Network Reference Models

4.1 OSI Reference Model :

1. 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.
2. 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.
3. The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software.
4. The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable. ISO is the organization. OSI is the model.
5. The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems.
6. It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network **(see Figure1)**.
7. **Figure**

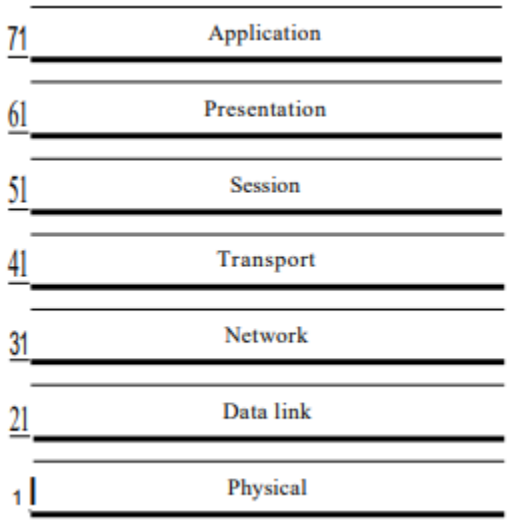


Figure 1: Seven layers of the OSI model

4.1.1) Layered Architecture

1. The OSI model is composed of seven ordered layers: physical (layer 1), data link (layer 2), network (layer 3), transport (layer 4), session (layer 5), presentation (layer 6), and application (layer 7).
2. Figure 2 shows the layers involved when a message is sent from device A to device B. As the message travels from A to B, it may pass through many intermediate nodes.

3. These intermediate nodes usually involve only the first three layers of the OSI model. In developing the model, the designers distilled the process of transmitting data to its most fundamental elements.
4. They identified which networking functions had related uses and collected those functions into discrete groups that became the layers.
5. Each layer defines a family of functions distinct from those of the other layers. By defining and localizing functionality in this fashion, the designers created an architecture that is both comprehensive and flexible.
6. Most importantly, the OSI model allows complete interoperability between otherwise incompatible systems. Within a single machine, each layer calls upon the services of the layer just below it.
7. Layer 3, for example, uses the services provided by layer 2 and provides services for layer 4. Between machines, layer x on one machine communicates with layer x on another machine.
8. This communication is governed by an agreed-upon series of rules and conventions called protocols.

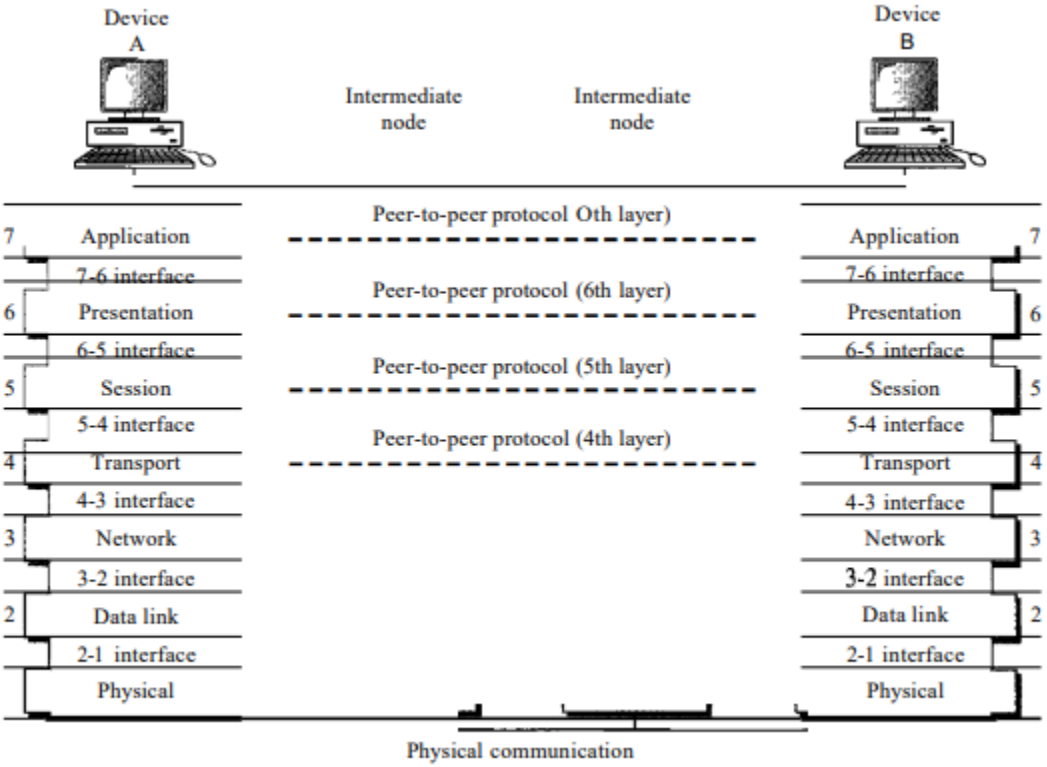


Figure 2: The interaction between layers in the OSI model

4.1.2) Peer-to-Peer Processes

1. The processes on each machine that communicate at a given layer are called peer-to-peer processes. Communication between machines is therefore a peer-to-peer process using the protocols appropriate to a given layer.
2. At the physical layer, communication is direct: In Figure 2, device A sends a stream of bits to device B (through intermediate nodes).
3. At the higher layers, however, communication must move down through the layers on device A, over to device B, and then back up through the layers.
4. Each layer in the sending device adds its own information to the message it receives from the layer just above it and passes the whole package to the layer just below it.
5. At layer I the entire package is converted to a form that can be transmitted to the receiving device.

6. At the receiving machine, the message is unwrapped layer by layer, with each process receiving and removing the data meant for it.
7. For example, layer 2 removes the data meant for it, then passes the rest to layer 3.
8. Layer 3 then removes the data meant for it and passes the rest to layer 4, and so on.

4.1.3) Interfaces between layers

1. The passing of the data and network information down through the layers of the sending device and back up through the layers of the receiving device is made possible by an interface between each pair of adjacent layers.
2. Each interface defines the information and services a layer must provide for the layer above it. Well-defined interfaces and layer functions provide modularity to a network.
3. As long as a layer provides the expected services to the layer above it, the specific implementation of its functions can be modified or replaced without requiring changes to the surrounding layers.

4.1.4) Protocols

Note: 1) Kindly refer to figure 2 same figure for Interface, Peer to peer & Layered Architecture…

2) Kindly refer protocol for more detail in chapter 5th

4.1.5) Organization of layers

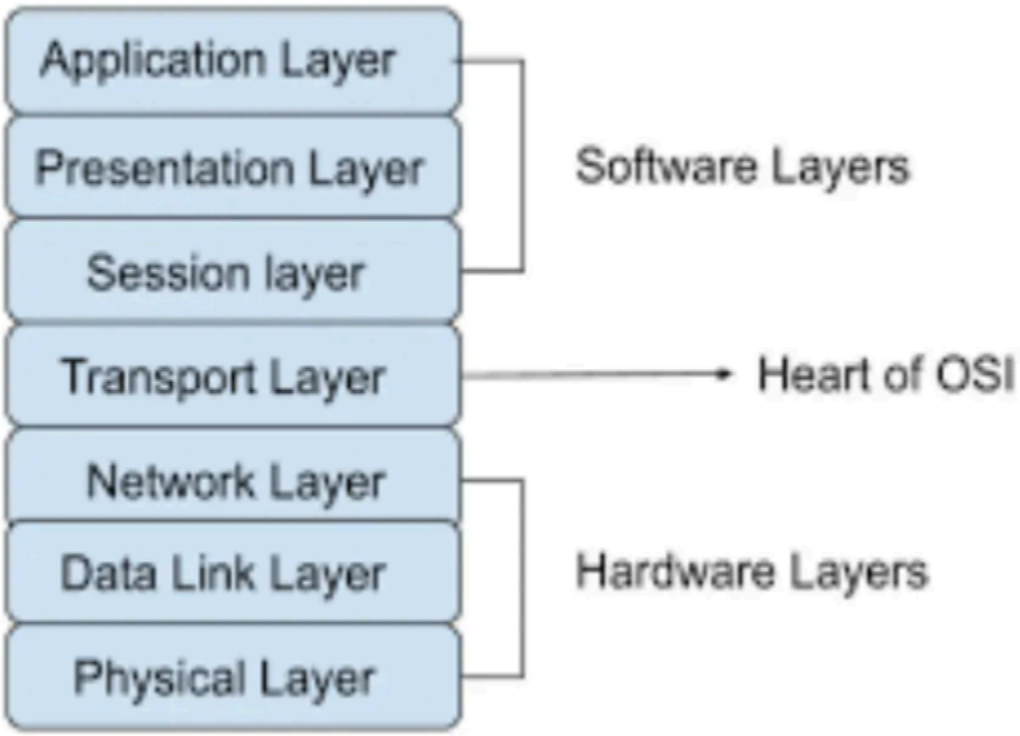


Figure: Organization of layers

<u>The seven layers can be thought of as belonging to three subgroups.</u>

1. Layers I, 2, and 3-physical, data link, and network-are the network support layers; they deal with the physical aspects of moving data from one device to another (such as electrical specifications, physical connections, physical addressing, and transport timing and reliability).
2. **Software Layers :** Layers 5, 6, and 7-session, presentation, and application-can be thought of as the user support layers; they allow interoperability among unrelated software systems.
3. **Heart of OSI Layers :** Layer 4, the transport layer, links the two subgroups and ensures that what the lower layers have transmitted is in a form that the upper layers can use.
4. **Hardware Layers:** The upper OSI layers are almost always implemented in software; lower layers are a combination of hardware and software, except for the physical layer, which is mostly hardware.

In Figure 3, which gives an overall view of the OSI layers, D7 means the data unit at layer 7, D6 means the data unit at layer 6, and so on.

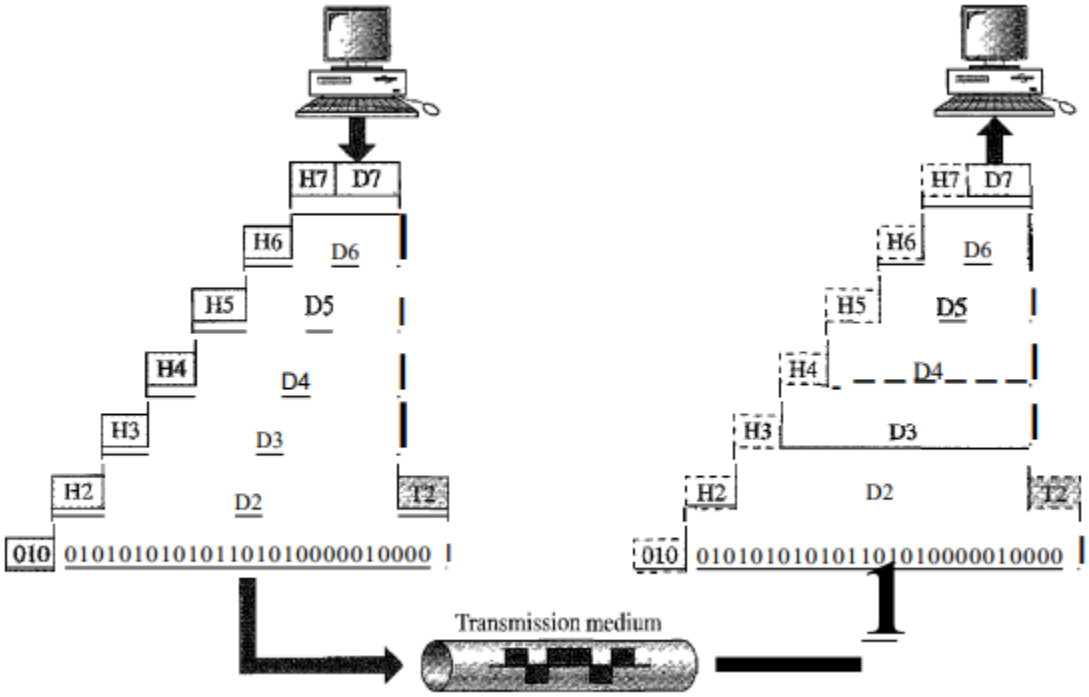


Figure. 3:An exchange using the OSI model

1. The process starts at layer 7 (the application layer), then moves from layer to layer in descending, sequential order.
2. At each layer, a header, or possibly a trailer, can be added to the data unit. Commonly, the trailer is added only at layer 2.
3. When the formatted data unit passes through the physical layer (layer 1), it is changed into an electromagnetic signal and transported along a physical link.
4. Upon reaching its destination, the signal passes into layer 1 and is transformed back into digital form.
5. The data units then move back up through the OSI layers. As each block of data reaches the next higher layer, the headers and trailers attached to it at the corresponding sending layer are removed, and actions appropriate to that layer are taken.
6. By the time it reaches layer 7, the message is again in a form appropriate to the application and is made available to the recipient.

4.1.6) Encapsulation

1. Figure reveals another aspect of data communications in the OSI model: encapsulation. A packet (header and data) at level 7 is encapsulated in a packet at level 6.
2. The whole packet at level 6 is encapsulated in a packet at level 5, and so on. In other words, the data portion of a packet at level N - 1 carries the whole packet (data and header and maybe trailer) from level N.
3. The concept is called encapsulation; level N - 1 is not aware of which part of the encapsulated packet is data and which part is the header or trailer. For level N - 1, the whole packet coming from level N is treated as one integral unit.

4.1.7) Functions and features of each layer.

Physical Layer

1. The physical layer coordinates the functions required to carry a bit stream over a physical medium.
2. It deals with the mechanical and electrical specifications of the interface and transmission medium.
3. It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to Occur.
4. The physical layer is responsible for movements of individual bits from one hop (node) to the next.

#Figure shows the position of the physical layer with respect to the transmission medium and the data link layer.

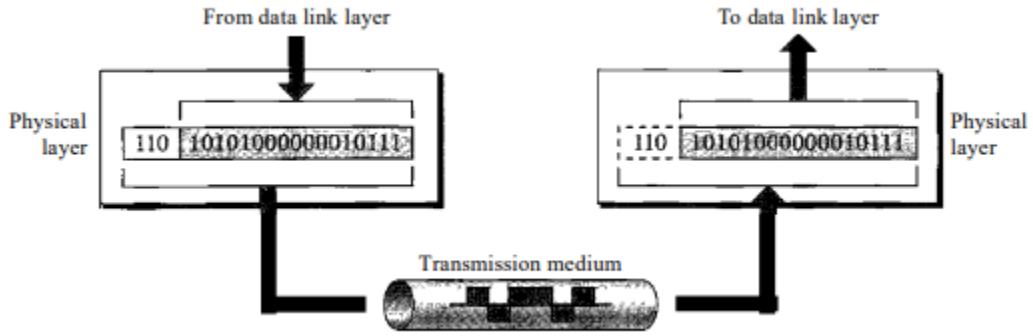


Figure: Physical layer

#The physical layer is also concerned with the following Features:

A. **Physical characteristics 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.
B. **Representation of bits.** The physical layer data consists of a stream of bits (sequence of Os or 1s) with no interpretation. To be transmitted, bits must be encoded into signals--electrical or optical. The physical layer defines the type of encoding (how Os and Is are changed to signals).
C. **Data rate.** The transmission rate-the number of bits sent each second-is also defined by the physical layer. In other words, the physical layer defines the duration of a bit, which is how long it lasts.
D. **Synchronization of bits.** The sender and receiver not only must use the same bit rate but also must be synchronized at the bit level. In other words, the sender and the receiver clocks must be synchronized.

E. **Line configuration.** The physical layer is concerned with the connection of devices to the media. In a point-to-point configuration, two devices are connected through a dedicated link. In a multipoint configuration, a link is shared among several devices.

F. **Physical topology.** The physical topology defines how devices are connected to make a network. Devices can be connected by using a mesh topology (every device is connected to every other device), a star topology (devices are connected through a central device), a ring topology (each device is connected to the next, forming a ring), a bus topology (every device is on a common link), or a hybrid topology (this is a combination of two or more topologies).

G. **Transmission mode.** The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex. In simplex mode, only one device can send; the other can only receive. The simplex mode is a one-way communication. In the half-duplex mode, two devices can send and receive, but not at the same time. In a full-duplex (or simply duplex) mode, two devices can send and receive at the same time.

Data Link Layer

1. The data link layer transforms the physical layer, a raw transmission facility, to a reliable link.
2. It makes the physical layer appear error-free to the upper layer (network layer).
3. The data link layer is responsible for moving frames from one hop (node) to the next.

#Figure shows the relationship of the data link layer to the network and physical layers.

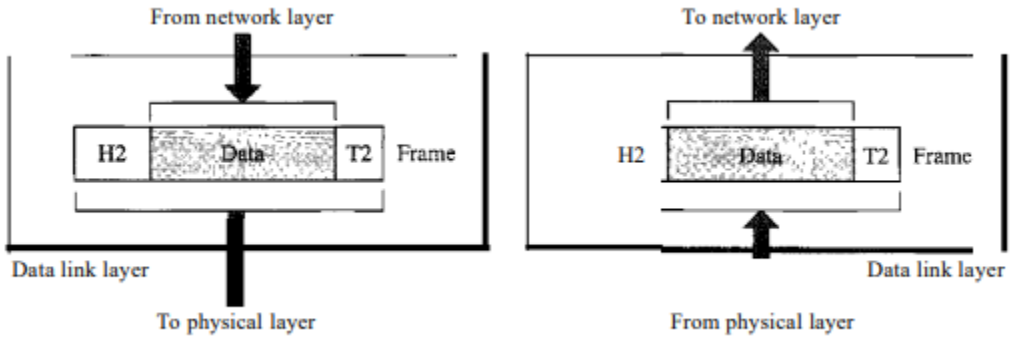


Figure: Data link layer

#Other responsibilities of the data link layer include the following Features:

A. **Framing.**:The data link layer divides the stream of bits received from the network layer into manageable data units called frames.

B. **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. If the frame is intended for a system outside the sender's network, the receiver address is the address of the device that connects the network to the next one.

C. **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.

D. **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. Error control is normally achieved through a trailer added to the end of the frame.

E. **Access 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.

Network Layer

1. The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links).
2. Whereas the data link layer oversees the delivery of the packet between two systems on the same network (links), the network layer ensures that each packet gets from its point of origin to its final destination.
3. If two systems are connected to the same link, there is usually no need for a network layer.
4. However, if the two systems are attached to different networks (links) with connecting devices between the networks (links), there is often a need for the network layer to accomplish source-to-destination delivery.

#Figure 2.8 shows the relationship of the network layer to the data link and transport layers.

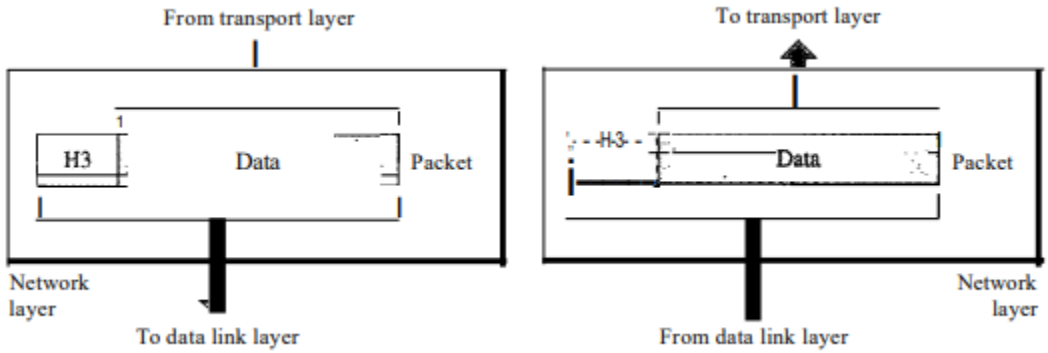


Figure:Network layer

#Other responsibilities of the network layer include the following Features:

A. **Logical addressing:** 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.

B. **Routing:** When independent networks or links are connected to create internetworks (network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination. One of the functions of the network layer is to provide this mechanism.

Transport Layer

1. The transport layer is responsible for process-to-process delivery of the entire message. A process is an application program running on a host.
2. Whereas the network layer oversees source-to-destination delivery of individual packets, it does not recognize any relationship between those packets.
3. It treats each one independently, as though each piece belonged to a separate message, whether or not it does.

4. The transport layer, on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level.

#Figure shows the relationship of the transport layer to the network and session layers.

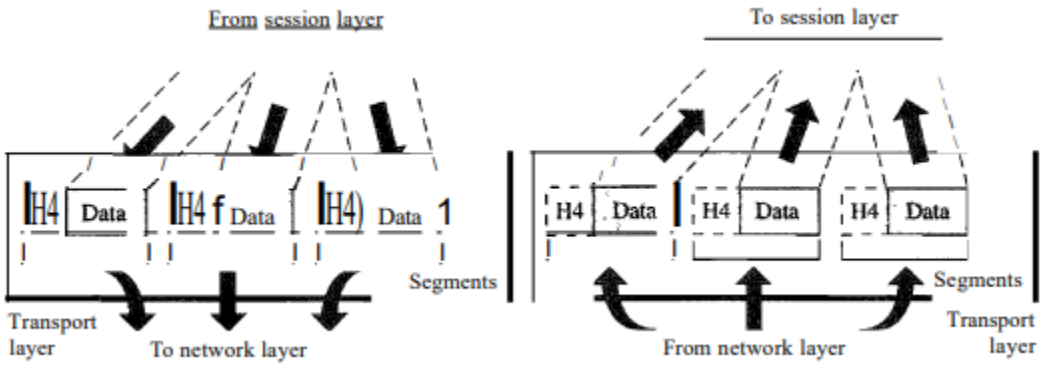


Figure: Transport Layer

#Other responsibilities of the transport layer include the following Features:

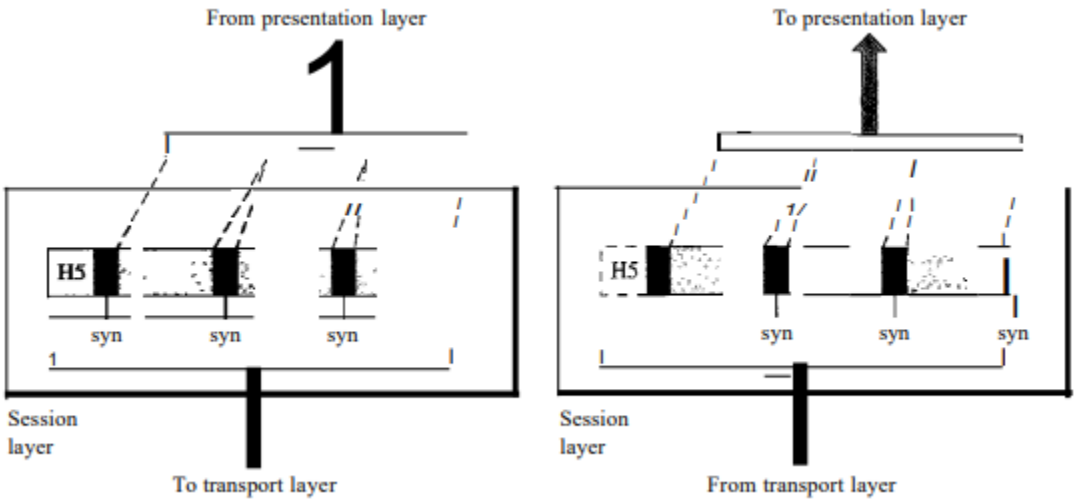
A. **Service-point addressing:** Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other. The transport layer header must therefore include a type of address called a service-point address (or port address). The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.
B. **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.
C. **Connection control:** The transport layer can be either connectionless or connection oriented. A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connection oriented 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.
D. **Flow control:** Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end to end rather than across a single link.
E. **Error control:** Like the data link layer, the transport layer is responsible for error control. However, error control at this layer is performed process-to-process rather than across a single link. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication). Error correction is usually achieved through retransmission.

Session Layer

1. The services provided by the first three layers (physical, data link, and network) are not sufficient for some processes.

2. The session layer is the network dialog controller. It establishes, maintains, and synchronizes the interaction among communicating systems.
3. The session layer is responsible for dialog control and synchronization.

#Figure illustrates the relationship of the session layer to the transport and presentation layers.



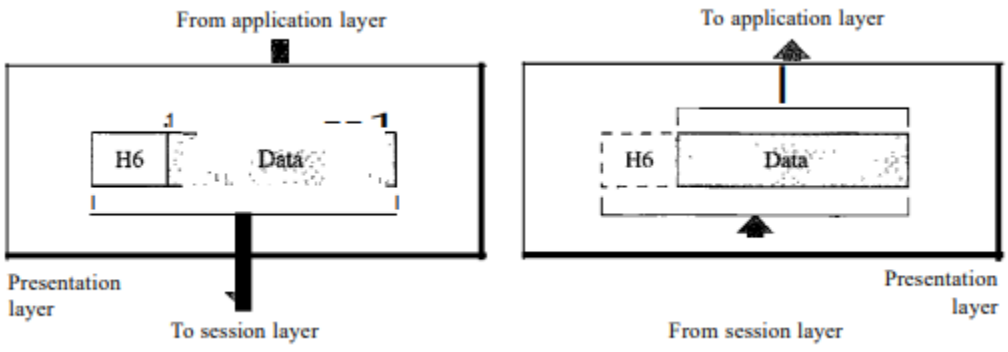
#Specific responsibilities of the session layer include the following Features:

A. **Dialog control:** The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half duplex (one way at a time) or full-duplex (two ways at a time) mode.
B. **Synchronization.** The session layer allows a process to add checkpoints, or synChronization points, to a stream of data. For example, if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently. In this case, if a crash happens during the transmission of page 523, the only pages that need to be resent after system recovery are pages 501 to 523. Pages previous to 501 need not be resent.

Presentation Layer

1. The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.
2. The presentation layer is responsible for translation, compression, and encryption.

#Figure shows the relationship between the presentation layer and the application and session layers.



#Specific responsibilities of the presentation layer include the following Features:

A. **Translation:** The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on. The information 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. The presentation layer at the sender changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format.
B. **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.
C. **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.

Application Layer

1. The application layer enables the user, whether human or software, to access the network.
2. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.
3. The application layer is responsible for providing services to the user.

#Figure shows the relationship of the application layer to the user and the presentation layer

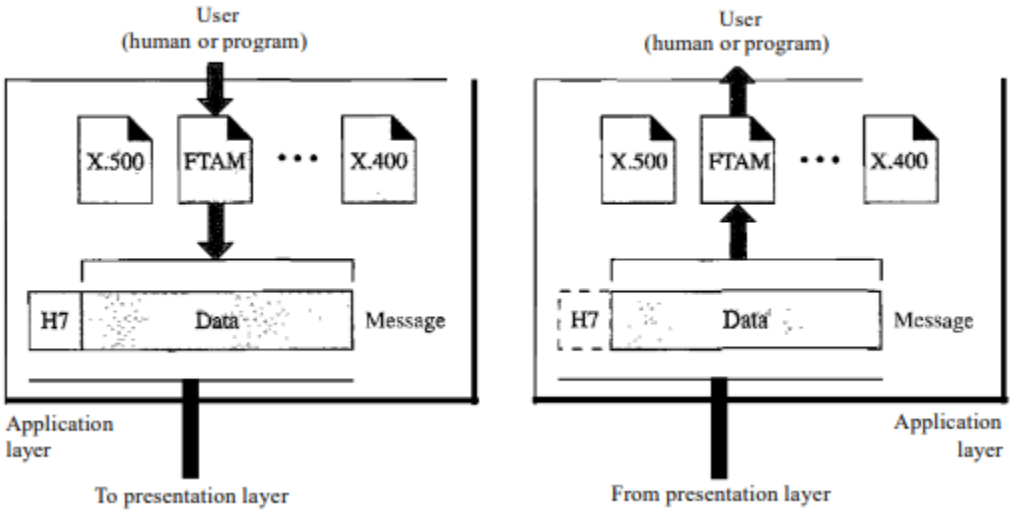


Figure: Application Layer

Specific services provided by the application layer include the following Features:

A. **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.

B. **File transfer, 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.

C. **Mail services:** This application provides the basis for e-mail forwarding and storage. o Directory services. This application provides distributed database sources and access for global information about various objects and services.

4.2 TCP/IP Model :

1. The TCP/IP protocol suite was developed prior to the OSI model. Therefore, the layers in the TCP/IP protocol suite do not exactly match those in the OSI model.
2. TCP/IP is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality; however, the modules are not necessarily interdependent.
3. Whereas the OSI model specifies which functions belong to each of its layers, the layers of the TCP/IP protocol suite contain relatively independent protocols that can be mixed and matched depending on the needs of the system.
4. It consist of five layer i.e. Application Layer, Transport Layer, Network Layer/Internet Layer & Link layer/ Network Access Layer/Host to Network Layer.

4.2.1) TCP/IP Layered Architecture,

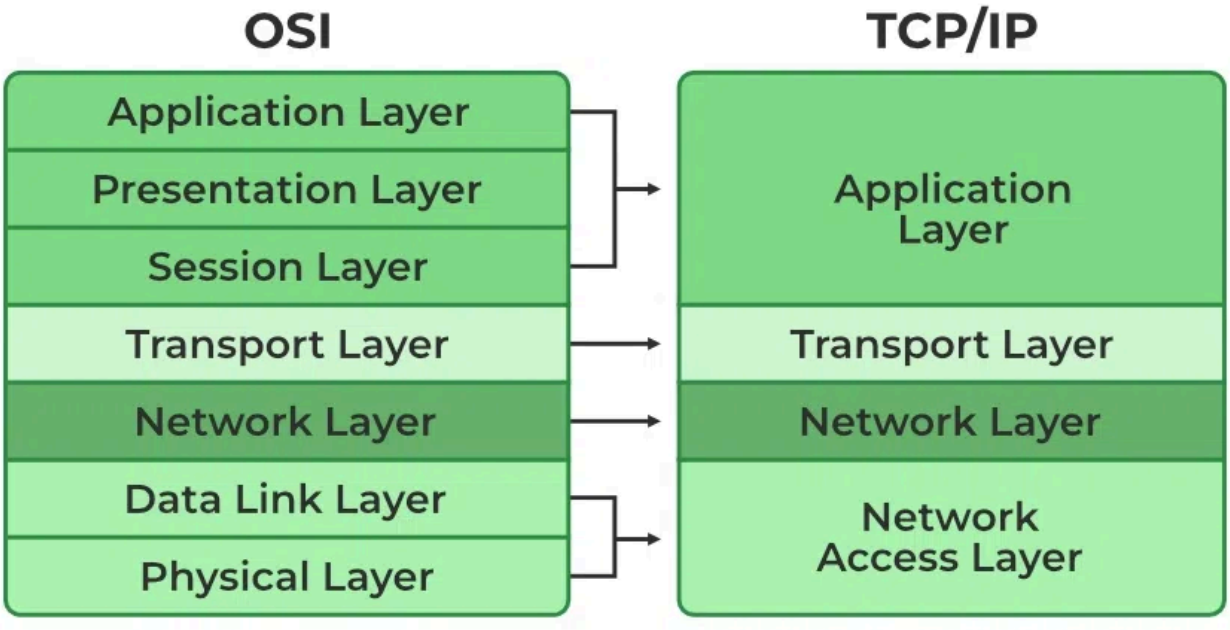


Figure: TCP/IP Layered Architecture

1. The original TCP/IP protocol suite was defined as having four layers: host-to-network, internet, transport, and application.

2. However, when TCP/IP is compared to OSI, we can say that the host-to-network layer is equivalent to the combination of the physical and data link layers.
3. The internet layer is equivalent to the network layer, and the application layer is roughly doing the job of the session, presentation, and application layers with the transport layer in TCP/IP taking care of part of the duties of the session layer.
4. The TCP/ IP protocol suite is made of five layers: physical, data link, network, transport, and application.
5. The first four layers provide physical standards, network interfaces, internetworking, and transport functions that correspond to the first four layers of the OSI model.
6. The three topmost layers in the OSI model, however, are represented in TCP/IP by a single layer called the application layer.

4.2.2) Organization of layers,

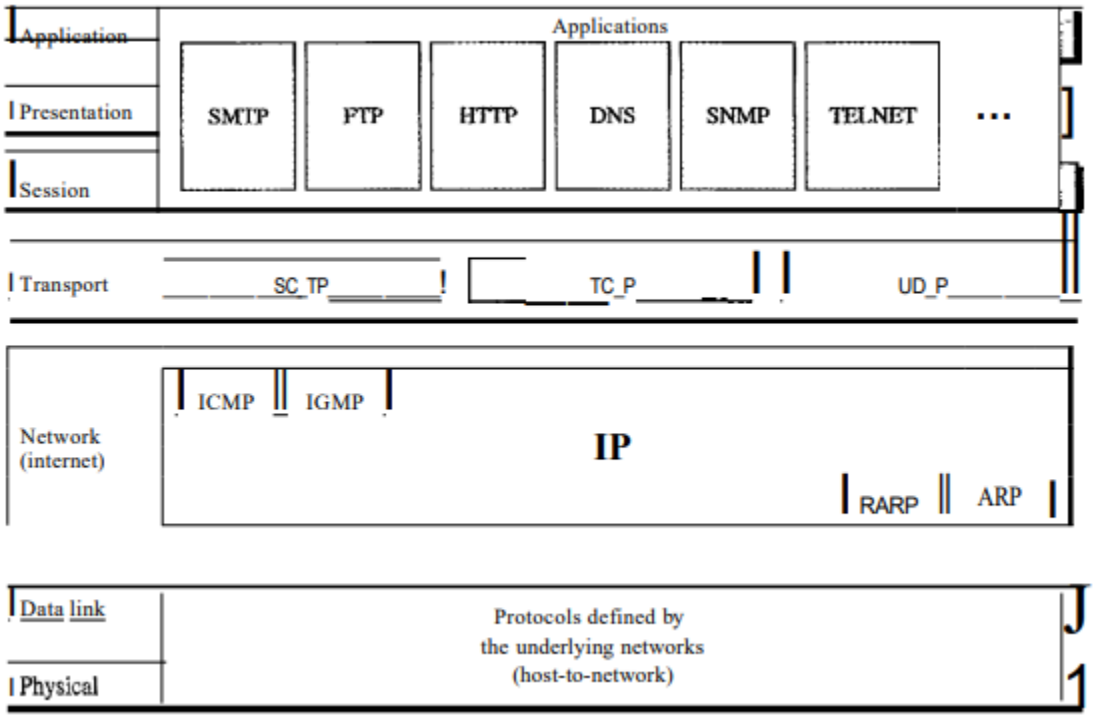


Figure: Organization of layers of TCP/IP Protocol Suite

The original TCP/IP protocol suite was defined as having four layers:

#Host-to-network Layer :

1. However, when TCP/IP is compared to OSI, we can say that the host-to-network layer is equivalent to the combination of the physical and data link layers.
2. Protocols defined by the underlaying network (Host to Network).

#Internet Layer:

1. The internet layer is equivalent to the network layer, and the application layer is roughly doing the job of the session, presentation, and application layers with the transport layer in TCP/IP taking care of part of the duties of the session layer.

2. At the network layer, the main protocol defined by TCP/IP is the Internetworking Protocol (IP); there are also some other protocols like ARP,RARP, ICMP & IGMP that support data movement in this layer.

#Transport Layer:

1. At the transport layer, TCP/IP defines three protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Stream Control Transmission Protocol (SCTP).
2. It supports connection oriented & connectionless service as well as reliable or unreliable service.

#Application Layer.

1. The application layer in TCP/IP is equivalent to the combined session, presentation, and application layers in the OSI modeL Many protocols are defined at this layer.
2. It consists of HTTP,HTTPS,SMTP ,SNMP,TELNET,DNS and FTP protocol.

The TCP/ IP protocol suite is made of five layers: physical, data link, network, transport, and application.

1. The first four layers provide physical standards, network interfaces, internetworking, and transport functions that correspond to the first four layers of the OSI model.
2. The three topmost layers in the OSI model, however, are represented in TCP/IP by a single layer called the application layer.

4.2.3)Functions and features of TCP/IP layers.

Physical and Data Link Layers:

1. At the physical and data link layers, TCP/IP does not define any specific protocol. It supports all the standard and proprietary protocols.
2. A network in a TCPIIP internetwork can be a local-area network or a wide-area network.

Network Layer:

1. At the network layer (or, more accurately, the internetwork layer), TCP/IP supports the Internetworking Protocol.
2. IP, in turn, uses four supporting protocols: ARP, RARP, ICMP, and IGMP. Each of these protocols is described -

- **Internetworking Protocol (IP):**
    1. The Internetworking Protocol (IP) is the transmission mechanism used by the TCP/IP protocols.
    2. It is an unreliable and connectionless protocol-a best-effort delivery service. The term best effort means that IP provides no error checking or tracking.
    3. IP assumes the unreliability of the underlying layers and does its best to get a transmission through to its destination, but with no guarantees.
    4. IP transports data in packets called datagrams, each of which is transported separately. Datagrams can travel along different routes and can arrive out of sequence or be duplicated.
    5. IP does not keep track of the routes and has no facility for reordering datagrams once they arrive at their destination.

6. The limited functionality of IP should not be considered a weakness, however. IP provides bare-bones transmission functions that free the user to add only those facilities necessary for a given application and thereby allows for maximum efficiency.

- **Address Resolution Protocol:**
    1. The Address Resolution Protocol (ARP) is used to associate a logical address with a physical address.
    2. On a typical physical network, such as a LAN, each device on a link is identified by a physical or station address, usually imprinted on the network interface card (NIC).
    3. ARP is used to find the physical address of the node when its Internet address is known.
- **Reverse Address Resolution Protocol:**
    1. The Reverse Address Resolution Protocol (RARP) allows a host to discover its Internet address when it knows only its physical address.
    2. It is used when a computer is connected to a network for the first time or when a diskless computer is booted.
- **Internet Control Message Protocol:**
    1. The Internet Control Message Protocol (ICMP) is a mechanism used by hosts and gateways to send notification of datagram problems back to the sender.
    2. ICMP sends query and error reporting messages.
    3. Internet Group Message Protocol The Internet Group Message Protocol (IGMP) is used to facilitate the simultaneous transmission of a message to a group of recipients.

Transport Layer

1. Traditionally the transport layer was represented in TCP/IP by two protocols: TCP and UDP.
2. UDP and TCP are transport level protocols responsible for delivery of a message from a process (running program) to another process.
3. A new transport layer protocol, SCTP, has been devised to meet the needs of some newer applications.

#User Datagram Protocol:

1. The User Datagram Protocol (UDP) is the simpler of the two standard TCP/IP transport protocols.
2. It is a process-to-process protocol that adds only port addresses, checksum error control, and length information to the data from the upper layer.

#Transmission Control Protocol:

1. The Transmission Control Protocol (TCP) provides full transport-layer services to applications. TCP is a reliable stream transport protocol.
2. The term stream, in this context, means connection-oriented: A connection must be established between both ends of a transmission before either can transmit data.
3. At the sending end of each transmission, TCP divides a stream of data into smaller units called segments. Each segment includes a sequence number for reordering after receipt, together with an acknowledgment number for the segments received. Segments are carried across the internet inside of IP datagrams.

4. At the receiving end, TCP collects each datagram as it comes in and reorders the transmission based on sequence numbers.

#Stream Control Transmission Protocol:

The Stream Control Transmission Protocol (SCTP) provides support for newer applications such as voice over the Internet. It is a transport layer protocol that combines the best features of UDP and TCP.

Application Layer

3. The application layer in TCP/IP is equivalent to the combined session, presentation, and application layers in the OSI modeL Many protocols are defined at this layer.
4. It consists of HTTP,HTTPS,SMTP ,SNMP,TELNET,DNS and FTP protocol.

4.3 Comparison between OSI Model and TCP/IP Model.

OSI (Open System Interconnection)	TCP/IP (Transmission Control Protocol / Internet Protocol)
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer guarantees,the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. Follows vertical approach.	3. Follows horizontal approach.
4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.
5. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	5. TCP/IP model is, in a way implementation of the OSI model.
6. Network layer of OSI model provides both,connection oriented and connectionless service.	6. The Network layer in TCP/IP model provides connectionless service.

7. OSI model has a problem of fitting the,protocols into the model.	7. TCP/IP model does not fit any protocol.
8. Protocols are hidden in OSI model and are,easily replaced as the technology changes.	8. In TCP/IP replacing protocol is not easy.
9. OSI model defines services, interfaces and,protocols very clearly and makes clear distinction between them. It is,protocol independent.	9. In TCP/IP, services, interfaces and,protocols are not clearly separated. It is also protocol dependent.
10. It has 7 layers	10. It has 4 layers