PRACTICAL 1

Aim :

To compare **OSI model and TCP/IP model**

Hardware Required : Not Any

Software Required : Not Any

Theory :

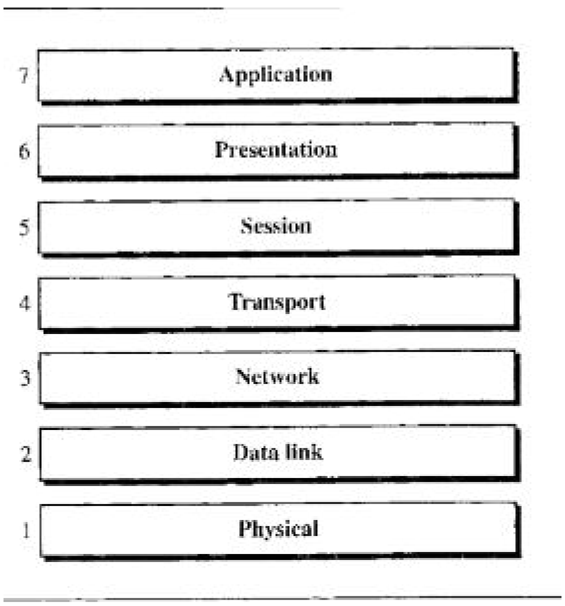
OSI Model

Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection model. It was first introduced in the late 1970s. An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.

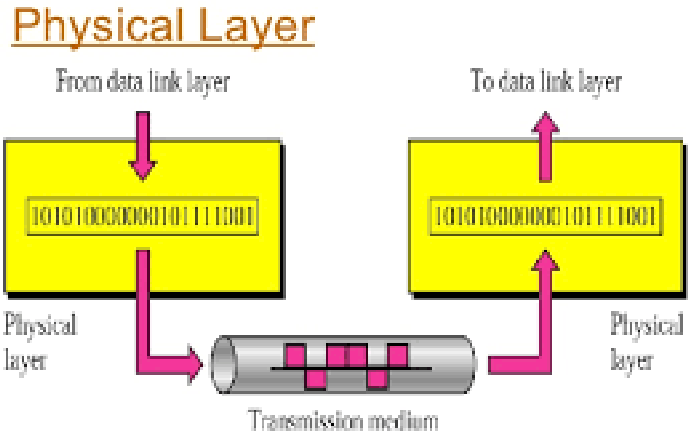
OSI is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.

OSI consists of seven layers, and each layer performs a particular network function. OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task. Each layer is self-contained, so that task assigned to each layer can be performed independently.

Layers of OSI model



1. Physical Layer (Layer 1) :



The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of bits. It is responsible for the actual physical connection between the devices. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.

It is Also Responsible for the following:
-Physical Characteristic of Interfaces and Medium:The physical layer defines the characteristics of the interface between the devices and the transmission medium. It also defines the type of transmission medium.
-Representation of Bits:s. The physical layer data consists of a stream of bits with no interpretation. To be transmitted, bits must be encoded into signals–electrical or optical. The physical layer defines the type of encoding.
-Data Rate:The transmission rate-the number of bits sent each second-is also defined by the physical layer.
-Synchronization Of Bits:The sender and receiver not only must use the same bit rate but also must be synchronized at the bit level.
-Line Configuration:The physical layer is concerned with the connection of devices to the media.
-Physical Topology:The physical topology defines how devices are connected to make a network.
-Transmission mode:The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex.

2. Data Link Layer (DLL) (Layer 2) :

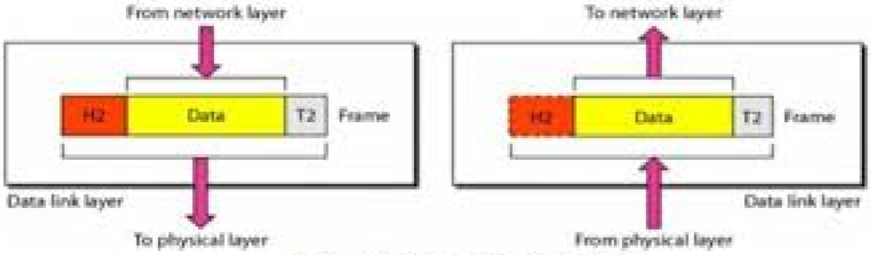
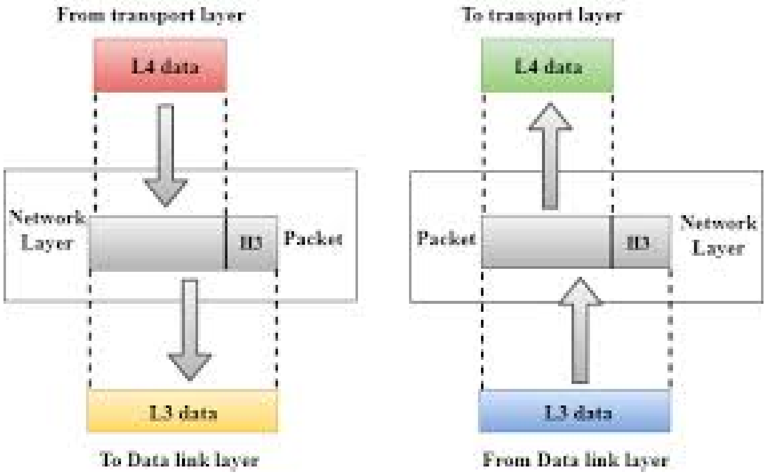


Fig. Data Link Layer

The data link layer is responsible for the node to node delivery of the message. The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address. Data Link Layer is divided into

two sub layers : Logical Link Control (LLC)
Media Access Control (MAC)
It is Also Responsible for the following:
-Framing:. The data link layer divides the stream of bits received from the network layer into manageable data units called frames.
-Physical Addressing:If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame. I
-Flow Control:If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.
-Error Control:The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames.
-Acess Control:When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

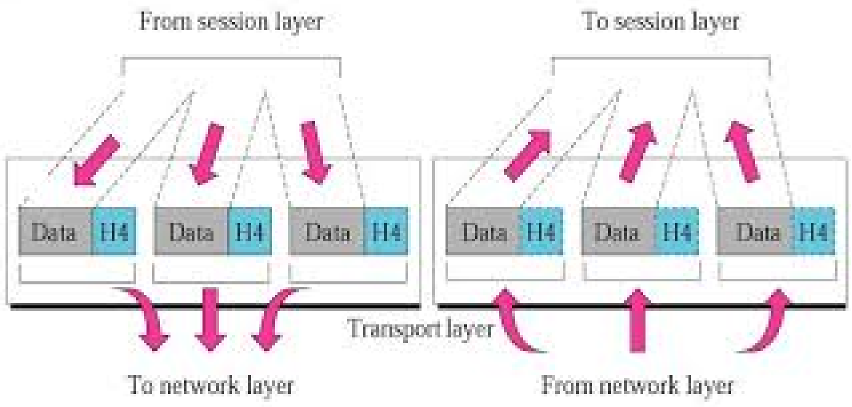
3. Network Layer (Layer 3) :



Network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet rout-

ing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender and receiver's IP address are placed in the header by network layer.
It is Also Responsible for the following:
-Logical Addressing:The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.
-Routing:When independent networks or links are connected to create intemetworks (network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination.

4. Transport Layer (Layer 4) :



Transport layer provides services to application layer and takes services from network layer. The data in the transport layer is referred to as Segments. It is responsible for the End to End delivery of the complete message. Transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found.
It is Also Responsible for the following:
-Segmentation And Reassembly:A message is divided into transmittable segments, with each segment containing a sequence number. These

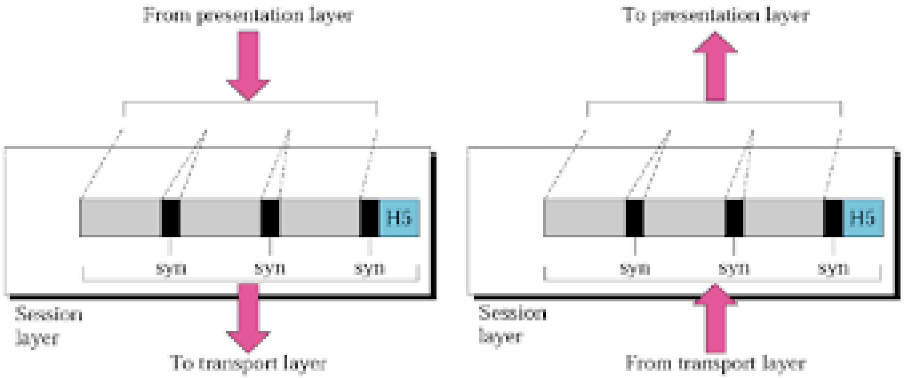
numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.

-Connection Control:The transport layer can be either connectionless or connectionoriented. A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connectionoriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated.

-Flow Control:flow control at this layer is performed end to end rather than across a single link.

-Error Control:Like the data link layer, the transport layer is responsible for error control. However, error control at this layer is performed process-toprocess rather than across a single link. Error correction is usually achieved through retransmission.

5. Session Layer (Layer 5) :



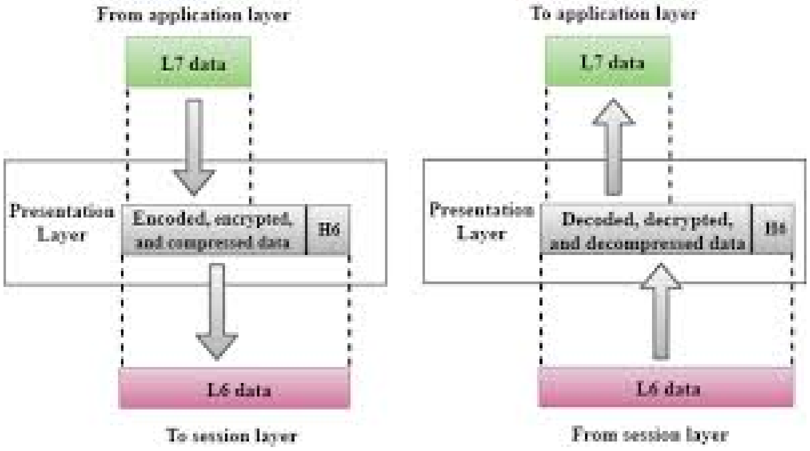
This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.

It is Also Responsible for the following:

-Dialouge Control:The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either halfduplex (one way at a time) or full-duplex (two ways at a time) mode.

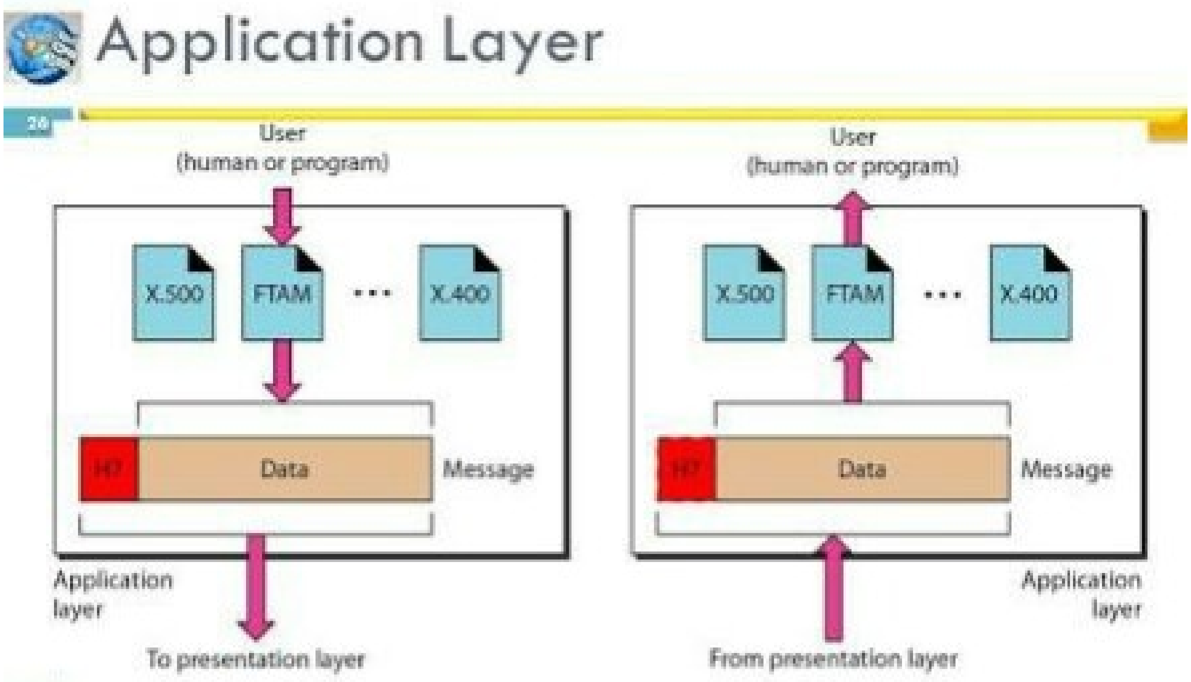
-Synchronization:The session layer allows a process to add checkpoints, or synChronization points, to a stream of data.

6. Presentation Layer (Layer 6) :



Presentation layer is also called the Translation layer.The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.
It is Also Responsible for the following:
-Translation:The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on. The infonnation must be changed to bit streams before being transmitted. Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods.
-Compression:Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.
-Encryption:To carry sensitive information, a system must be able to ensure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form

7. Application Layer (Layer 7) :



At the very top of the OSI Reference Model stack of layers, we find Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user.

It is Also Responsible for the following:

-Network Virtual Terminal:A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host. The user's computer talks to the software terminal which, in turn, talks to the host, and vice versa. The remote host believes it is communicating with one of its own terminals and allows the user to log on.

-Mail Services:This application provides the basis for e-mail forwarding and storage.

-Directory Services:This application provides distributed database sources and access for global information about various objects and services.

-File Tranfer,Access and Management:This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.

TCP/IP MODEL:

TCP/IP stands for transmission control protocol/internet working protocol. It is used in the internet, was developed prior to the OSI Model. Therefore, the layers in the TCP/IP suite donot match exactly with those in the OSI model. The TCP/IP protocol suite is made of five layers: physical, datalink, network, transport, and application. The first four layers provide physical standard, network interface, inter networking, and transport function that correspond to the first four layers of the OSI Model. The three topmost layer is the OSI model, however, are represented in TCP/IP by a single layer called the application layer. TCP/IP Protocal suite contain relatively independent protocols that can be mixed and matched depending on the needs of the system. The term HIERARCHICAL means that each upper- level protocol is supported by one or more lower-level protocols. At the transport layer, TCP/IP defines two protocols: Transmission control protocol(TCP) and User Datagram Protocol(UDP). At the network layer, the main protocol defined by TCP/IP is Internetworking protocol(IP), although there are some other protocols that support data movement in this layer.

TCP/IP features:

- The popularity of the TCP/IP protocols did not grow rapidly just because the protocols were there, or because connecting to the Internet mandated their use. They met an important need (worldwide data communication) at the right time, and they had several important features that allowed them to meet this need. These features are:

- Open protocol standards, freely available and developed independently from any specific computer hardware or operating system. Because it is so widely supported, TCP/IP is ideal for uniting different hardware and software components, even if you don't communicate over the Internet.

- Independence from specific physical network hardware. This allows TCP/IP to integrate many different kinds of networks. TCP/IP can be run over an Ethernet, a DSL connection, a dial-up line, an optical network, and virtually any other kind of physical transmission medium.

- A common addressing scheme that allows any TCP/IP device to uniquely address any other device in the entire network, even if the network is as large as the worldwide Internet.

- Standardized high-level protocols for consistent, widely available user services.

Layers of TCP/IP Model:

Layer 1. Network Access Layer:

Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire. The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc. The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

Layer 2. Internet layer:

Internet Layer is the second layer of the four layer TCP/IP model. The position of Internet layer is between Network Access Layer and Transport layer. Internet layer pack data into data packets known as

IP datagrams, which contain source and destination address (logical address or IP address) information that is used to forward the datagrams between hosts and across networks. The Internet layer is also responsible for routing of IP datagrams. The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) and IGMP (Internet Group Management Protocol).
-IP:The Internet Protocol is responsible for addressing host interfaces, encapsulating data into datagrams (including fragmentation and reassembly) and routing datagrams from a source host interface to a destination host interface across one or more IP networks.
-ICMP:It is used by network devices, including routers, to send error messages and operational information indicating.
-ARP:The Address Resolution Protocol is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address.
-RARP:The Reverse Address Resolution Protocol is an obsolete computer networking protocol used by a client computer to request its address from a computer network, when all it has available is its link layer or hardware address, such as a MAC address.
-IGMP:IGMP can be used for one-to-many networking applications such as online streaming video and gaming, and allows more efficient use of resources when supporting these types of applications.

Layer 3. Transport layer:

Transport Layer is the third layer of the four layer TCP/IP model. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data.

The main protocols included at Transport layer are TCP (Transmis-

sion Control Protocol) and UDP (User Datagram Protocol).
-TCP:TCP is a connection-oriented protocol, which means a connection is established and maintained until the application programs at each end have finished exchanging messages.
-UDP:UDP provides checksums for data integrity, and port numbers for addressing different functions at the source and destination of the datagram.

Layer 4. Application layer:

Application layer is the top most layer of four layer TCP/IP model. Application layer is present on the top of the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol) , DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.
-HTTP:HTTP is the underlying protocol used by the World Wide Web and this protocol defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.
-POP3:POP3 (Post Office Protocol 3) is the most recent version of a standard protocol for receiving e-mail. POP3 is a client/server protocol in which e-mail is received and held for you by your Internet server.
-SMTP:SMTP is a push protocol and is used to send the mail whereas POP (post office protocol) or IMAP (internet message access protocol) are used to retrieve those mails at the receiver's side.
STP:The Spanning Tree Protocol (STP) is a network protocol that builds a loop-free logical topology for Ethernet networks. The basic function of STP is to prevent bridge loops and the broadcast radiation that results from them. Spanning tree also allows a network design to

include backup links to provide fault tolerance if an active link fails.
TFTP:Trivial File Transfer Protocol (TFTP) is an Internet software utility for transferring files that is simpler to use than the File Transfer Protocol (FTP) but less capable. It is used where user authentication and directory visibility are not required.

Conclusion :

From this practical we have learned some of the major components of Networks i.e. The OSI and TCP/IP model;Diferrent layers Of OSI And TCP/IP and their function or role.Knowing how networks are built gives us a better understanding of what physical or logical sensitivity are introduced by choosing one particular network design over another.

Compare TCP And UDP?

TCP(Transmission Control Protocol)	***UDP(User Datagram Protocol)***
TCP is a connection-oriented protocol.	UDP is a connectionless protocol.
TCP provides extensive error checking mechanisms.	UDP has only the basic error checking mechanism using checksums.
TCP is comparatively slower than UDP.	UDP is faster, simpler and more efficient than TCP.
TCP is suited for application that require high reliability,and transmission time is relatively less critical.	UDP is suitable for applications that need fast, efficient transmission, such as games.
TCP is used by HTTP, HTTPs, FTP, SMTP and Telnet	UDP is used by DNS, DHCP, TFTP, SNMP, RIP, and VoIP.

References :

Data Communications and Networking By Behrouz A.Forouzan.
-www.geeksforgeeks.org
-https://searchnetworking.techtarget.com