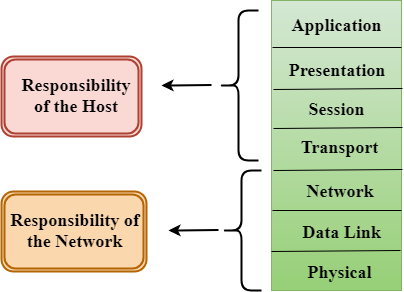
Experiment 01

**AIM**

To study different layers of OSI Model and define proper functions of protocols involved in OSI Model.

**THEORY**

* OSI stands for Open System Interconnection is a reference model that describes how information from a [software](https://www.javatpoint.com/software) application in one [computer](https://www.javatpoint.com/what-is-computer) moves through a physical medium to the software application in another computer.
* OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
* OSI consists of seven layers, and each layer performs a particular network function.
* Model) is a conceptual framework used to describe the functions of a networking system. The OSI model characterizes computing functions into a universal set of rules and requirements in order to support interoperability between different products and software. In the OSI reference model, the communications between a computing system are split into seven different abstraction layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.



**LAYERS**

The 7 Layers of the OSI Model:

1. Application Layer
2. Presentation Layer
3. Session Layer
4. Transport Layer
5. Network Layer
6. Datalink Layer
7. Physical Layer

**FUNCTIONS OF LAYERS**

**Application Layer**

At this layer, both the end user and the application layer interact directly with the software application. This layer sees network services provided to end-user applications such as a web browser or Office 365. The application layer identifies communication partners, resource availability, and synchronizes communication. An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer. This layer provides the network services to the end-users.

**Presentation Layer**

It acts as a data translator for a network. This layer is a part of the operating system that converts the data from one presentation format to another format. Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network. It at times also called the syntax layer.

**Session Layer**

The session layer controls the conversations between different computers. A session or connection between machines is set up, managed, and terminates at layer 5. Session layer services also include authentication and reconnections.

**Transport Layer**

The transport layer manages the delivery and error checking of data packets. It regulates the size, sequencing, and ultimately the transfer of data between systems and hosts. One of the most common examples of the transport layer is TCP or the Transmission Control Protocol. It receives the data from the upper layer and converts them into smaller units known as segments.

This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably. When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.

**Network Layer**

The network layer is responsible for receiving frames from the data link layer, and delivering them to their intended destinations among based on the addresses contained inside the frame. The network layer finds the destination by using logical addresses, such as IP (internet protocol). At this layer, routers are a crucial component used to quite literally route information where it needs to go between networks.

**Datalink Layer**

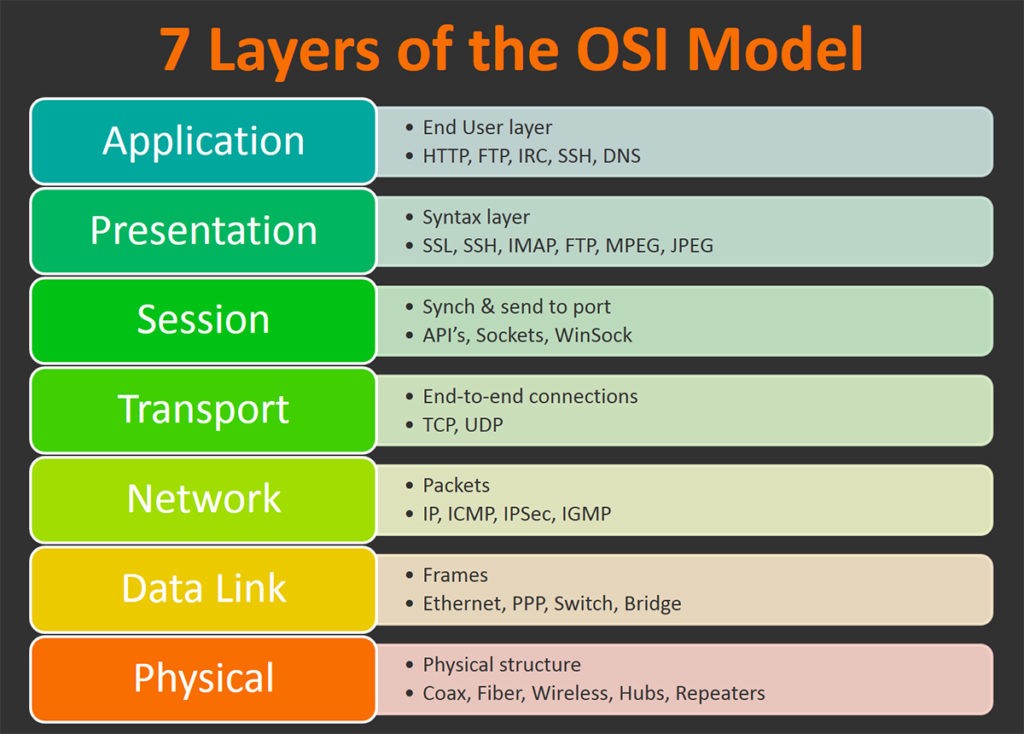
At the data link layer, directly connected nodes are used to perform node-to-node data transfer where data is packaged into frames. The data link layer also corrects errors that may have occurred at the physical layer.

The data link layer encompasses two sub-layers of its own. The first, media access control (MAC), provides flow control and multiplexing for device transmissions over a network. The second, the logical link control (LLC), provides flow and error control over the physical medium as well as identifies line protocols.

**Physical Layer**

The lowest layer of the OSI Model is concerned with electrically or optically transmitting raw unstructured data bits across the network from the physical layer of the sending device to the physical layer of the receiving device. It can include specifications such as voltages, pin layout, cabling, and radio frequencies. At the physical layer, one might find “physical” resources such as network hubs, cabling, repeaters, network adapters or modems.

**PROTOCOLS**

****

1. HTTP: Hypertext Transfer Protocol (HTTP) is an application-layer protocol for transmitting hypermedia documents, such as HTML. It was designed for communication between web browsers and web servers.
2. FTP: The File Transfer Protocol is a standard communication protocol used for the transfer of computer files from a server to a client on a computer network. FTP is built on a client–server model architecture using separate control and data connections between the client and the server.
3. DNS: DNS stands for Domain Name System. The main function of DNS is to translate domain names into IP Addresses, which computers can understand. It also provides a list of mail servers which accept Emails for each domain name.
4. IMAP: In computing, the Internet Message Access Protocol is an Internet standard protocol used by email clients to retrieve email messages from a mail server over a TCP/IP connection.
5. TCP: TCP stands for Transmission Control Protocol a communications standard that enables application programs and computing devices to exchange messages over a network. It is designed to send packets across the internet and ensure the successful delivery of data and messages over networks.
6. UDP: User datagram protocol (UDP) operates on top of the Internet Protocol (IP) to transmit datagrams over a network.
7. IP: An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.
8. ICMP: Internet Control Message Protocol (ICMP) is used for reporting errors and performing network diagnostics. In the error reporting process, ICMP sends messages from the receiver to the sender when data does not come though as it should.
9. SSH: SSH provides password or public-key based authentication and encrypts connections between two network endpoints. It is a secure alternative to legacy login protocols (such as telnet, login) and insecure file transfer methods (such as FTP).
10. IRC:  It is mainly used for group discussion in chat rooms called “channels” although it supports private messages between two users, data transfer, and various server-side and client-side commands.