OSI and TCP/IP model

OSI model

Established in 1947. It was first introduced in late 1970s.

An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.

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. The OSI model is not a protocol it is a model for understanding and designing a network architecture that is flexible, robust and interoperable.

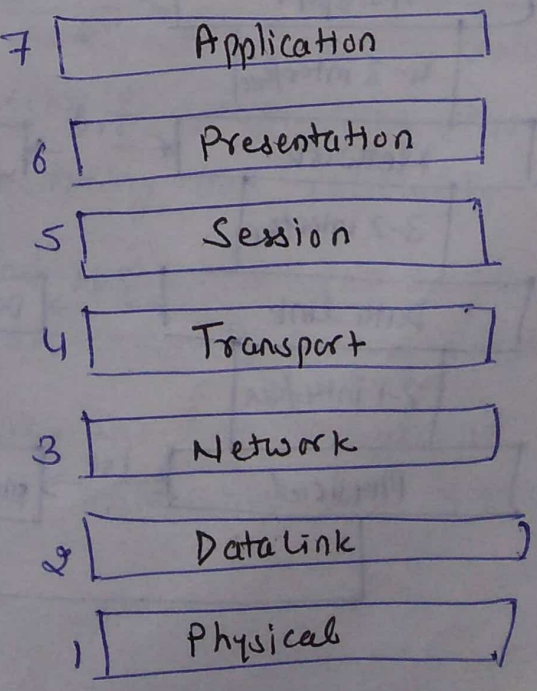
ISO (international standards organization) is the organization.

OSI (Open system interconnection) is the model.

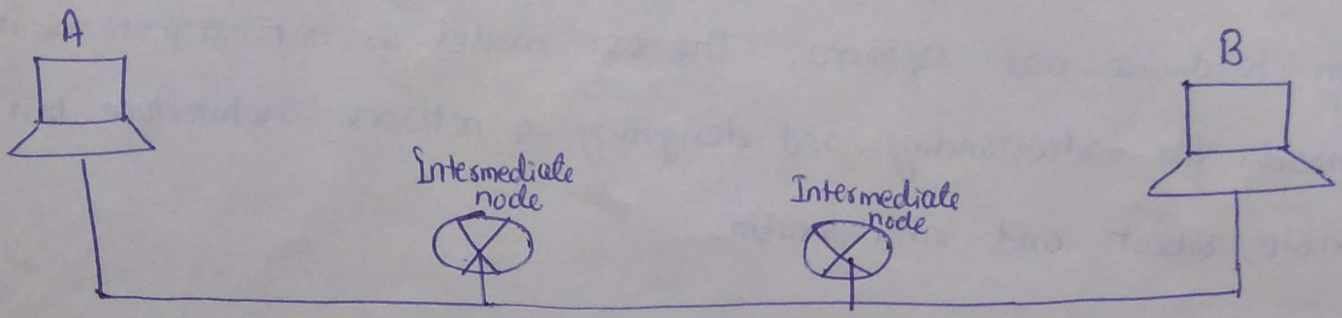
The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network.

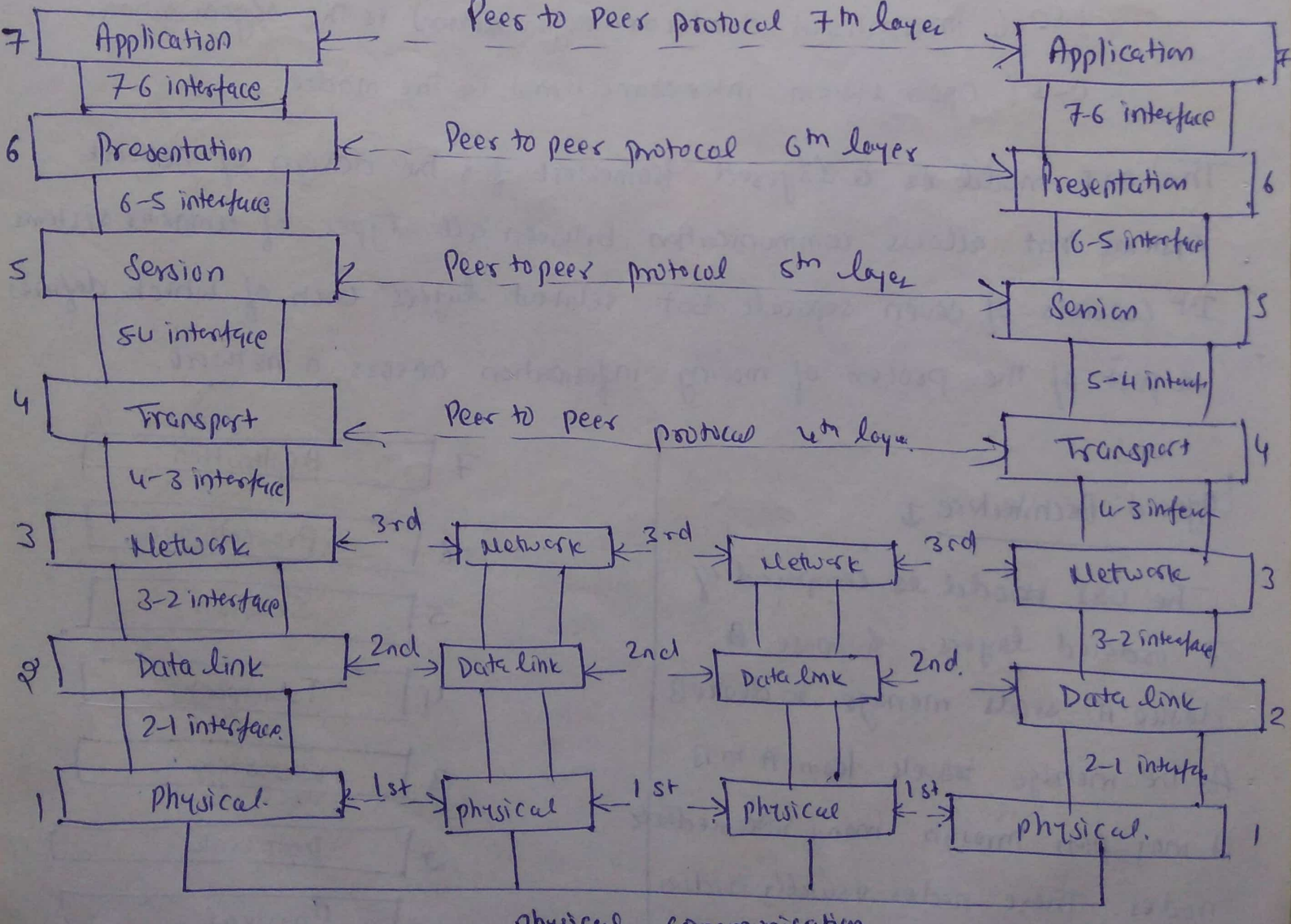
Layered Architecture

The OSI model is composed of 7 ordered layers. Suppose device A sends menage to device B As the menage travels from A to B it may pass through many intermediate nodes. These nodes usually involves only the first three layers of the OSI model.



Between machines, layer x on one machine communicates with layer x on another machine. This communication is governed by an agreed upon series of rules and conventions called protocols. The processes on each machine that communicate at a given layer are called peer to peer processes.





Each layer in the sending device adds its own information to the menage it receives from the layer just above it and passes the whole package to the layer just below it. At receiving machine, the menage is unwrapped layer by layer with each process receiving and removing the data meant for it.

Interfaces Blw Layers :

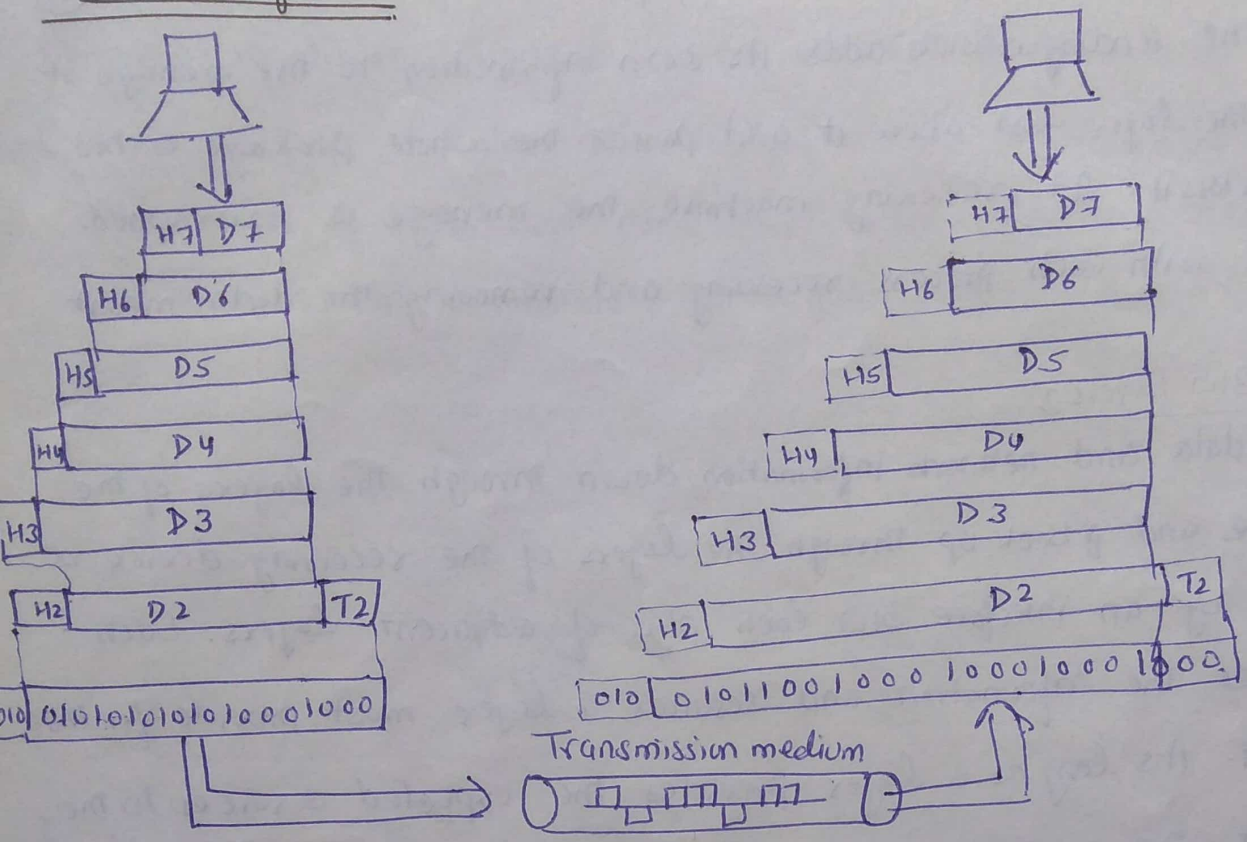
The passing of data and network information down through the layers of the sending device and back up through the layers of the receiving device is made possible by an interface blw each pair of adjacent layers. Each interface defines the information and services a layer must provide for the layer above it. 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.

Organization of layers :

The seven layers can be thought of as belonging to 3 subgroups. Layers 1, 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 addrening and transport timing and reliability.

Layers 5, 6 and 7 - session presentation and application - can be thought of as the user support layer : they allow interoperability among unrelated software systems. Layer 4 - 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.

Working of OSI



D7 means the data unit at layer 7, D6 means the data units at layers 6 and so on. The process starts at layer 7 (application layer), then moves from layer to layer in descending, sequential order. At each layer a header, or possibly, a trailer can be added to data unit. Commonly the trailer is added only at layer 2. When the formatted data unit passes through the physical layer, it is changed into an electromagnetic signal and transported along a physical link.

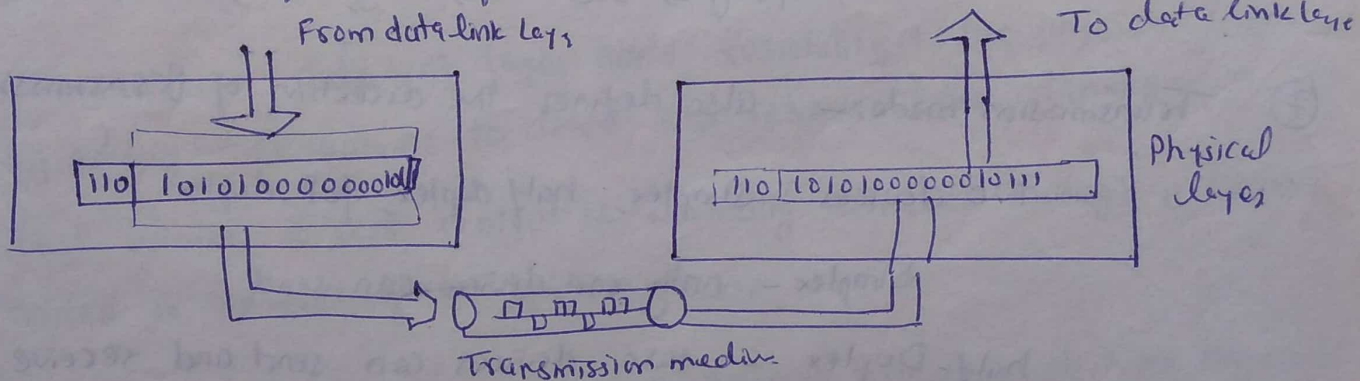
Upon reaching its destination the signal passes into layer 1 and is transformed back into digital form. The data units then move back up through the OSI layers. As each block of data reaches the next higher layer, the headers and trailers attached to it at the corresponding sending layers are removed and actions appropriate to that layer are taken. By the time it reaches layer 7, the message is again in form appropriate to the application and is made available to the recipient.

Data portion of a packet at level N-1 carries the whole packet (data and header and maybe trailer) from level N. The concept is called encapsulation.

Layers in the OSI model ↓

Physical Layer ↓

The physical layer coordinates the functions required to carry a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and transmission medium.



Physical layer is also concerned with the following:

① 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.

② Representation of bits: ↓ The physical layer data consists of a stream of bits (sequence of 0s and 1s) with no interpretation. To be transmitted, bits must be encoded into signals - electrical or optical. Layer defines type of encoding how 0s and 1s are changed into signals.

(3) Data rate :- transmission rate the no of bits sent each second is also defined by the physical layer.

(4) Synchronization of bits :- The sender and receiver not only must use the same bit rate but also must be synchronized at the bit level. [clocks must be synchronized]

(5) Line Configuration :- 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.

(6) Physical topology :- how devices are connected to make a network. topologies are bus, Ring, star, mesh, tree, Hybrid.

(7) Transmission mode :- also defines the direction of transmission b/w two devices : simplex, half duplex, full duplex.

Simplex - only one device can send

half-Duplex - two devices can send and receive but not at same time

full-Duplex - two devices can send and receive at the same time.

Data Link Layer ↓

Transforms the physical ~~link~~ layer a raw transmission facility to reliable link. It makes physical layer appear error-free to the upper layer.

The data link layer is responsible for moving frames one hop to the next.

① Framing :- divides the stream of bits received from the network layer into manageable data units called frames.

② 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.

③ 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.

④ Error control :- data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. Error control is normally achieved through a trailer added to the end of the frame.

⑤ 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 :- The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links). 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.

If two systems are connected to the same link, there is usually no need for a network layer.

The network layer is responsible for the delivery of individual packets from the source host to the destination host.

Logical addressing:- The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the nlw 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 or a large network, the connecting devices (routers, switches) route or switch the packets to their final destination.

Transport Layer:- The transport layer is responsible for procen-to-procen delivery of the entire menage. A procen in an application program running on a host. whereas the network layer oversees source-to-destination delivery of individual packets, it does not recognize any relationship between those packets.

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

The transport layer is responsible for the delivery of a menage from one procen to another.

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 procen on one computer to a specific procen on the other. The transport layer header must therefore include a type of address called a service-point address (or port addren).
The network layer gets each packet to the correct computer; the transport layer gets the entire menage to the correct process on that computer.

Segmentation and reassembly:- A message is divided into transmittable segments, with each segment containing a sequence number. These no. enable the transport layer to reassemble the menage 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 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 data are transferred the connection is terminated.

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

Error Control :-

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 → The services provided by the first three layers are not sufficient for some process. The session layer is the network dialog controller. It establishes, maintains and synchronizes the interaction among communicating systems.

The session layer is responsible for dialog control and synchronization.

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 or full-duplex mode.

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

Presentation Layer :- The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems

Translation:- The processes 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.

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 menage out over the network. Decryption reverses the original process to transform the menage back to its original form.

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 vedio.

Application layer:- The application ~~layer~~ layer enables the user whether human or software to access the network. 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.

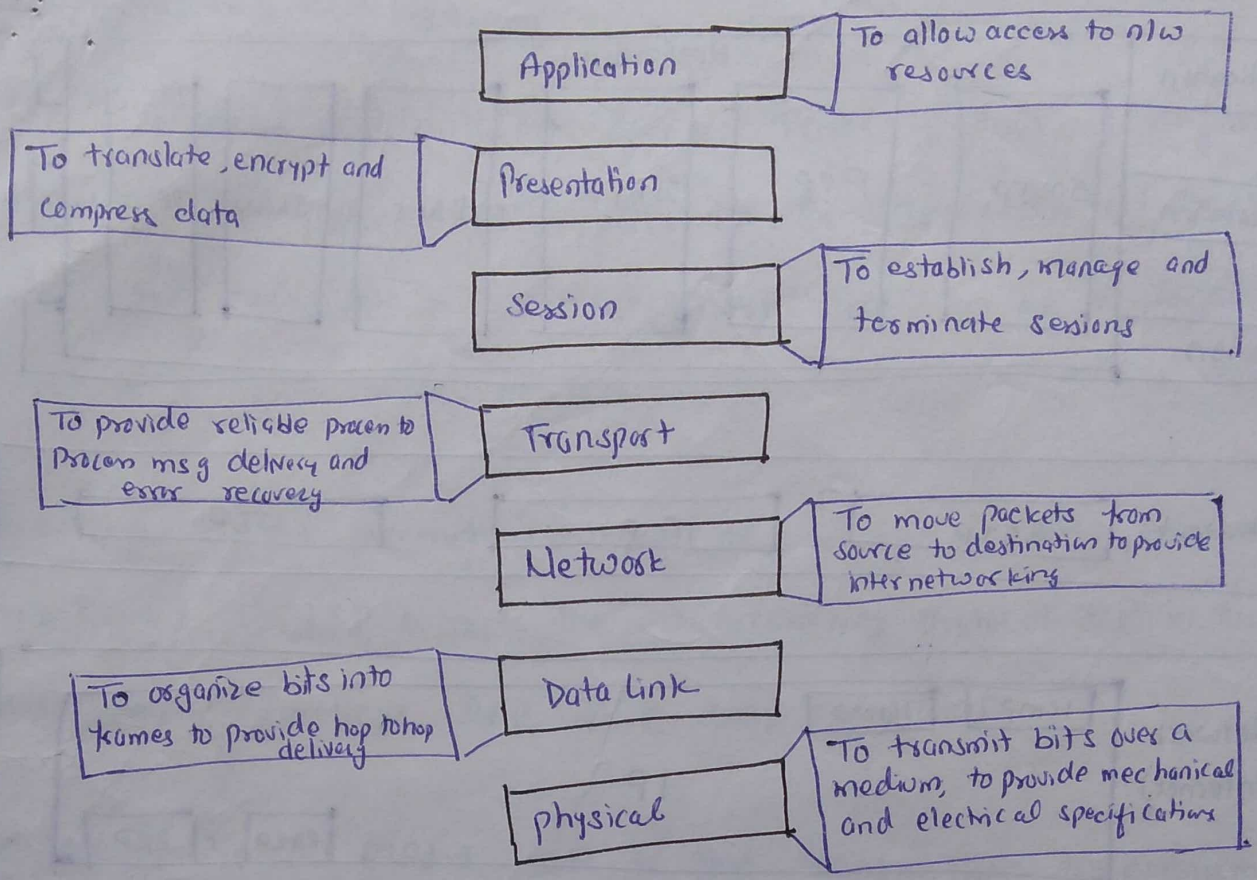
The application layer is responsible for providing services to the user.

Network virtual terminal:- A network virtual terminal is a s/w version of a physical terminal and it allows a users to log on to a remote host.

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.

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

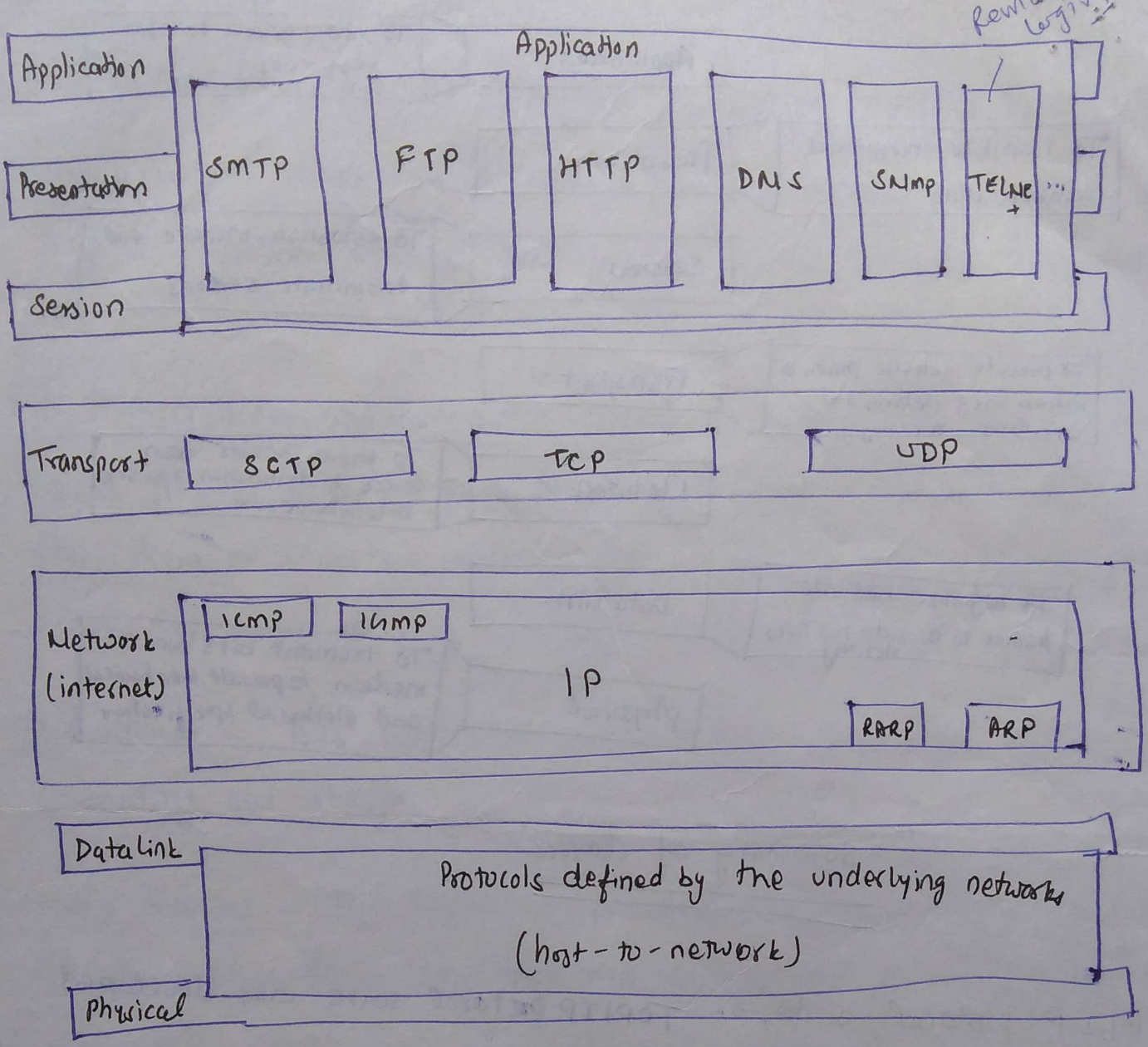
Directory services:- This application provides ~~the basis for e-mail forwarding~~ distributed database sources and access for global information about various objects and services.



Summary of layers

TCP/IP protocol suite → 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. TCP/IP protocol suite is made of 5 layers: physical, data link, network, transport and application. The first 4 layers provide physical standards, network interfaces, internetworking and transport functions that correspond to the first 4 layers of the OSI model. The 3 topmost layers in the OSI model however, are represented in TCP/IP by a single layer called the application layer.

Simple nlw management Protocal



TCP/IP is a hiesarchical protocal made up of interactive modules, each of which provides a specific functionality however the modules are not necessarily interdependent. Whereas the OSI model specifies which functions belong to each of its layers, the layers of the 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 protocal is supported by one or more lower-level protocals.

Physical and data link layer →

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

Network Layer — At the network layer (or, more accurately, the internet work layer), TCP/IP supports the internetworking protocol. IP in turn uses 4 supporting protocols: ARP, RARP, ICMP and IGMP.

Internetworking Protocol (IP) → IP is the transmission mechanism used by the TCP/IP protocols. 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. IP assumes the unreliability of the underlying layers and does its best to get a transmission through to its destination, but with no guarantees.

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. IP does not keep track of the routes and has no facility for reordering datagrams once they arrive at their destination.

Address ~~Resolution~~ resolution Protocol:- ARP is used to associate a logical address with a physical address. On a typical physical network such as LAN, each device on a link is identified by a physical or station address, usually imprinted on the network interface card. ARP is used to find the physical address of the node when its internet address is known.

Reverse Address Resolution Protocol :-

RARP allows a host to discover its internet address when it knows only its physical address. 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 :- ICMP is a mechanism used by hosts and gateways to send notification of datagram problems back to the sender. ICMP sends query and error reporting messages.

Internet Group message Protocol:- IGMP is used to facilitate the simultaneous transmission of a message to a group of recipients.

Transport Layer → Transport layer was represented in TCP/IP by two protocols: TCP and UDP. IP is host-to-host protocol, meaning that it can delivery a packet from one physical device to another. UDP and TCP are transport level protocols responsible for delivery of a message from a process (running program) to another process.

User datagram Protocol:- UDP is the simplest of the two standard TCP/IP transport protocols. It is 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:- TCP provides full transport-layer services to applications. TCP is a reliable stream transport protocol. 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. 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 acknowledgement number for the segments received. Segments are carried across the internet inside of IP datagram. At the receiving end, TCP collects each datagram as it comes in and reorders the transmission based on sequence number.

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

Application Layer:- The application layer in TCP/IP is equivalent to the combined session, presentation, and application layers in the OSI model.

User datagram Protocol:- UDP is the simplest of the two standard TCP/IP transport protocols. It is 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:- TCP provides full transport-layer services to applications. TCP is a reliable stream transport protocol. 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. 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 acknowledgement number for the segments received. Segments are carried across the internet inside of IP datagram. At the receiving end, TCP collects each datagram as it comes in and reorders the transmission based on sequence number.

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

Application Layer:- The application layer in TCP/IP is equivalent to the combined session, presentation, and application layers in the OSI model.