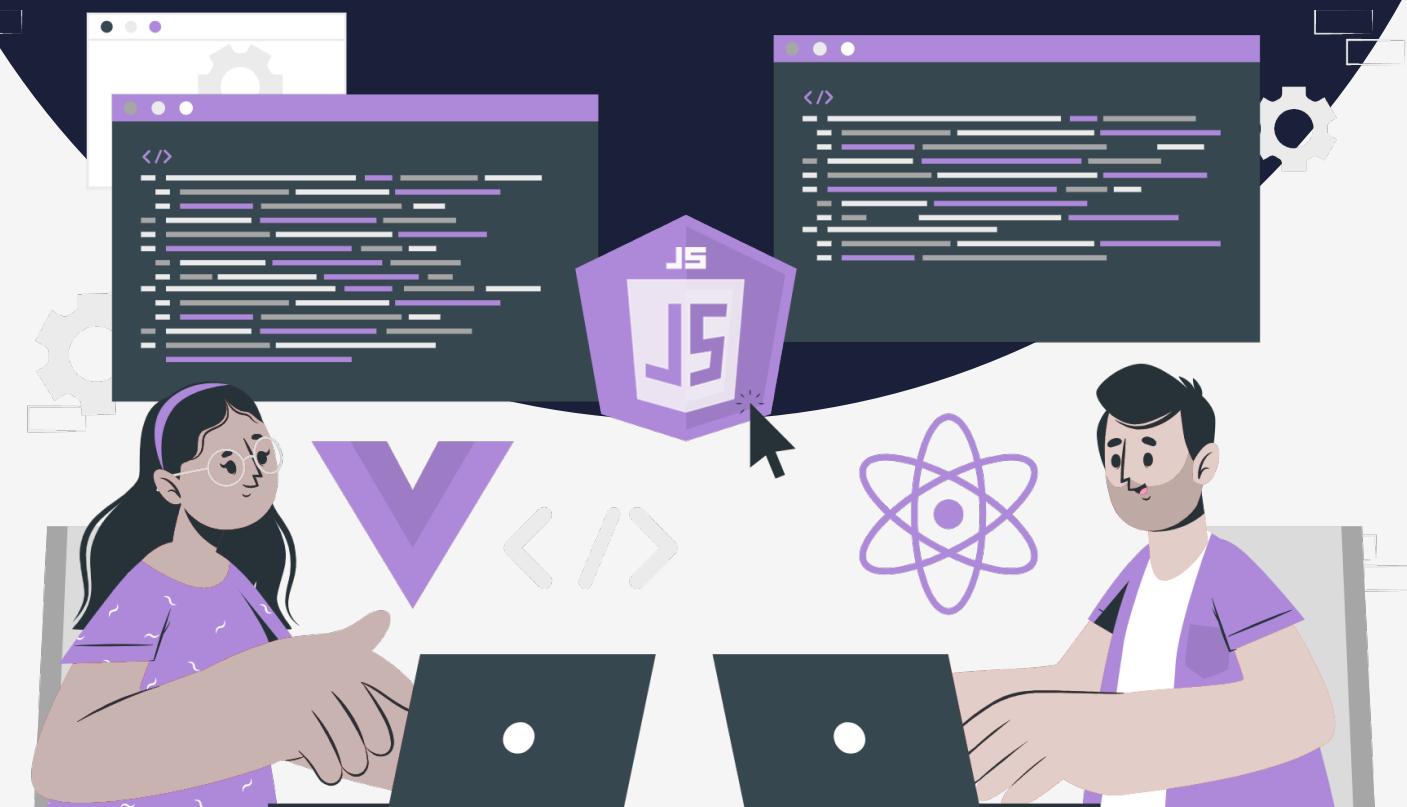


# Lesson:

## OSI Model



# Topics Covered

1. Introduction.
2. OSI Model.
3. Layers of OSI Model.
4. Basic Principle of dividing layers in the OSI Model.
5. Understanding layers of OSI Model.
6. Advantages of OSI Model.
7. Disadvantages of OSI Model.

The OSI (Open Systems Interconnection) model is a conceptual framework that defines how different communication systems should communicate with each other. It is divided into seven layers, each of which performs a specific function and communicates with the layers above and below it. The OSI model provides a standardized way for different computer systems to communicate with each other, regardless of their underlying technology or protocols.

Web developers need to understand the OSI model because it provides a framework for understanding how web applications communicate with each other over networks. Web applications rely on a wide range of network protocols, such as HTTP, TCP, and IP, which operate at different layers of the OSI model. By understanding how these protocols interact with each other and with the underlying hardware and software systems, web developers can design more efficient and secure applications that work seamlessly with other systems. Additionally, the OSI model provides a common language and terminology that developers can use to communicate with other stakeholders in the development process, such as network administrators and software engineers.

## **OSI Model.**

The Open Systems Interconnection (OSI) Model is an International Standard Organisation (ISO) standard that covers all aspects of network communication. It is a reference model developed in 1984 by the International Organization for Standardization that specifies how information from one computer's software application passes through physical media to another computer's software application.

The OSI model is a conceptual framework consisting of seven layers, each with a specific function that governs how computer systems communicate with each other over networks. By providing a standardized approach to network design, the OSI model enables interoperability between different types of computer systems, regardless of their underlying architecture and protocols. This ensures that data can be transmitted reliably and efficiently across a wide range of networks and systems, from local area networks (LANs) to the internet.

## **Layers of OSI Model.**

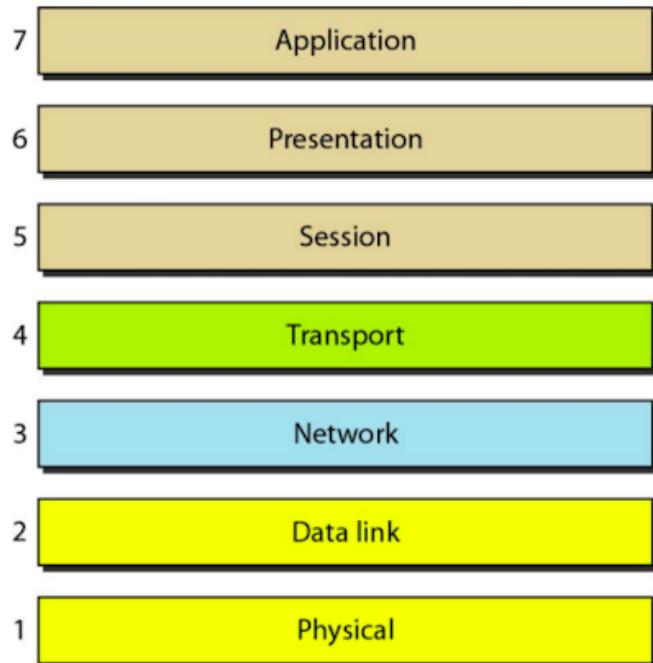
The OSI model can be compared to a bookshelf with seven different shelves. Each shelf represents a different layer of the OSI model, with the bottom shelf being the Physical layer and the top shelf being the Application layer. Each shelf has a specific purpose, just like each layer of the OSI model has a specific function.

For example, the bottom shelf of the bookshelf (Physical layer) is responsible for holding heavy items like large textbooks, just as the Physical layer of the OSI model is responsible for transmitting signals over the physical media like cables, wires, and radio waves. Similarly, the middle shelves (Data Link, Network, and Transport layers) are responsible for organizing and moving the books around the bookshelf, just like these layers of the OSI model are responsible for organizing and moving data packets around the network.

The top shelves of the bookshelf (Session, Presentation, and Application layers) hold books that are easy to access and read, just like the top layers of the OSI model are responsible for making data accessible and readable to the end-users. Overall, just like a bookshelf with different shelves helps in organizing books, the OSI model with seven different layers helps in organizing network communication and making it more efficient and secure.

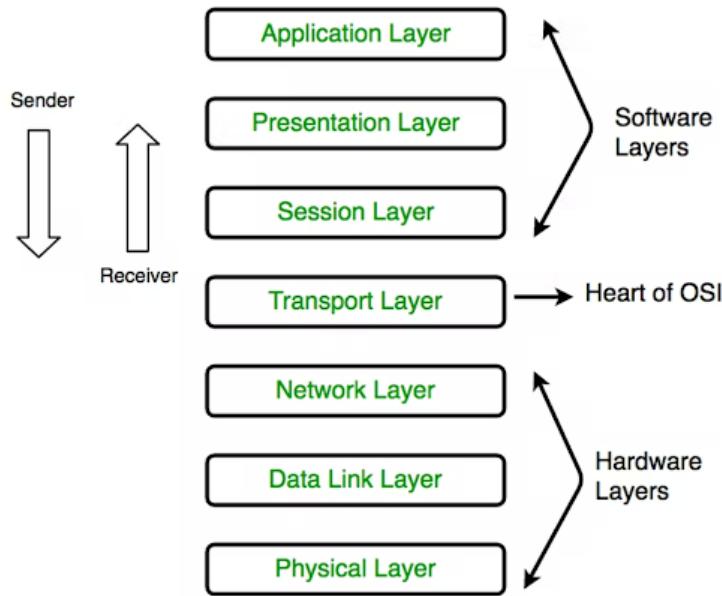
The OSI model consists of 7 separate but related layers, each of which defines a part of the process of moving information across a network.

### **Layers in the OSI Model**



1. Physical layer
2. Data Link layer
3. Network layer
4. Transport layer
5. Session layer
6. Presentation layer
7. Application layer

These seven layers are again broadly categorized into two groups: hardware layers and software layers.



The top three layers of the OSI model are commonly referred to as the software layer, while the bottom three layers are typically referred to as the hardware layer. Among these layers, the transport layer is considered to be the crucial component of the OSI model. Data is transmitted from the sender's end through the physical layer and is then passed up to the application layer. Conversely, at the receiver's end, data is received from the application layer and then sent down through the physical layer.

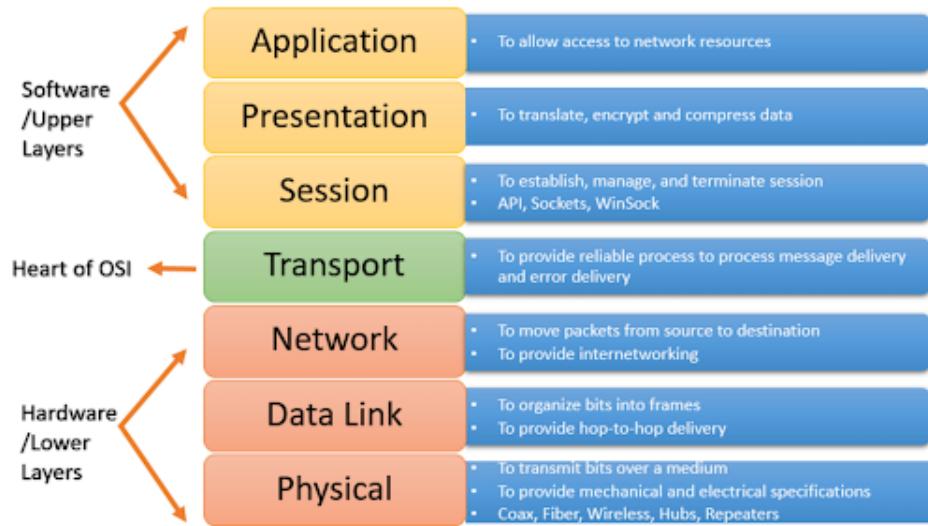
### **Basic Principle of dividing layers in the OSI Model.**

The OSI model is designed to break down the complex process of network communication into smaller, more manageable parts, which are organized into seven distinct layers.

Each layer of the OSI model is responsible for a specific aspect of network communication, such as data transmission, addressing, error correction, and flow control. By dividing the process of network communication into these distinct layers, the OSI model enables hardware and software manufacturers to develop products that adhere to a standardized approach to network communication.

The layering approach of the OSI model also allows network engineers to isolate and troubleshoot network problems more easily. By dividing the network communication process into smaller parts, they can focus on specific layers when diagnosing issues, instead of having to examine the entire network infrastructure.

The layers defined in the OSI model provide a standardized framework for network communication, which enables devices and applications from different vendors to communicate with each other seamlessly, while also providing a structured approach to network troubleshooting and maintenance.



Understanding layers of OSI Model.

### 1. Physical Layer.

The physical layer, positioned at the bottom of the OSI model, facilitates the transmission of raw and unstructured data over the physical medium. Its primary function is to establish and manage the physical connection between devices, which includes activation, maintenance, and deactivation. The physical layer utilizes various protocols and standards to ensure that data is transmitted at the appropriate speed and sequence. It is also responsible for detecting and correcting errors that may occur during transmission through different mechanisms.

The physical layer of a communication system is responsible for transmitting raw bit streams over a communication channel. This layer transforms the data bits into signals that can be transmitted over a physical medium, such as copper wires, optical fibers, or wireless channels.

The physical layer also sets the voltage levels, light speeds, or other physical characteristics of the signals for transmission. The data rate, or the number of bits transmitted per second, is also determined by the physical layer.

The main features of the physical layer are:

- Convert raw data into signals that can be transmitted over a physical medium.
- Transmit the signals over the medium.
- Amplify the signals to ensure they reach their destination.
- Control the speed of data transmission.

There are several protocols and devices used in the physical layer of a communication system. Here are a few examples:

#### Protocols:

- Ethernet: A widely used protocol for wired local area networks (LANs).
- Wi-Fi: A wireless networking protocol used for local and wide area networks.
- Bluetooth: A wireless protocol used for short-range communication between devices.

**Devices:**

- Transmitter: A device that converts electrical signals into optical or radio waves for transmission over the physical medium.
- Receiver: A device that converts optical or radio waves back into electrical signals for processing by the higher layers of the protocol stack.
- Modem: A device that converts digital signals from a computer into analog signals for transmission over telephone lines.

**2. Data Link Layer.**

The data link layer is responsible for providing error-free communication between two nodes on the same network. It achieves this by breaking the data into frames and adding header and trailer information to each frame. This information includes source and destination addresses, as well as error detection and correction codes to ensure the integrity of the data.

In addition to error detection and correction, the data link layer also provides flow control mechanisms to prevent a fast sender from overwhelming a slower receiver. The data link layer also performs channel access control, determining which node has the right to transmit data over the shared communication channel.

Functions of data link layer:

- Framing: The data link layer breaks the data received from the network layer into smaller units called frames. These frames include header and trailer information, which helps in identifying the start and end of each frame.
- Physical addressing: The data link layer adds physical addresses to each frame so that it can be delivered to the correct destination.
- Error control: The data link layer includes error detection and correction mechanisms in the frames to ensure that the data is transmitted without errors.
- Flow control: The data link layer provides flow control mechanisms to manage the flow of data between nodes on the network. This helps to prevent a fast sender from overwhelming a slower receiver.

There are several protocols and devices used in the data link layer of a communication system. Here are a few of them:

- Point-to-Point Protocol (PPP): A protocol used for establishing a direct connection between two nodes over a serial link.

Devices:

- Network Interface Card (NIC): A hardware component that connects a computer to a network and provides the physical and data link layer functionality needed for communication over the network.
- Switch: A networking device that operates at the data link layer and is used to forward data between nodes on a network.
- Bridge: A device that connects two separate network segments and operates at the data link layer to manage the flow of data between the segments.

**3. Network Layer.**

The network layer is responsible for providing communication between hosts on different networks. It achieves this by dividing the data received from the transport layer into packets and adding routing information to each packet. This routing information is used to direct packets to their destination across different networks.

The network layer also provides two modes of communication: connection-oriented and connectionless. In connection-oriented communication, a virtual circuit is established between the sender and receiver before data transmission begins. This provides a reliable and ordered delivery of packets. In connectionless communication, each packet is sent independently and may take different paths to reach its destination. This provides a more flexible and efficient mode of communication.

The functions of the network layer are:

- Logical addressing: The network layer provides logical addressing to identify devices on different networks. This logical address is typically an IP address, which is used to route packets to their destination.
- Routing: The network layer uses routing algorithms and protocols to determine the best path for a packet to travel from the source to the destination. This involves selecting the next hop or router that the packet should be sent to on its journey.
- Packet fragmentation and reassembly: The network layer is responsible for breaking large packets into smaller units, called fragments, to facilitate transmission across different networks. The network layer at the receiving end reassembles these fragments into their original packets.
- Error handling: The network layer handles errors in packet delivery by using mechanisms such as error detection and retransmission.

#### **Protocols:**

- Internet Protocol (IP): The primary network layer protocol used for routing packets across the internet and other networks.
- Internet Control Message Protocol (ICMP): A protocol used for error reporting and diagnostic purposes on IP networks.
- Address Resolution Protocol (ARP): A protocol used to map an IP address to a physical address (such as a MAC address) on a local network.

#### **Devices:**

- Router: A networking device that operates at the network layer and is used to forward packets between different networks.

### **4. Transport Layer.**

The transport layer is the fourth layer of the OSI model which is responsible for the process to process delivery of data. The main aim of the transport layer is to maintain order so that the data must be received in the same sequence as it was sent by the sender. The transport layer provides two types of services namely – connection-oriented and connectionless.

The functions and services of the transport layer are:

- Segmentation and reassembly: The transport layer divides data received from the application layer into smaller units called segments, and adds a header with sequence numbers, to ensure that data is delivered in the correct order. At the receiving end, the transport layer reassembles the segments back into their original data.
- Flow control: The transport layer is responsible for controlling the flow of data between the sender and receiver, preventing the receiver from being overwhelmed with too much data too quickly.
- Error control: The transport layer provides mechanisms to detect and correct errors that may occur during data transmission.
- Multiplexing/demultiplexing: The transport layer allows multiple applications to share the same network connection, by providing a way to identify which data belongs to which application. This is done through port numbers

- Connection-oriented and connectionless services: The transport layer provides two types of services: connection-oriented, where a virtual circuit is established between the sender and receiver before data transmission begins, and connectionless, where each segment is sent independently and may take different paths to reach its destination.

Some common protocols and devices associated with the transport layer:

Protocols:

- Transmission Control Protocol (TCP): A connection-oriented protocol that provides reliable, ordered delivery of data, flow control, and error control.
- User Datagram Protocol (UDP): A connectionless protocol that provides fast, but unreliable delivery of data.

Devices:

- Load balancers: Devices that distribute network traffic between multiple servers, operating at the transport layer to balance the load between different connections.

## 5. Session Layer

The session layer is the fifth layer of the OSI model, responsible for establishing, managing, and terminating sessions between applications running on different hosts. A session is a logical connection between two applications, and the session layer ensures that this connection is maintained throughout the duration of the session.

The functions of session layer are:

- Session establishment: The session layer is responsible for establishing, maintaining, and terminating sessions between applications. It provides mechanisms for initiating sessions, authenticating users, and exchanging session parameters.
- Session management: Once a session has been established, the session layer manages the session by coordinating the exchange of data between applications. It provides mechanisms for controlling the flow of data, synchronizing data transfer, and ensuring that data is sent and received in the correct order.
- Session security: The session layer provides mechanisms for securing sessions, such as by encrypting data, authenticating users, and controlling access to shared resources.
- Session recovery: The session layer provides mechanisms for recovering from errors and interruptions in a session. It can save the current state of a session, allowing it to be resumed later if the session is interrupted.

The session layer is primarily concerned with managing sessions between applications, rather than with specific devices or protocols. However, some common examples of devices and protocols that operate at the session layer include:

- Remote Procedure Call (RPC): RPC is a protocol that allows a client application to call a procedure on a remote server as if it were a local procedure. The session layer provides mechanisms for establishing and managing these remote procedure calls.
- Telnet: Telnet is a protocol that allows a user to connect to a remote computer and interact with it as if it were a local computer. The session layer provides mechanisms for establishing and managing these remote terminal sessions.

## 6. Presentation Layer

The Presentation Layer is the sixth layer of the OSI model and is responsible for ensuring that data is presented in a format that can be understood by the receiving application. The main function of the Presentation Layer is to provide a standard representation of data that can be exchanged between different systems. This includes functions such as data compression, encryption, and data conversion.

The Presentation Layer takes data from the Application Layer and transforms it into a format that can be sent across the network. This may involve converting data into a common format that can be understood by both the sending and receiving systems, such as converting character data from one encoding to another. The Presentation Layer can also be used to compress data to reduce the amount of data that needs to be transmitted over the network, or to encrypt data to provide security for sensitive information.

The functions of the presentation layer:

- Data representation: The Presentation Layer is responsible for converting data from one format to another so that it can be understood by the receiving application. This includes functions such as character encoding, data compression, and data encryption.
- Syntax recognition: The Presentation Layer is responsible for identifying the syntax of the data being transmitted so that it can be interpreted correctly by the receiving application.
- Encryption and decryption: The Presentation Layer provides encryption and decryption services to protect sensitive data as it is transmitted over the network.
- Compression and decompression: The Presentation Layer can compress data to reduce the amount of data that needs to be transmitted over the network, and then decompress the data at the receiving end.
- Translation: The Presentation Layer can translate data from one language or character set to another so that it can be understood by the receiving application.

Some of the protocols and devices used in the Presentation Layer include:

- AFP (Apple Filing Protocol): AFP is a protocol used by Apple computers to share files and resources over a network. It is used to transfer files, directories, and metadata between computers running on Apple's Macintosh operating system.
- ICA (Independent Computing Architecture): ICA is a protocol used by Citrix to deliver remote desktop services to clients. It is used to transfer screen updates, keyboard and mouse inputs, and audio and video data between the server and the client.
- Citrix System Core Protocol: The Citrix System Core Protocol (CSCP) is a protocol used by Citrix to manage user sessions and application delivery. It is used to transfer information about user sessions, applications, and policies between servers and clients.

## 7. Application Layer.

The Application Layer is the topmost layer in the OSI model and is responsible for providing services to end users. The Application Layer interacts with software applications running on a system and enables users to access network resources. It provides protocols and services that allow applications to exchange data over the network, regardless of the underlying hardware and software.

The main function of the Application Layer is to provide a means for applications to communicate with each other and exchange data in a way that is transparent to the end users. This layer includes protocols for email, file transfer, remote login, and many other applications that users interact with on a daily basis.

The Application Layer includes a wide range of protocols and devices that enable applications to communicate over the network.

- HTTP (Hypertext Transfer Protocol): This is a protocol used for web browsing and enables clients to request web pages from servers.
- SMTP (Simple Mail Transfer Protocol): This protocol is used for sending and receiving email messages over the network.
- FTP (File Transfer Protocol): This protocol is used for transferring files between systems over the network.
- DNS (Domain Name System): This is a protocol used for converting domain names into IP addresses.

### **Advantages of OSI Model.**

- The OSI model establishes a standard framework for network communication, allowing different vendors to create network devices and software that can communicate with each other.
- The seven-layer design of the OSI model allows for easier troubleshooting and problem diagnosis by providing a clear separation of network functions and responsibilities.
- By breaking down complex networks into smaller, more manageable components, the layered approach of the OSI model simplifies network design and maintenance.
- The interoperability between different network devices and software is enhanced by the OSI model, which allows for seamless communication between different networks and applications.
- Each layer in the OSI model has a specific function, which reduces complexity and allows for the development of specialized network equipment and software.
- The flexibility of the OSI model allows for the development of new protocols and technologies to meet the changing needs of network communication.

### **Disadvantages of OSI Model.**

While the OSI model has several advantages, it also has some disadvantages, including:

- Complex: The OSI model is complex and can be difficult to understand for beginners, which can make it challenging to implement and troubleshoot.
- Expensive: Implementing the OSI model requires significant investment in specialized hardware and software, which can be expensive for organizations with limited budgets.
- Inefficient: The OSI model involves a lot of overhead due to its layered approach, which can slow down network communication and make it less efficient.
- Limited applicability: The OSI model was designed for use in traditional wired networks and may not be suitable for newer technologies such as wireless networks or the Internet of Things.
- Lack of adoption: Despite its advantages, the OSI model has not been widely adopted in the industry, with many organizations using simpler models such as the TCP/IP model.