RESEARCH AND DEVELOPMENT DOCUMENT

**ON**

**Working of all the layers of OSI Model**

A blue background with white text

AI-generated content may be incorrect.

A blue background with white text

AI-generated content may be incorrect.

By

**Anirudh Sharma**

**(CT\_CSI\_CI\_66)**

Under

Celebal Summer Internship on Cloud Infra & Security

Table of Contents

[OSI Model 3](#_heading=h.pgu2ymkn3oxj)

[Layers of OSI Model 4](#_heading=h.yfz6kqbibnzt)

[Application Layer 4](#_heading=h.89jihtafsog3)

[Presentation Layer 6](#_heading=h.unuah2e033rd)

[Session Layer 8](#_heading=h.3qip6i36q5vk)

[Transport Layer 10](#_heading=h.wezssftov8kk)

[Network Layer 12](#_heading=h.g5xetiaanpaq)

[Data Link Layer 14](#_heading=h.hsqpf169j2s5)

[Physical Layer 16](#_heading=h.mf2lu2bqo94k)

References…………………………………………………………………………………………………………………………19

**OSI Model**

# The OSI (Open Systems Interconnection) Model is a set of rules that explains how different computer systems communicate over a network. OSI Model was developed by the International Organization for Standardization (ISO). The OSI Model consists of 7 layers, and each layer has specific functions and responsibilities. This layered approach makes it easier for different devices and technologies to work together. OSI Model provides a clear structure for data transmission and managing network issues.

# The OSI Model is widely used as a reference to understand how network systems function.

**Advantages of OSI Model**

* It divides network communication into 7 layers which makes it easier to understand and troubleshoot.
* It standardizes network communications, as each layer has fixed functions and protocols.
* Diagnosing network problems is easier with the**OSI model.**
* It is easier to improve with advancements as each layer can get updates separately.

**Disadvantages of OSI Model**

* The OSI Model has seven layers, which can be complicated and hard to understand for beginners.
* In real-life networking, most systems use a simpler model called the Internet protocol suite (TCP/IP), so the OSI Model is not always directly applicable.
* Each layer in the OSI Model adds its own set of rules and operations, which can make the process more time-consuming and less efficient.
* The OSI Model is more of a theoretical framework, meaning it's great for understanding concepts but not always practical for implementation.

# Layers of OSI Model

Layer 7—Application Layer

Layer 6—Presentation Layer

Layer 5—Session Layer

Layer 4—Transport Layer

Layer 3—Network Layer

Layer 2—Data Link Layer

Layer 1—Physical Layer

## Application Layer

The Application Layer of OSI (Open System Interconnection) model, is the top layer in this model and takes care of network communication. The application layer provides the functionality to send and receive data from users. It acts as the interface between the user and the application. The application provides services like file transmission, mail service, etc.

**Functions of Application Layer**

* Data Representation
* Network Service Access
* Application Protocols
* Session Management

**Working of Application Layer**

* At first, client sends a command to server and when server receives that command, it allocates port number to client.
* Thereafter, the client sends an initiation connection request to server and when server receives request, it gives acknowledgement (ACK) to client through client has successfully established a connection with the server.

**Application Layer Protocols:**

* **HTTP (Hyper Text Transfer Protocol):** Used for browsing the web. It transfers web pages and works on a client-server model. It uses port 80 and is stateless.
* **DNS (Domain Name System):** Converts website names (like google.com) into IP addresses. It uses port 53.
* **TELNET:** Allows users to access another computer remotely and manage files over the internet. Uses port 23.
* **DHCP (Dynamic Host Configuration Protocol):** Automatically assigns IP addresses to devices in a network. Uses ports 67 and 68.
* **FTP (File Transfer Protocol):** Transfers files between computers. Uses port 20 for data and 21 for control.
* **SMTP (Simple Mail Transfer Protocol):** Sends emails from one device to another. Uses ports 25 and 587.
* **NFS (Network File System):** Lets users access files over a network as if they were on their own computer. Uses port 2049.
* **SNMP (Simple Network Management Protocol):** Collects and manages network device information. Uses ports 161 (TCP) and 162 (UDP).

**Services Provided by Application Layer Protocols**

* The Application Layer protocol defines process for both parties which are involved in communication.
* These protocols define the type of message being sent or received from any side (either source host or destination host).
* These protocols also define basic syntax of the message being forwarded or retrieved.
* These protocols define the way to send a message and the expected response.
* These protocols also define interaction with the next level.

## Presentation Layer

Presentation Layer is the 6th layer in the Open System Interconnection (OSI) model. This layer is also known as **Translation layer**, as this layer serves as a data translator for the network. The data which this layer receives from the Application Layer is extracted and manipulated here as per the required format to transmit over the network. The main responsibility of this layer is to provide or define the data format and encryption. The presentation layer is also called the **Syntax layer** since it is responsible for maintaining the proper syntax of the data.

**Functions of Presentation Layer**

* Data Translation
* Data Compression
* Data Encryption/Decryption
* Syntax and Semantics Management

**Working of Presentation Layer**

* **Data Translation**: Converts data into a standardized format (e.g., EBCDIC to ASCII).
* **Data Compression**: Reduces data size to optimize bandwidth and speed.
* **Data Encryption/Decryption**: Secures data during transmission (e.g., SSL/TLS).
* **Syntax and Semantics**: Ensures data is interpreted correctly across systems.
* **Interoperability**: Bridges differences in data formats between devices.

**Presentation Layer Protocols:**

* **AFP (Apple Filing Protocol):** A file-sharing protocol used mainly on Mac systems for accessing files over a network.
* **LPP (Lightweight Presentation Protocol):** Offers ISO presentation services over TCP/IP networks. It helps in handling data formats in a lightweight way.
* **NCP (NetWare Core Protocol):** Used for accessing services like file sharing, printing, time sync, and messaging in NetWare networks.
* **NDR (Network Data Representation):** Defines how data types are represented when sent across the network, especially for remote communication.
* **XDR (External Data Representation):** Standard way to encode and decode data to ensure different systems can understand it, even if they use different architectures.
* **SSL (Secure Socket Layer):** Secures communication between a web browser and server by encrypting the connection, keeping the data private and safe from attackers.

**Services Provided by the Presentation Layer**

The presentation layer helps in making sure that data sent between devices is properly understood. It offers the following key services:

* **Data Compression:** Reduces the size of data so it takes up less bandwidth during transfer, making communication faster.
* **Data Encryption/Decryption:** Adds encryption when sending data and decrypts it when receiving. This ensures secure communication between devices.
* **Data Formatting:** Ensures the data is in a proper, readable format so that different systems can understand and process it without compatibility issues.
* **Transfer Syntax Negotiation:** Helps decide the format in which data will be transferred between devices so that both ends agree and understand the structure.
* **Efficient Data Handling:** Compresses the data before sending it to the session layer, improving speed and reducing the load on the network.

## Session Layer

The Session Layer is the 5th layer in the Open System Interconnection (OSI) model which plays an important role in controlling the dialogues (connections) between computers. This layer is responsible for setting up, coordinating, and terminating conversations, exchanges, and dialogues between the applications at each end. It establishes, manages, and terminates the connections between the local and remote applications.

**Functions of Session Layer**

* **Session Establishment**
* **Communication Synchronization**
* **Activity Management**
* **Dialog Management**
* **Data Transfer**
* **Resynchronization**

**Working of Session Layer**

* The Session Layer manages communication sessions between applications over a network.
* It establishes connections, negotiating session parameters like authentication and communication direction (full-duplex or half-duplex).
* It oversees data exchange by using tokens to manage transmission rights and prevent collisions.
* Synchronization techniques are implemented, inserting checkpoints for recovery in case of disruptions.
* It ensures orderly communication, reducing message loss, duplication, or errors caused by overlapping communication.
* The Session Layer gracefully terminates the session, ensuring all data is exchanged and both sides agree to close

**Session Layer Protocols:**

* **ADSP (AppleTalk Data Stream Protocol):** Created by Apple, this protocol connects devices in a local network without setup. It includes AARP and NBP for automatic address resolution and name binding.
* **RTCP (Real-time Transport Control Protocol):** Works with RTP to monitor and manage streaming quality by reporting stats like packet loss and delays.
* **PPTP (Point-to-Point Tunnelling Protocol):** Used to create VPNs by sending encrypted data through a tunnel. It ensures private and secure remote access.
* **PAP (Password Authentication Protocol):** Authenticates users in a network using passwords. It uses a simple handshake method during connection setup.
* **RPCP (Remote Procedure Call Protocol):** Allows a program to run code on another machine without needing to know the details of the remote execution. It's a client-server interaction method.
* **SDP (Sockets Direct Protocol):** Supports fast communication using RDMA instead of TCP. It helps boost data transfer speed without changing how applications work

**Services Provided by Session Layer Protocols**

* **Session Establishment, Maintenance, and Termination:** It starts, keeps alive, and ends sessions between devices so that the communication can happen smoothly.
* **Synchronization:** Adds checkpoints in the data stream. This means if a connection fails, it can restart from the last checkpoint instead of starting over.
* **Dialog Control:** Manages who can send or receive data at a given time (either one-way or two-way communication), helping avoid data mix-ups.
* **Token Management:** Ensures that only one party can access a critical section of data or process at a time, avoiding conflicts.
* **Session Recovery:** If a session is interrupted, this layer helps recover and continue the session without data loss.

## Transport Layer

The transport layer, or layer 4 of the OSI model, controls network traffic between hosts and end systems to guarantee full data flows.It is positioned between the network and session layers in the OSI paradigm. The data packets must be taken and sent to the appropriate machine by the network layer. After that, the transport layer receives the packets, sorts them, and looks for faults. Subsequently, it directs them to the session layer of the appropriate computer program. Now, the properly structured packets are used by the session layer to hold the data for the application.

**Functions of Transport Layer**

* **End-To-End Communication**
* **Flow Control**
* **Connection Establishment**
* **Connection Termination**
* **Reliable Data Delivery**

**Working of Transport Layer**

* The primary function of the transport layer is to give application processes operating on several hosts direct access to communication services.
* Logical communication between application processes operating on separate hosts is facilitated by the transport layer. Application processes use the logical communication offered by the transport layer to deliver messages to one other even when they are running on different hosts and are not physically connected.
* The network routers do not implement the transport layer protocols; only the end systems do.
* For instance, the network layer receives services from TCP and UDP, two transport layer protocols, which offer distinct functionalities.
* Protocols at the transport layer offer multiplexing and demultiplexing capabilities. In addition, it offers other services including bandwidth assurances, latency guarantees, and dependable data transport.
* Every application at the application layer can send a message via either TCP or UDP. Either of these two protocols can be used by the application to interact. The internet protocol on the internet layer will then be communicated with by both TCP and UDP. The transport layer is readable and writeable by the applications.

**Transport Layer Protocols**

**Transmission Control Protocol (TCP)**

* **Connection-oriented** and **reliable**.
* Establishes a connection, sends data, and then closes the connection.
* Ensures data arrives correctly and in order.
* Used in email, file transfer, and web browsing.

**User Datagram Protocol (UDP)**

* **Connectionless** and **faster**, but not reliable.
* Sends data without checking for errors or order.
* Ideal for live streaming and online games where speed matters.

**Stream Control Transmission Protocol (SCTP)**

* **Reliable** like TCP but supports **multiple streams and paths**.
* Suitable for applications needing fault tolerance and advanced features.
* Used in telecom and real-time applications.

**Services Provided by Transport Layer Protocols**

* **Segmentation and Reassembly:** Breaks large messages into smaller segments for transmission and reassembles them at the receiver's end.
* **Connection Control:** Manages connection types – connection-oriented (TCP) and connectionless (UDP).
* **Flow Control:** Ensures that the sender does not overwhelm the receiver by sending too much data too quickly.
* **Error Control:** Uses mechanisms like checksums and acknowledgments to detect and correct errors in data transmission.
* **Reliable Data Transfer (TCP):** Guarantees that data is delivered correctly, in order, and without duplication.

## Network Layer

The Network Layer is the 5th Layer from the top and the 3rd layer from the Bottom of the OSI Model. It is one of the most important layers which plays a key role in data transmission. The main job of this layer is to maintain the quality of the data and pass and transmit it from its source to its destination. It also handles routing, which means that it chooses the best path to transmit the data from the source to its destination, not just transmitting the packet. There are several important protocols that work in this layer.

**Functions of Network Layer**

* **Assigning Logical Address**: It provides unique IP addresses to devices for identification and communication across networks.
* **Packetizing**: It encapsulates data into packets for efficient transmission.
* **Host-to-Host Delivery**: It ensures data is delivered from the sender to the intended receiver across networks.
* **Forwarding**: It is the process of moving packets from the input to the appropriate output interface in a router, based on the destination address
* **Fragmentation and Reassembly**: It splits large packets into smaller fragments for transmission and reassembles them at the destination.
* **Logical Subnetting**: It divides larger networks into smaller subnetworks for better management and routing efficiency.
* **Network Address Translation (NAT):** Maps private IP addresses to a public IP for internet access, conserving IPs and adding security.
* **Routing**: It determines the best path for packets to travel to their destination across multiple networks.

**Working of Network Layer**

* Every device gets a unique address (IP address) to identify it on the network.
* Data is packaged into small packets, with labels showing where it’s coming from and where it’s going.
* Routers figure out the best path to send the packets to their destination.
* Packets travel step by step through different routers until they reach the right device.
* If a packet is too big, it gets broken into smaller pieces to fit through the network.
* At the destination, the pieces are put back together into the original data.
* If something goes wrong, like the destination can’t be reached, an error message is sent back.

**Protocols Used at Network Layer**

* IP (Internet Protocol)
* ICMP (Internet Control Message Protocol)
* ARP (Address Resolution Protocol)
* RARP (Reverse Address Resolution Protocol)
* NAT (Network Address Translation)
* RIP (Routing Information Protocol)
* OSPF (Open Shortest Path First)
* BGP (Border Gateway Protocol)
* IPSec (Internet Protocol Security)
* MPLS (Multiprotocol Label Switching)

**Services Provided by Network Layer Protocols**

* Logical Addressing: Assigns IP addresses to devices, helping identify each device uniquely on a network.
* Routing: Chooses the best path for data to travel from the sender to the receiver across networks.
* Packet Forwarding: Transfers data packets from one network to another using routers.
* Fragmentation and Reassembly: Breaks down large packets into smaller ones (if needed) and reassembles them at the destination.
* Error Handling and Diagnostics: Uses protocols like ICMP to report errors and test network status (e.g., ping).
* Internetworking: Connects different types of networks and ensures data flows smoothly between them.

## Network Layer

The Network Layer is the 5th Layer from the top and the 3rd layer from the Bottom of the OSI Model. It is one of the most important layers which plays a key role in data transmission. The main job of this layer is to maintain the quality of the data and pass and transmit it from its source to its destination. It also handles routing, which means that it chooses the best path to transmit the data from the source to its destination, not just transmitting the packet. There are several important protocols that work in this layer.

**Sub-layers of the Data Link Layer**

* 1. **Logical Link Control (LLC) Sub-layer**

Deals with identifying network layer protocols and error control.

* 1. **Media Access Control (MAC) Sub-layer**

Controls how devices access the medium and get permission to transmit data.

**Functions and Services provided by the Data Link Layer**

* Framing
* Error Detection
* Error Correction
* Flow Control
* Addressing

**Working of Data Link Layer**

* **Framing:** Encapsulates network layer data into frames for transmission.
* **MAC Addressing:** Uses physical (MAC) addresses to identify source and destination on the same network.
* **Error Detection:** Adds checks like CRC to detect transmission errors.
* **Error Correction (optional):** Some protocols correct errors without retransmission.
* **Flow Control:** Prevents sender from overwhelming receiver (e.g., sliding window).
* **Media Access Control:** Manages access to shared media (e.g., CSMA/CD in Ethernet).
* **Acknowledgment & Retransmission:** Ensures delivery through ACKs and frame retransmission if needed.

**Protocols used in Data Link Layer**

* **Ethernet (IEEE 802.3)** – Widely used in wired LANs.
* **Wi-Fi (IEEE 802.11)** – Wireless LAN protocol.
* **PPP (Point-to-Point Protocol)** – Used for direct connections between two nodes (e.g., dial-up).
* **HDLC (High-Level Data Link Control)** – Bit-oriented protocol used in WANs.
* **Frame Relay** – Used for efficient data transmission over WANs.
* **MAC (Media Access Control)** – Sub-layer responsible for physical addressing and access control.

## Physical Layer

The physical Layer is the bottom-most layer in the **Open System Interconnection (OSI) Model,**which is a physical and electrical representation of the system. It consists of various network components such as power plugs, connectors, receivers, cable types, etc. The physical Layer defines the types of encoding (that is how the 0's and 1's are encoded in a signal). It is responsible for the communication of unstructured raw data streams over a physical medium.

**Physical Topologies**

Physical topologies describe the physical arrangement of devices and cables in a network.

**Line Configuration**

* **Point-to-Point configuration: In Point-to-Point configuration, there is a line (link) that is fully dedicated to carrying the data between two devices.**
* **Multi-Point configuration: In a Multi-Point configuration, there is a line (link) through which multiple devices are connected.**

**Modes of Transmission Medium**

* Simplex mode: In this mode, out of two devices, only one device can transmit the data, and the other device can only receive the data.
  + Example- Input from keyboards, monitors, TV broadcasting, Radio broadcasting, etc.
* Half Duplex mode: In this mode, out of two devices, both devices can send and receive the data but only one at a time not simultaneously.
  + Examples- Walkie-Talkie, Railway Track, etc.
* Full-Duplex mode: In this mode, both devices can send and receive the data simultaneously.
  + Examples- Telephone Systems, Chatting applications, etc.

**Functions of Physical Layer**

* **Bit by Bit Transmission**
* **Encoding and Decoding**
* **Signal Transmission**
* **Modulation and Demodulation**
* **Transmission Modes**
* **Data Control**

**Protocols in Physical Layer**

* Ethernet (IEEE 802.3) – Widely used for wired networks.
* Wi-Fi (IEEE 802.11) – For wireless communication.
* Bluetooth (IEEE 802.15.1) – Short-range wireless communication.
* USB (Universal Serial Bus) – For connecting devices over short distances.

**Working of Physical Layer**

* **Bit Transmission:** Transmits raw bits (0s and 1s) over a physical medium (e.g., cables, radio waves).
* **Physical Medium Handling:** Defines the type of media (copper wire, fiber optics, wireless).
* **Signal Encoding:** Converts bits into electrical, optical, or radio signals.
* **Data Rate Control:** Specifies the rate (speed) at which bits are transmitted (e.g., Mbps, Gbps).
* **Synchronization:** Ensures sender and receiver are synchronized at the bit level.
* **Topology Specification:** Defines physical layout (e.g., star, bus, ring).
* **Transmission Mode:** Supports simplex, half-duplex, and full-duplex communication.
* **Interface Standards:** Defines hardware interfaces (e.g., connectors, pin layouts, voltage levels).

**Services Provided by the Physical layer**

* Bit Transmission: Sends raw binary bits (0s and 1s) over the physical medium.
* Medium Selection: Provides the interface to transmission media (e.g., copper, wireless).
* Signal Encoding & Modulation: Converts digital data to signals suitable for the medium.
* Bit Synchronization: Ensures sender and receiver are synchronized for accurate bit interpretation.
* Data Rate Specification: Defines how fast bits are transmitted (bit rate).
* Physical Topology Support: Supports network layout (e.g., star, ring, bus).
* Transmission Mode Support: Enables simplex, half-duplex, or full-duplex communication.
* Hardware Interface Specification: Defines physical and electrical characteristics of devices (e.g., voltages, pin configurations, cable types).

**References**

* GeeksForGeeks
* Webopedia
* Wikipedia