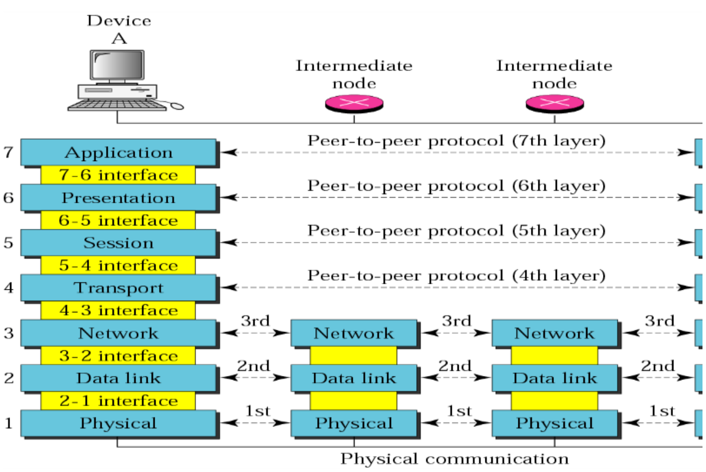
International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 01 | January - 2023 Impact Factor: 7.185 ISSN: 2582-3930

OSI Model

Parth Savla, Harsh Panchal and Tejas Panchal
Student, K.J. Somaiya Polytechnic, Vidhyavihar

- Introduction :

The Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network. It was the first standard model for network communications, adopted by all major computer and telecommunication companies in the early 1980s. 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, and helps isolate and troubleshoot networking problems. OSI was introduced in 1983 by representatives of the major computer and telecom companies, and was adopted by ISO as an international standard in 1984.



In the early- and mid-1970s, networking was largely either government-sponsored (NPL network in the UK, ARPANET in the US, CYCLADES in France) or vendor-developed with proprietary standards, such as IBM's System Network Architecture and Digital Equipment Corporation's DECnet. Public data networks were only just beginning to emerge, and these began to use the X.25 standard in the late 1970s.

The Experimental Packet Switched System in the UK circa 1973–1975 identified the need for defining higher level protocols. The UK National Computing Centre publication 'Why Distributed Computing' which came from considerable research into future configurations for computer systems, resulted in the UK presenting the case for an international standards committee to cover this area at the ISO meeting in Sydney in March 1977.

Beginning in 1977, the ISO initiated a program to develop general standards and methods of networking. A similar process evolved at the International Telegraph and Telephone Consultative Committee (CCITT, from French: Comité Consultatif International Téléphonique et Télégraphique). Both bodies developed documents that defined similar networking models. The British Department of Trade and Industry acted as the secretariat and universities in the United Kingdom developed prototypes of the standards.

The OSI model was first defined in raw form in Washington, DC, in February 1978 by Hubert Zimmermann of France and the refined but still draft standard was published by the ISO in 1980.

- Layer Architecture of OSI model:

Layer 1: Physical layer

Physical Layer defines electrical and physical specifications for devices. The physical layer defines the relationship between a device and a transmission medium, such as a copper or optical cable. This includes the layout of pins, voltages, cable specifications, hubs, repeaters, network adapters, host bus adapters (HBA used in storage area networks) and more.

The major functions and services performed by the physical layer are:

1) Establishment and termination of a connection to a communications medium.

2) Participation in the process whereby the communication resources are effectively shared among multiple users (for example, contention resolution and flow control).

3) Modulation, or conversion between the representation of digital data in user equipment and the corresponding signals transmitted over a communications channel; these are signals operating over the physical cabling (such as copper and optical fiber) or over a radio link.

Layer 2: Data link layer

The data link layer provides node-to-node data transfer a link between two directly connected nodes. It detects and possibly corrects errors that may occur in the physical layer. It defines the protocol to establish and terminate a connection between two physically connected devices. It also defines the protocol for flow control between them.

IEEE 802 divides the data link layer into two sublayers:

- Medium access control (MAC) layer – responsible for controlling how devices in a network gain access to a medium and permission to transmit data.
- Logical link control (LLC) layer – responsible for identifying and encapsulating network layer protocols, and controls error checking and frame synchronization.

The MAC and LLC layers of IEEE 802 networks such as 802.3 Ethernet, 802.11 Wi-Fi, and 802.15.4 Zigbee operate at the data link layer.

The Point-to-Point Protocol (PPP) is a data link layer protocol that can operate over several different physical layers, such as synchronous and asynchronous serial lines.

The functions of the Data Link layer are :

1. Framing: Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
2. Physical addressing: After creating frames, the Data link layer adds physical addresses (MAC address) of the sender and/or receiver in the header of each frame.
3. Error control: Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
4. Flow Control: The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates the amount of data that can be sent before receiving acknowledgement.
5. Access control: When a single communication channel is shared by multiple devices, the MAC sub-layer of the data link layer helps to determine which device has control over the channel at a given time.

Layer 3: Network layer

The network layer provides the functional and procedural means of transferring packets from one node to another connected in "different networks".

If the message is too large to be transmitted from one node to another on the data link layer between those nodes, the network may implement message delivery by splitting the message into several fragments at one node, sending the fragments independently, and reassembling the fragments at another node. It may, but does not need to, report delivery errors.

The functions of network layer are :

1. Routing: The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.
2. Logical Addressing: In order to identify each device on internetwork uniquely, the network layer defines an addressing scheme. The sender & receiver's IP addresses are placed in the header by the network layer. Such an address distinguishes each device uniquely and universally.

Layer 4: Transport layer

The transport layer provides the functional and procedural means of transferring variable-length data sequences from a source host to a destination host from one application to another across a network, while maintaining the quality-of-service functions. Transport protocols may be connection-oriented or connectionless.

This may require breaking large protocol data units or long data streams into smaller chunks called "segments", since the network layer imposes a maximum packet size called the maximum transmission unit (MTU), which depends on the maximum packet size imposed by all data link layers on the network path between the two hosts. The amount of data in a data segment must be small enough to allow for a network-layer header and a transport-layer header. For example, for data being transferred across Ethernet, the MTU is 1500 bytes, the minimum size of a TCP header is 20 bytes, and the minimum size of an IPv4 header is 20 bytes, so the maximum segment size is 1500-(20+20) bytes, or 1460 bytes. The process of dividing data into segments is called segmentation; it is an optional function of the transport layer. Some connection-oriented transport protocols, such as TCP and the OSI connection-oriented transport protocol (COTP), perform segmentation and reassembly of segments on the receiving side; connectionless transport protocols, such as UDP and the OSI connectionless transport protocol (CLTP), usually do not.

The OSI connection-oriented transport protocol defines five classes of connection-mode transport protocols ranging from class 0 (which is also known as TP0 and provides the fewest features) to class 4 (TP4, designed for less reliable networks, similar to the Internet). Class 0 contains no error recovery and was designed for use on network layers that provide error-free connections. Class 4 is closest to TCP, although TCP contains functions, such as the graceful close, which OSI assigns to the session layer. Also, all OSI TP connection-mode protocol classes provide expedited data and preservation of record boundaries. Detailed characteristics of TP0-4 classes are shown in the following table.

The functions of the transport layer are as follows:

1. Segmentation and Reassembly: This layer accepts the message from the (session) layer, and breaks the message into smaller units.Each of the segments produced has a header associated with it. The transport layer at the destination station reassembles the message.
2. Service Point Addressing: In order to deliver the message to the correct process, the transport layer header includes a type of address called service point address or port address. Thus by specifying this address, the

transport layer makes sure that the message is delivered to the correct process.

Layer 5: Session layer

The Session Layer creates the setup, controls the connections, and ends the teardown, between two or more computers, which is called a "session". Since DNS and other Name Resolution Protocols operate in this part of the layer, common functions of the Session Layer include user logon (establishment), name lookup (management), and user logoff (termination) functions. Including this matter, authentication protocols are also built into most client software, such as FTP Client and NFS Client for Microsoft Networks. Therefore, the Session layer establishes, manages and terminates the connections between the local and remote application. The Session Layer also provides for full-duplex, half-duplex, or simplex operation, and establishes procedures for checkpointing, suspending, restarting, and terminating a session between two related streams of data, such as an audio and a video stream in a web-conferencing application. Therefore, the session layer is commonly implemented explicitly in application environments that use remote procedure calls.

The functions of the session layer are :

1. Session establishment, maintenance, and termination: The layer allows the two processes to establish, use and terminate a connection.
2. Synchronization: This layer allows a process to add checkpoints which are considered synchronization points into the data. These synchronization points help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
3. Dialog Controller: The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

Layer 6: Presentation layer

The Presentation Layer establishes data formatting and data translation into a format specified by the application layer during the encapsulation of outgoing messages while being passed down the protocol stack, and possibly reversed during the deencapsulation of incoming messages when being passed up the protocol stack. The Presentation Layer handles protocol conversion, data encryption, data decryption, data compression, data decompression, incompatibility of data representation between OSs, and graphic commands. Since the presentation layer converts data and graphics into a display format for the Application Layer, the Presentation Layer is sometimes called the syntax layer. For this reason, the Presentation Layer negotiates the transfer of syntax structure through the Basic Encoding Rules of Abstract Syntax Notation One (ASN.1), with capabilities such as converting an EBCDIC-coded text file to an ASCII-coded file, or serialization of objects and other data structures from and to XML.

The functions of the presentation layer are :

1. Translation: For example, ASCII to EBCDIC.
2. Encryption/ Decryption: Data encryption translates the data into another form or code. The encrypted data is known as the ciphertext and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
3. Compression: Reduces the number of bits that need to be transmitted on the network.

Layer 7: Application layer

The application layer is the layer of the OSI model that is closest to the end user, which means both the OSI Application Layer and the user interact directly with software application that implements a component of communication between the client and server, such as File Explorer and Microsoft Word. Such application programs fall outside the scope of the OSI model unless they are directly integrated into the Application layer through the functions of communication, as is the case with applications such as Web Browsers and Email Programs. Other examples of software are Microsoft Network Software for File and Printer Sharing and Unix/Linux Network File System Client for access to shared file resources.

Application-layer functions typically include file sharing, message handling, and database access, through the most common protocols at the application layer, known as HTTP, FTP, SMB/CIFS, TFTP, and SMTP. When identifying communication partners, the application layer determines the identity and availability of communication partners for an application with data to transmit. The most important distinction in the application layer is the distinction between the application-entity and the application. For example, a reservation website might have two application-entities: one using HTTP to communicate with its users, and one for a remote database protocol to record reservations.

The function of application layer:

1. Network virtual terminal
2. FTAM : File Transfer access management
3. Mail services
4. Directory services

Conclusion :

OSI Model is reference model for implementation for network in real world model. OSI has seven layers, which has given task in distributed manner. There is same real world model called TCP/IP model with layers stated in OSI model.