**Introduction**

Open Systems Interconnection Model (OSI Model) is a conceptual model which was first defined in raw form in Washington, D.C., in February 1978 by French software engineer Hubert Zimmermann, and the refined but still draft standard was published by the ISO in 1980. It had two major components: an abstract model of networking, called the Basic Reference Model or seven-layer model, and a set of specific protocols. The OSI reference model was a major advance in the standardization of network concepts as although not a standard itself, it was a framework in which future standards could be defined.

It was made by an industry effort that attempted to get industry participants to agree on common network standards to provide multi-vendor interoperability as it was common for large networks to support multiple network protocol suites, with many devices unable to interoperate with other devices because a lack of common protocols.

The OSI protocol suite was considered by many as too complicated and inefficient and to a large extent unimplementable. Due to this, the TCP/IP model of 5 layers was picked up for practical implementation. It didn’t help that the TCP/IP model provided independent implementations of simplified protocols making it easier to apply practically.

This doesn’t mean that the OSI model is not used nowadays at all. Due to being a detailed model, it is still used by users and operators to determine the required hardware and software to build their network, understand and communicate the process followed by components communicating across a network, Perform troubleshooting, by identifying which network layer is causing an issue and focusing efforts on that layer.

**Overview of the OSI Model**

Application Layer

* The top layer of the OSI model is the Application layer.
* It does not refer to the actual applications that users run it just provides the framework that the actual applications run on top of it.
* In simple words to know what the application layer does, for example, a user wanted to use a web browser like Firefox, Chrome, etc. to open an FTP session and transfer a file. In this particular case, the application layer would define the file transfer protocol. This protocol is not directly accessible to the end user. The end user must still use an application that is designed to interact with the file transfer protocol. In this case, Internet Explorer would be that application.
* Some protocol of FPT are: telnet, DNS, DHCP, FTP, SNMOP, HTTP, NFS etc.

Presentation Layer

* The presentation layer takes the data that is provided by the application layer and converts it into a standard format that the other layers can understand.
* Likewise, this layer converts the inbound data that is received from the session layer into something that the application layer can understand.
* Also, it does Encryption and decryption of data, and compression for bandwidth management of data while handling the data.
* In order for network communications to function properly, the data needs to be structured in a standard way because applications handle data differently from one another. So this layer is necessary.

Session Layer:

* Once the data has been put into the correct format, the sending host must establish a session with the receiving host. This is where the session layer comes into play.
* It is mainly responsible for establishing, maintaining, and eventually terminating the session with the remote host with token management.
* The interesting thing about the session layer is that it is more closely related to the application layer than it is to the physical layer because sessions are established between applications.
* If a user is running multiple applications, several of those applications may have established sessions with remote resources at any time.
* Some session layer protocols are PPTP: Point-to-Point Tunneling Protocol, RPC: Remote Procedure Call Protocol, RTCP: Real-time Transport Control Protocol, SCP: Session Control Protocol, SDP: Session Description Protocol, etc.

Transport Layer

* The Transport layer is responsible for maintaining flow control and congestion control using TCP (Transmission Control Protocol).
* An operating system allows users to run multiple applications simultaneously and it is therefore possible that multiple applications may need to communicate over the network simultaneously so this layer takes the data from each application, and integrates it all into a single stream i.e., segment (which is also data unit in this layer).
* This layer is also responsible for providing error checking and performing data recovery when necessary.
* The transport Layer is responsible for ensuring that all of the data is sent from sending host to the receiving host.
* Apart from that Best-effort delivery of segments with no guarantees on ordering, integrity, reliability, and with no congestion and flow control is done by User Datagram Protocol (UDP).

Network Layer

* The Network Layer is responsible for determining how the data will reach the recipient.
* In simple words, it creates logical paths, known as virtual circuits, between the source and destination hosts.
* This layer handles things like addressing, routing, and logical protocols.
* The Network Layer is also responsible for its own error handling and packet sequencing and congestion control.
* The amount of data that must be transmitted often exceeds the maximum packet size I.e. MTU(maximum transmission unit). Therefore, the data is fragmented into multiple packets. When this happens, the Network Layer assigns each packet a sequence number. When the data is received by the remote host, that device’s Network layer examines the sequence numbers of the inbound packets and uses the sequence number to reassemble the data and to figure out if any packets are missing.
* Data units in this layer are called call a Packet.

Data link layer:

* The data link layer can be sub-divided into two other layers:
* Media Access Control (MAC) layer,
* The MAC layer basically establishes the computer’s identity on the network, via its MAC address.
* A MAC address is the address that is assigned to a network adapter at the hardware level
* Which is used while sending and receiving a data frame( which is the data unit of this layer) and also checks for chances of collision occurrence.
* Logical Link Control (LLC) layer
* The LLC layer controls frame synchronization, and flow control multiplexing of the L3 protocol and provides a degree of error checking.

Physical Layer

* The physical layer of the OSI model refers to the actual hardware specifications or characteristics such as timing and voltage.
* The physical layer defines the means of transmitting raw bits rather than logical data packets over a physical link connecting network nodes.
* The physical layer provides an electrical, mechanical, and procedural interface to the transmission medium.
* The shapes and properties of the electrical connectors, the frequencies to broadcast on, the modulation scheme to use, and similar low-level parameters, are specified here.