Session Layer in OSI model

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.

- The Session Layer is responsible for establishing active communication sessions between two devices.
- In the OSI model, the transport layer is not responsible for releasing a connection. Instead, the session layer is responsible for that. However, in modern TCP/IP networks, TCP already provides orderly closing of connections at the transport layer.
- Dialogue Control is also implemented in the Session Layer of the OSI model but in TCP/IP the dialogue control is implemented in the Application Layer.
- Session-layer services are commonly used in application environments that use remote procedure calls (RPCs).
- Zone Information Protocol in AppleTalk is an example of Session Layer Implementation.
- Session Layer has synchronization and resynchronization techniques that ensure reliable and orderly communication over networks, which is particularly important in applications requiring high levels of data integrity and continuity.
- Synchronization points are markers or tokens inserted into the data stream that allow communication sessions to have checkpoints and on the other hand Resynchronization involves restoring a session to a known state after a disruption, such as a network failure or session timeout.

In Session Layer, data streams are received and further marked, which is then resynchronized properly, so that the ends of the messages are not cut initially and further data loss is avoided. This layer establishes a connection between the session entities. This layer handles and manipulates data that it receives from the Session Layer as well as from the Presentation Layer.

Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Layer
Physical Layer

Working of Session Layer

- The Session Layer as the fifth layer in the OSI model, is integral to managing communication sessions between two applications across a network. It begins by establishing connections, where it negotiates session parameters such as authentication and whether the session will be full-

duplex or half-duplex. Once established, it oversees the orderly exchange of data, employing mechanisms like tokens to manage transmission rights and prevent data collision. To ensure robust communication, the Session Layer implements synchronization techniques, inserting checkpoints in the data stream to allow recovery from the last synchronized state in case of disruptions, rather than restarting the entire transmission.

- Dialogue control contributes to the robustness and reliability of the communication by managing these modes effectively. It helps in creating a structured communication environment where data packets are sent and received orderly and efficiently, reducing the risk of message loss, duplication, or errors due to overlap in communication.
- Towards the end of the communication, this layer is responsible for gracefully terminating the session, ensuring all data has been successfully exchanged and both sides agree to close the session. Furthermore, it handles error recovery, enabling the session to revert to a pre-error state, ensuring continuity and integrity of the communication process. This comprehensive management makes the Session Layer crucial in maintaining efficient, reliable network interactions.

Functions of Session Layer

The session layer being the fifth layer in the OSI model performs several different as well as important functions that are needed for establishing as well as maintaining a safe and secure connection.

Data from Presentation Layer <=> Session Layer <=> Data from Transport Layer

Following are some of the functions which are performed by Session Layer:

- Session Layer works as a dialog controller through which it allows systems to communicate in either half-duplex mode or full duplex mode of communication.
- This layer is also responsible for token management, through which it prevents two users to simultaneously access or attempting the same critical operation.
- This layer allows synchronization by allowing the process of adding checkpoints, which are considered as synchronization points to the streams of data.
- This layer is also responsible for session checkpointing and recovery.
- This layer basically provides a mechanism of opening, closing and managing a session between the end-user application processes.
- The services offered by Session Layer are generally implemented in application environments using remote procedure calls (RPCs).
- The Session Layer is also responsible for synchronizing information from different sources.
- This layer also controls single or multiple connections for each-end user application and directly communicates with both Presentation and transport layers.
- Session Layer creates procedures for checkpointing followed by adjournment, restart and termination.

- Session Layer uses checkpoints to enable communication sessions which are to be resumed from that particular checkpoint at which communication failure has occurred.
- The session Layer is responsible for fetching or receiving data information from its previous layer (transport layer) and further sends data to the layer after it (presentation layer).

Session Layer Protocols

Session Layer uses some protocols which are required for safe, secure and accurate communication which exists between two-ender user applications. Following are some of the protocols provided or used by the Session Layer:

- **AppleTalk Data Stream Protocol (ADSP):** ADSP is that type of protocol which was developed by Apple Inc. and it includes a number of features that allow local area networks to be connected with no prior setup. This protocol was released in 1985. This protocol rigorously followed the OSI model of protocol layering. ADSP itself has two protocols named: AppleTalk Address Resolution Protocol (AARP) and Name Binding Protocol (NBP), both aimed at making system self-configuring.
- **Real-time Transport Control Protocol (RTCP):** RTCP is a protocol which provides out-of-band statistics and control information for an RTP (Real-time Transport Protocol) session. RTCP's primary function is to provide feedback on the quality of service (QoS) in media distribution by periodically sending statistical information such as transmitted octet and packet counts or packet loss to the participants in the streaming multimedia session.
- **Point-to-Point Tunneling Protocol (PPTP):** PPTP is a protocol which provides a method for implementing virtual private networks. PPTP uses a TCP control channel and a Generic Routing Encapsulation tunnel to encapsulate PPP (Point-to-Point Protocol) packets This protocol provides security levels and remote access levels comparable with typical VPN (Virtual Private Network) products.
- **Password Authentication Protocol (PAP):** It is a password-based authentication protocol used by Point to Point Protocol (PPP) to validate users. Almost all network operating systems, remote servers support PAP. PAP authentication is done at the time of the initial link establishment and verifies the identity of the client using a two-way handshake (Client-sends data and server in return sends Authentication-ACK (Acknowledgement) after the data sent by client is verified completely).
- **Remote Procedure Call Protocol (RPCP):** It is a protocol that is used when a computer program causes a procedure (or a sub-routine) to execute in a different address space without the programmer explicitly coding the details for the remote interaction. This is basically the form of client-server interaction, typically implemented via a request-response message-passing system.
- **Sockets Direct Protocol (SDP):** It is a protocol that supports streams of sockets over Remote Direct Memory Access (RDMA) network fabrics. The purpose of SDP is to provide an RDMA-accelerated alternative to the TCP protocol. The primary goal is to perform one particular thing in such a manner which is transparent to the application.

Conclusion

The Session Layer in the OSI model is essential for managing communication sessions between applications on different devices. It establishes, maintains, and terminates these sessions, ensuring stable and efficient communication. This layer enables two-way data exchanges, either one at a time or simultaneously, and helps in recovering from interruptions by using checkpoints. Thus, it ensures that applications can interact smoothly over a network, making it vital for reliable data transmission and coordinated operations in network-based services.