends control messages (e.g., destination unreachable, time exceeded)
  + Not used for data transport, but for network troubleshooting