OSI Model

What Is the OSI Model?

The Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network. The OSI model is divided into seven distinct layers, each with specific responsibilities, ranging from physical hardware connections to high-level application interactions.

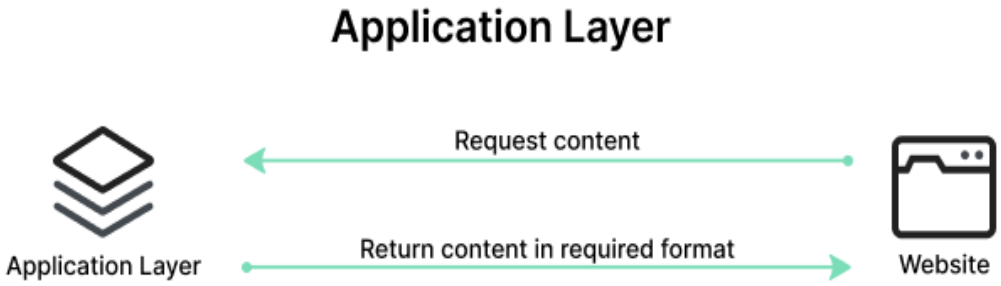
Each layer of the OSI model interacts with the layer directly above and below it, encapsulating and transmitting data in a structured manner. This approach helps network professionals troubleshoot issues, as problems can be isolated to a specific layer. The OSI model serves as a universal language for networking, providing a common ground for different systems to communicate effectively.

The OSI model was the first standard model for network communications, adopted by all major computer and telecommunication companies in the early 1980s. It was introduced in 1983 by representatives of the major computer and telecom companies, and was adopted by ISO as an international standard in 1984.

The modern Internet is not based on OSI, but on the simpler TCP/IP model. However, the OSI 7-layer model is still widely used, as it helps visualize and communicate how networks operate.

The OSI model provides a standardized approach to networking. It helps vendors and developers create interoperable network hardware and software by clearly defining network functions across 7 logical layers. Understanding this model is crucial for diagnosing network issues, designing systems, and working with protocols effectively.

7. Application Layer



The Application Layer serves as the interface between the end-user applications and the underlying network services. This layer provides protocols and services that are directly utilized by end-user applications to communicate across the network. Key functionalities of the Application Layer include resource sharing, remote file access, and network management.

Examples of protocols operating at the Application Layer include Hypertext Transfer Protocol (HTTP) for web browsing, File Transfer Protocol (FTP) for file transfers, Simple Mail Transfer Protocol (SMTP) for email services, and Domain Name System (DNS) for resolving domain names to IP addresses. These protocols ensure that user applications can effectively communicate with each other and with servers over a network.

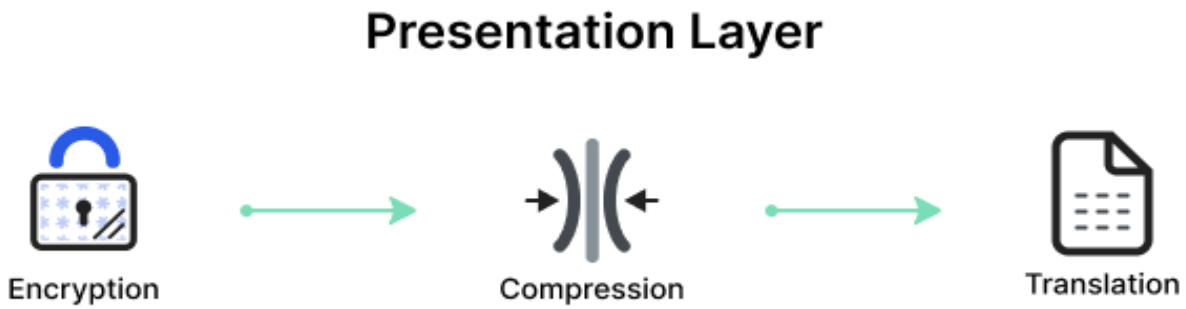
Key Functions:

- Interface for the user.
- Application services such as email, file transfer, and web browsing.
- Protocols: HTTP, FTP, SMTP, DNS, SNMP.

Examples:

- Web browsers
- Email clients
- File transfer programs

6. Presentation Layer



The Presentation Layer, also known as the syntax layer, is responsible for translating data between the application layer and the network format. It ensures that data sent from the application layer of one system is readable by the application layer of another system. This layer handles data formatting, encryption, and compression, facilitating interoperability between different systems.

One of the key roles of the Presentation Layer is data translation and code conversion. It transforms data into a format that the application layer can understand. For example, it may convert data from ASCII to EBCDIC. It also includes encryption protocols to ensure data security during transmission and compression protocols to reduce the amount of data for efficient transmission.

Key Functions:

- Data translation, encryption/decryption, and compression.
- Syntax and semantics of the information.
- Converts between different data formats (e.g., EBCDIC to ASCII).

Examples:

- SSL/TLS (also spans other layers)
- JPEG, MPEG, GIF
- XML, JSON

5. Session Layer

The Session Layer manages and controls the connections between computers. It establishes, maintains, and terminates connections, ensuring that data exchanges occur efficiently and in an organized manner. The layer is responsible for session checkpointing and recovery, which allows sessions to resume after interruptions.

Protocols operating at the Session Layer include Remote Procedure Call (RPC), which enables a program to execute a procedure on a remote host as if it were local, and the session establishment phase in protocols like NetBIOS and SQL. These services enable reliable communication, especially in complex network environments.

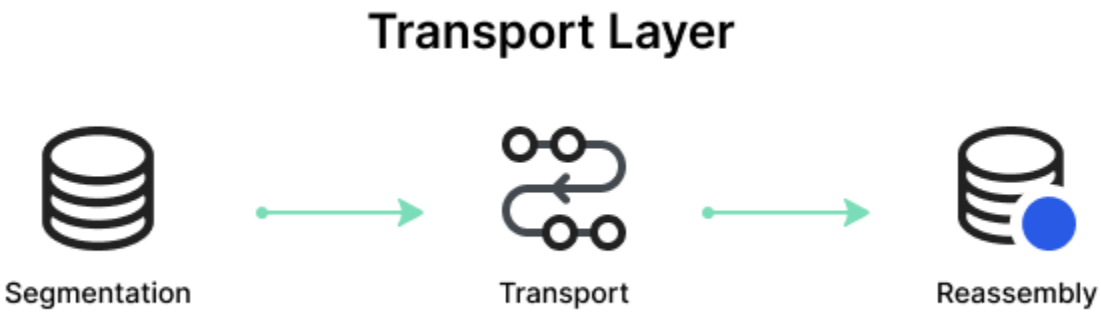
Key Functions:

- Establishment, maintenance, and termination of sessions.
- Synchronization (checkpoints in data streams).
- Dialog control (half/full duplex).

Examples:

- APIs
- NetBIOS
- RPC (Remote Procedure Call)

4. Transport Layer



The Transport Layer provides end-to-end communication services for applications. It ensures complete data transfer, error recovery, and flow control between hosts. This layer segments and reassembles data for efficient transmission and provides reliability with error detection and correction mechanisms.

Protocols at this layer include Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). TCP is connection-oriented and ensures reliable data transfer with error checking and flow control, making it suitable for applications like web browsing and email. UDP is connectionless, offering faster, though less reliable, transmission, suitable for applications like video streaming and online gaming.

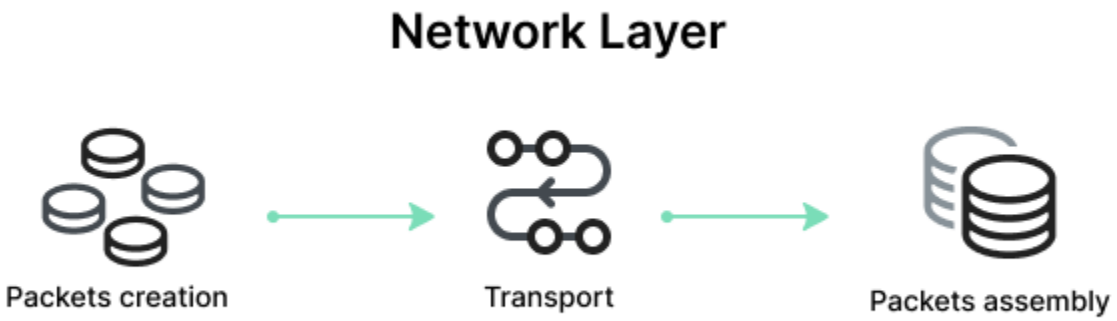
Key Functions:

- Segmentation and reassembly.
- Connection establishment, maintenance, and termination.
- Flow control and error recovery.
- Protocols: TCP (reliable), UDP (unreliable but faster).

Devices:

- Gateways
- Firewalls (some operate at this layer)

3. Network Layer



The Network Layer is responsible for data routing, forwarding, and addressing. It determines the best physical path for data to reach its destination based on network conditions, the priority of service, and other factors. This layer manages logical addressing through IP addresses and handles packet forwarding.

Key protocols at this layer include the Internet Protocol (IP), which is important for routing and addressing, Internet Control Message Protocol (ICMP) for diagnostic and error-reporting purposes, and routing protocols like Routing Information Protocol (RIP) that manage the routing of data across networks.

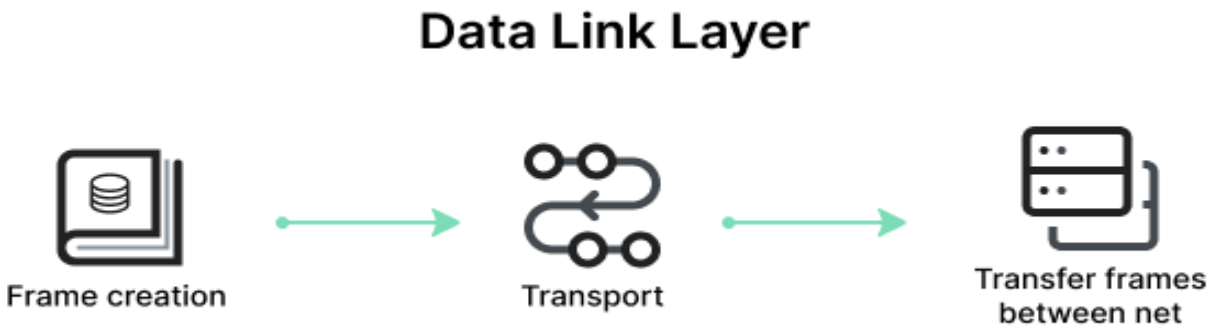
Key Functions:

- Logical addressing (IP addressing).
- Routing (finding the best path).
- Packet forwarding and fragmentation.

Devices:

- Routers
- Layer 3 switches

2. Data Link Layer



The Data Link Layer is responsible for node-to-node data transfer and error detection and correction. It ensures that data is transmitted to the correct device on a local network segment. This layer manages MAC (Media Access Control) addresses and is divided into two sublayers: Logical Link Control (LLC) and Media Access Control (MAC).

Protocols and technologies at this layer include Ethernet, which defines the rules for data transmission over local area networks (LANs), and Point-to-Point Protocol (PPP) for direct connections between two network nodes. It also includes mechanisms for detecting and possibly correcting errors that may occur in the Physical Layer.

Key Functions:

- Framing of data into packets.
- Error detection and correction (e.g., CRC).
- Flow control and access control (MAC – Media Access Control).
- Handling MAC addresses.

Devices:

- Switches
- Bridges
- Network Interface Cards (NICs)

1. **Physical Layer**

The Physical Layer is responsible for the physical connection between devices. It defines the hardware elements involved in the network, including cables, switches, and other physical components. This layer also specifies the electrical, optical, and radio characteristics of the network.

Functions of the Physical Layer include the modulation, bit synchronization, and transmission of raw binary data over the physical medium. Technologies such as Fiber Optics and Wi-Fi operate at this layer, ensuring that the data physically moves from one device to another in the network.

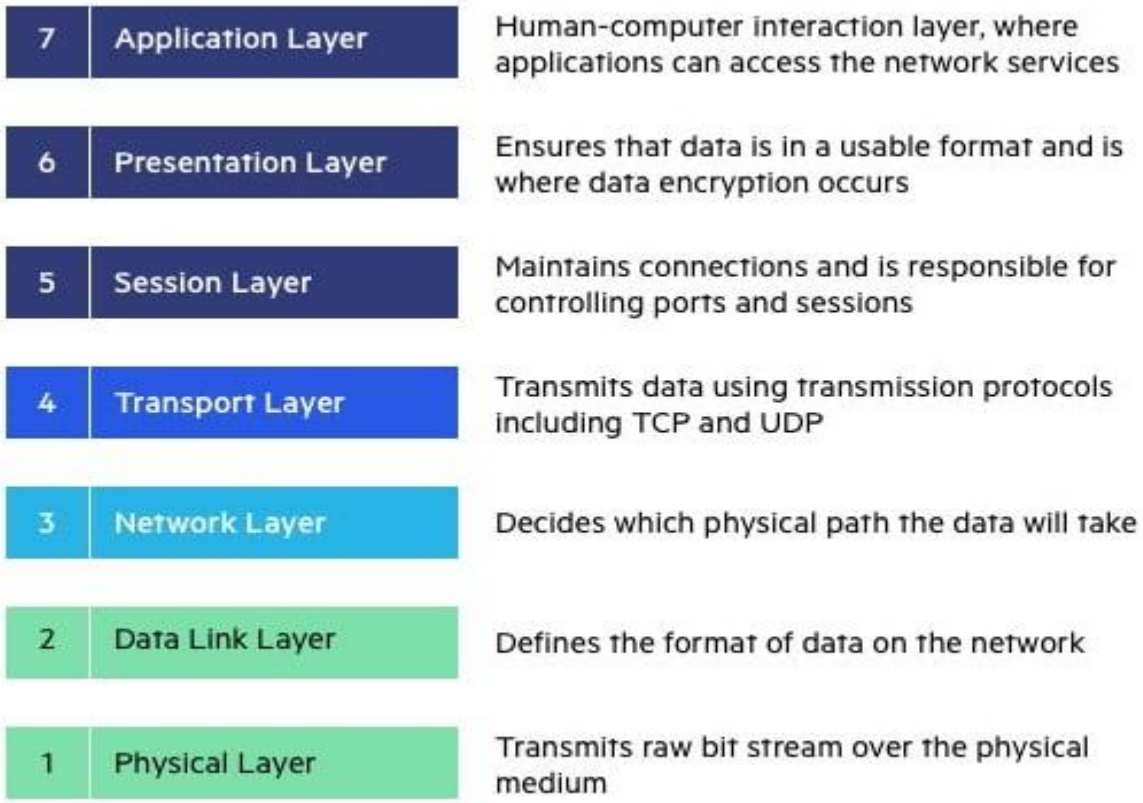
Key Functions:

- Transmission and reception of raw bit streams over a physical medium.
- Specifies electrical/optical signals, bit rates, voltages, cable types.
- Topologies (e.g., mesh, bus) and transmission mode (simplex, half-duplex, full-duplex).

Devices:

- Hubs
- Repeaters
- Cables (Coaxial, Fiber Optic, Twisted Pair)

OSI Model Explained: The OSI 7 Layers



We can understand how data flows through OSI Model with the help of an example mentioned below.

Let us suppose, **Person A** sends an e-mail to his friend **Person B**.

Step 1: Person A interacts with e-mail application like **Gmail**, **outlook**, etc. Writes his email to send. (This happens at **Application Layer**).

Step 2: At Presentation Layer, Mail application prepares for data transmission like encrypting data and formatting it for transmission.

Step 3: At Session Layer, there is a connection established between the sender and receiver on the internet.

Step 4: At Transport Layer, Email data is broken into smaller segments. It adds sequence number and error-checking information to maintain the reliability of the information

Step 5: At Network Layer, addressing of packets is done in order to find the best route for transfer.

Step 6: At Data Link Layer, data packets are encapsulated into frames, then MAC address is added for local devices and then it checks for error using error detection.

Step 7: At Physical Layer, Frames are transmitted in the form of electrical/ optical signals over a physical network medium like ethernet cable or WiFi.

After the email reaches the receiver i.e. **Person B**, the process will reverse and decrypt the e-mail content. At last, the email will be shown on **Person B** email client.

The Importance of the OSI Model

The OSI Model's relevance in networking lies in its ability to serve as a universal reference framework. Here's why it's crucial:

LayeredApproach:
The model breaks down network communication into discrete layers, making it easier to design, develop, troubleshoot, and maintain network protocols and systems.

Standardization:
It offers a standardized way to discuss and understand network communication. This standardization simplifies communication between different vendors and technologies.

Interoperability:
By defining clear boundaries and responsibilities for each layer, the OSI Model promotes interoperability. Devices and software developed independently can communicate effectively if they adhere to the model's specifications.

Troubleshooting:
When network issues arise, the model helps in pinpointing the layer at which the problem exists. This aids network administrators and engineers in diagnosing and resolving issues efficiently.

Layer	Working	Protocol Data Unit	Protocols
1: Physical Layer	Establishing Physical Connections between Devices.	Bits	USB, SONET/SDH, etc.
2: Data Link Layer	Node to Node Delivery of Message.	Frames	Ethernet, PPP, etc.
3: Network Layer	Transmission of data from one host to another, located in different networks.	Packets	IP, ICMP, IGMP, OSPF, etc.

Layer	Working	Protocol Data Unit	Protocols
4: Transport Layer	Take Service from Network Layer and provide it to the Application Layer.	Segments (for TCP) or Datagrams (for UDP)	TCP, UDP, SCTP, etc.
5: Session Layer	Establishes Connection, Maintenance, Ensures Authentication and Ensures security.	Data	NetBIOS, RPC, PPTP, etc.
6: Presentation Layer	Data from the application layer is extracted and manipulated in the required format for transmission.	Data	TLS/SSL, MIME, etc.
7: Application Layer	Helps in identifying the client and synchronizing communication.	Data	FTP, SMTP, DNS, DHCP, etc.