1.7 layers of the OSI Model

OSI stands for Open System Interconnection Model. It is used to define and analyse how data is transferred from one computer to another in a computer network. OSI model has very significance where the communication between computers/computer networks with different configurations are required. It was introduced by ISO in 1984. It contains mainly 7 layers which will be explained below.

7. Application Layer

It is commonly used by applications in our PCs that require a network for their functioning. The web browsers in our devices uses the application layer. This is where the user gets involved, the actual software you interact with to do stuff online. Think of your email app, or when you're watching a video on a streaming service. Protocols in this crib are the ones you hear about all the time, like HTTP for websites, SMTP for sending mail, and FTP for file transfers. It's like the front desk of a hotel where you make your requests directly.

6. Presentation Layer

This layer is all about making sure the data you see makes sense to your application. It's the translator and the format fixer. When data arrives, this layer deciphers the code, makes sure the encryption is handled right (like SSL/TLS stuff), and translates the raw bits into something the Application Layer can actually display on your screen. It handles stuff like ensuring a JPEG image file actually looks like a picture and not random noise. In real-world terms, it's like having a universal translator at a U.N. summit—making sure everyone understands the message regardless of the original language.

5. Session Layer

A'ight, so the session layer keeps the communication line open and organized between two computers. It manages the whole "session"—making sure the right data goes to the right place at the right time. It sets up the talk, manages the flow, and shuts it down

when you're done. If a connection drops during a huge file download, this layer can sometimes pick up where it left off. Think of it as a phone call manager; it ensures the line stays open while you're talking and properly hangs up when the convo is over, rather than just yelling across the room.

4. Transport Layer

This is the delivery supervisor. It takes the big message from the upper layers and chops it into smaller, manageable chunks called "segments" so they can travel efficiently. Crucially, it makes sure every single piece arrives where it's supposed to go. It adds error-checking and flow control. The biggest players here are TCP, which guarantees delivery and checks for missing pieces, and UDP, which is faster but doesn't care if you miss a segment (good for streaming video where a lost frame isn't a big deal). It's like a reliable mail service that uses tracking numbers for every single box in your shipment to ensure the whole order arrives complete.

3. Network Layer

We're getting physical now, moving out into the actual network jungle. The network layer's main gig is routing data packets from the source machine across different networks to the destination machine. It figures out the best path to take, kinda like a GPS. This layer is all about IP addresses—your unique network location. The star protocol here is the Internet Protocol (IP). It's basically the postal service for the entire internet, sticking the addresses on the segments (now called packets) and making sure they start moving in the right general direction across cities and countries.

2. Data Link Layer

Okay, now we're talking about moving frames of data over a *single* direct link, like within your house's local network (LAN). This layer manages access to the physical cable and makes sure the transfer is smooth without crashes. It uses MAC addresses—a unique hardware ID burned into your network card—to manage traffic locally. This layer is split

into two sublayers: LLC (Logical Link Control) and MAC (Media Access Control). It's like the traffic cops at one specific intersection, managing who gets to drive on the local road right now to prevent total gridlock.

1. Physical Layer

This is where the rubber meets the road, the actual physical hardware. It's all about the raw bits—the electrical signals, light pulses, or radio waves that physically carry the information. This layer defines the cables, the Wi-Fi signal frequency, the voltage levels, and the actual pins on a network plug. It doesn't care what the data means, it just pushes 0s and 1s across the wire. Protocols here are hardware specs like Ethernet cables (CAT5, CAT6) or USB standards. It is literally the highway itself—the concrete, the lanes, and the speed limit signs that the cars (data) drive on.

2.OSI Mnemonic

Please Do Not Throw Sausage Pizza Away

This mnemonic facilitates the memorization of the layer order by associating the first letter of each word with the first letter of the respective layer name, as detailed in the table below:

Please	1	Physical Layer
Do	2	Data Link Layer
Not	3	Network Layer
Throw	4	Transport Layer
Sausage	5	Session Layer
Pizza	6	Presentation Layer
Away	7	Application Layer

3. OSI vs TCP/IP Model Comparison

The OSI model is a generic, conceptual framework used primarily as an educational and reference tool for understanding network communication, comprised of seven distinct, strictly defined layers. In contrast, the TCP/IP model is a practical, four-layer, protocol-dependent standard that forms the technical foundation of the modern internet and is widely implemented in real-world systems. The primary structural difference lies in their layering: the TCP/IP model combines the Application, Presentation, and Session layers of the OSI model into a single Application layer, and merges the Data Link and Physical layers into a Network Access (or Network Interface) layer. While the OSI model emphasizes clear distinctions between service, interface, and protocol specifications, the TCP/IP model is less rigid, with layers having more flexible, sometimes overlapping, responsibilities. Essentially, the OSI model provides a detailed blueprint for network functions, while the simpler TCP/IP model focuses on the essential protocols (like TCP and IP themselves) necessary for practical internetworking.

Mapping table between OSI and TCP/IP models.

OSI Layer	TCP/IP Layer
Application / Presentation / Session (L7/L6/L5)	Application Layer
Transport (L4)	Transport Layer
Network (L3)	Internet Layer
Data Link / Physical (L2/L1)	Network Access Layer

4. Protocol Data Units (PDUs)

OSI Layer		PDU Name
Layer 4	–	Transport Segment (for TCP) / Datagram (for UDP)
Layer 3	–	Network Packet
Layer 2	–	Data Link Frame
Layer 1	–	Physical Bits (or stream/symbol)

5. Addressing Concepts

MAC Address – used at Layer 2 (Data Link)

A MAC (Media Access Control) address is a **physical, hardware-based address** embedded in every network interface card (NIC). It uniquely identifies a device on a local network.

Relation to OSI:

Used in the **Data Link layer** for **frame addressing**, enabling devices on the same local network (LAN) to communicate.

IP Address – used at Layer 3 (Network)

An IP address is a **logical address** assigned to a device so it can communicate across different networks. It enables routing of packets between source and destination hosts.

Relation to OSI:

Used in the **Network layer** for **packet delivery and routing** over multiple interconnected networks.

Port Number – used at Layer 4 (Transport)

A port number identifies a **specific application or service** running on a device (e.g., HTTP uses port 80, DNS uses port 53). It allows multiplexing of data to the correct process.

Relation to OSI:

Used in the **Transport layer** for **segment identification**, enabling end-to-end communication between processes on different devices (TCP/UDP).