OSI Model – Professional Overview

By Dip Kar

OSI Model – Professional Overview

What is OSI Model?

The OSI (Open Systems Interconnection) Model is a conceptual framework developed by ISO that standardizes how different network systems communicate. It divides the communication process into seven logical layers, each responsible for specific network functions—from physical transmission to application-level interaction. It helps in troubleshooting, protocol design, and ensuring interoperability among diverse devices and technologies.

Flow of Layers:

[Application] ■ [Presentation] ■ [Session] ■ [Transport] ■ [Network] ■ [Data Link] ■ [Physical]

Each layer serves a unique purpose:

n Application: User interaction and services.

n Presentation: Data formatting, encryption, compression.

n Session: Connection setup and management.

n Transport: End-to-end communication via TCP/UDP.

n Network: Logical addressing and routing.

n Data Link: Reliable delivery in LAN (MAC-based).

n Physical: Transmission of raw bits through medium.

This layered approach enhances security, troubleshooting, and protocol efficiency across complex network environments.

OSI Model ■ Quick Definition

By Dip Kar

The OSI (Open Systems Interconnection) Model is a conceptual framework that defines how data is transmitted between devices in a network. It divides the communication process into seven layers, from Physical (hardware level) to Application (user level), ensuring interoperability between different systems and protocols. Purpose: To standardize networking communication, improve troubleshooting, and simplify protocol design.

Application (7)

Presentation (6)

Session (5)

Transport (4)

Network (3)

Data Link (2)

Physical (1)

Layer 7 ■ Application Layer

By Dip Kar

One-line: Interfaces between user applications and network services (where apps talk to the network).

Short Description

Provides network services directly to end-user applications; interface for software.

Data unit

Data

Main protocols (ports)

HTTP (80), HTTPS (443), FTP (20/21), SSH (22), SMTP (25), DNS (53), RDP (3389), MySQL (3306)

Devices / Examples

Web servers, Mail servers, Application servers, Browsers

Security focus

Quick note

Input validation, authentication, secure protocol configuration, proper session handling

Most exposed layer ■ common area for web app vulnerabilities and penetration testing.

Layer 6 ■ Presentation Layer

By Dip Kar

One-line: Prepares data for the application (encryption, compression, formatting).

Short Description

Handles data representation, encryption/decryption and compression for the application layer.

Data unit

Formatted data

Main protocols / tech

TLS/SSL (used with HTTPS on 443), MIME, ASN.1, image/audio codecs

Devices / Examples

SSL/TLS libraries, Codecs, Format converters

Security focus

Quick note

Encryption strength (TLS config), preventing downgrade attacks, data integrity

Ensures data is in a usable and secure format before reaching applications.

Layer 5 ■ Session Layer

By Dip Kar

One-line: Manages and secures dialogues/sessions between applications.

Short Description

Manages sessions (establish, control, terminate) and dialogs between applications.

Data unit

Sessions / Streams

Main protocols

NetBIOS, RPC, TLS session handling, SMB session control

Devices / Examples

Session managers, Middleware, RPC daemons

Security focus

Session hijacking protection, token/session timeout, secure session resumption

Quick note

Important for long-lived connections and maintaining secure dialogues.

Layer 4 ■ Transport Layer

By Dip Kar

One-line: End-to-end communication and port-based service delivery (TCP/UDP).

Short Description

Provides reliable (or unreliable) end-to-end communication, flow control and error handling.

Data unit

Segments (TCP) / Datagrams (UDP)

Main protocols (ports usage)

TCP (reliable) used by HTTP/HTTPS/SSH; UDP (connectionless) used by DNS (53), NTP (123), DHCP (67/68)

Devices / Examples

Gateways, Firewalls, Load balancers

Security focus

Port filtering, TCP attack mitigation (SYN flood), secure session teardown

Quick note

Where ports live ■ mapping services to ports and controlling access.

Layer 3 ■ Network Layer

By Dip Kar

One-line: Logical addressing and routing between networks (IP and routing protocols).

Short Description

Logical addressing and routing of packets between networks; path selection.

Data unit

Packets

Main protocols (with numbers)

IP (IPv4/IPv6), ICMP (1), IGMP (2), OSPF (89), BGP (179), RIP (520), GRE (47), IPsec (ESP 50 / AH 51)

Devices / Examples

Routers, Layer-3 switches; routing tables and controllers

Security focus

Routing security (BGP hardening), anti-spoofing, ACLs, IDS/IPS rules

Quick note

Critical for reachability; attackers exploit routing misconfigurations and spoofing.

Layer 2 ■ Data Link Layer

By Dip Kar

One-line: Node-to-node reliable delivery within a LAN (MAC & frames).

Short Description

Node-to-node delivery on the same physical network; framing and MAC addressing.

Data unit

Frames

Main protocols / tech

Ethernet (802.3), ARP, VLAN, PPP, STP

Devices / Examples

Switches, Bridges, NICs

Security focus

Quick note

MAC filtering, VLAN segregation, ARP spoofing prevention, port security on switches

Handles reliable delivery within a LAN segment; often targeted for lateral movement attacks.

Layer 1 ■ Physical Layer

By Dip Kar

One-line: Physical transmission of raw bits over cables, fiber or radio.

Short Description

Transmission of raw bits over the physical medium (electrical/optical/radio).

Data unit

Bits

Main components

Cables (Ethernet, Fiber), Hubs, Repeaters, Wireless radios, Physical connectors

Devices / Examples

NICs, Transceivers, Patch panels

Security focus

Physical access control, tamper detection, shielding, secure cabling

Quick note

If attackers get physical access, higher-layer controls can be bypassed ■ protect hardware.