Unit 2. Network Model

Design Issues of Layers:-

1. **Addressing:** Mechanism for identifying senders and receivers, on the network need some form of addressing. There are multiple processes running on one machine. Some means isneeded for a process on one machine to specify with whom it wants to communicate.
2. **Termination of Connection:** When the connection is not needed it should be terminated. That is why there should be mechanism available to terminate the connection.
3. **Data transfer:** There are the some rules for data transfer. These rules should be present in the design issue. Data transfer may be simplex, half duplex or may be full duplex.
4. **Error Control:** There may be erroneous transmission due to several problems during communication. These are due to problem in communication circuits, physical medium, due to thermal noise and interference. Many error detecting and error correcting codes are known, but both ends of the connection must agree on which one being used. In addition, the receiver must have some mechanism of telling the sender which messages have been received correctly and which has not.
5. **Flow control**: If there is a fast sender at one end sending data to a slow receiver, then there must be flow control mechanism to control the loss of data by slow receivers. There are several mechanisms used for flow control such as increasing buffer size at receivers, slow down the fast sender, and so on. Some process will not be in position to accept arbitrarily long messages. Then, there must be some mechanism to disassembling, transmitting and then reassembling messages.
6. **Multiplexing / demultiplexing**: If the data has to be transmitted on transmission media separately, it is inconvenient or expensive to setup separate connection for each pair of communicating processes. So, multiplexing is needed in the physical layer at sender end and demultiplexing is need at the receiver end.
7. **Routing:** When data has to be transmitted from source to destination, there may be multiple paths between them. An optimized (shortest) route must be chosen. This decision is made on the basis of several routing algorithms, which chooses optimized route to the destination.
8. **Connection Oriented and Connectionless Services:**

Layers can offer two types of services namely connection oriented service and connectionless service.

Connection oriented service:

The service user first establishes a connection, uses the connection and then releases the connection. Once the connection is established between source and destination, the path is fixed.

Connectionless Services:

In this type of services, no connection is established between source and destination. Here there is no fixed path.

9. To reduce design complexity, most networks are organized as a series of levers or levels. Each one built upon the one below it.
10. The number of layers, the name of layer, the contents of each layer, and the function of each layer is different from network to network.
11. The function of each layer is to provides the services to the layer above it. The active elements in each layer are often called entities. The entity may be software entity or hardware entity.

Protocol Hierarchies:-

1. To reduce their design complexity, most networks are organized as a stack of layers or levels, each one built upon the one below it.
2. The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network. The purpose of each layer is to offer certain services to the higher layers, shielding those layers from the details of how the offered services are actually implemented. In a sense, each layer is a kind of virtual machine, offering certain services to the layer above it.
3. The fundamental idea is that a particular piece of software (or hardware) provides a service to its users but keeps thedetails of its internal state and algorithms hidden from them.
4. Layer n on one machine carries on a conversation with layer n on another machine. The rules and conventions used in this conversation are collectively knownas the layer n protocol.

5.Basically, a protocol is an agreement between the communicating parties on how communication is to proceed.

6.A five-layer network is illustrated in Fig.

7.The entities comprising thecorresponding layers on different machines are called peers. The peers may be processes, hardware devices. In other words, it is the peers that communicate by using the protocol.

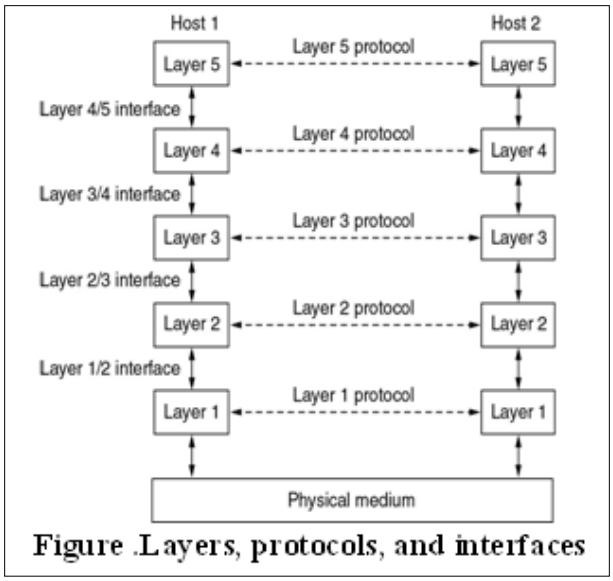


Figure .Layers, protocols, and interfaces

8. In reality, no data are directly transferred from layer n on one machine to layer n on another machine. Instead, each layer passes data and control information to the layer immediately below it, until the lowest layer is reached. Below layer 1 is the physical medium through which actual communication occurs.

9. In Fig., virtual communication is shown by dotted lines and physical communication by solid lines.

10. Between each pair of adjacent layers is an interface. The interface defines which primitive operations and services the lower layer makes available to the upper one. When networkdesigners decide how many layers to include in a network and what each one should do, one of the most important considerations is defining clean interfaces between the layers.

11. A set of layers and protocols is called network architecture. The specification of architecture must contain enough information to allow an implementer to write the program or build the hardware for each layer so that it will correctly obey the appropriate protocol.

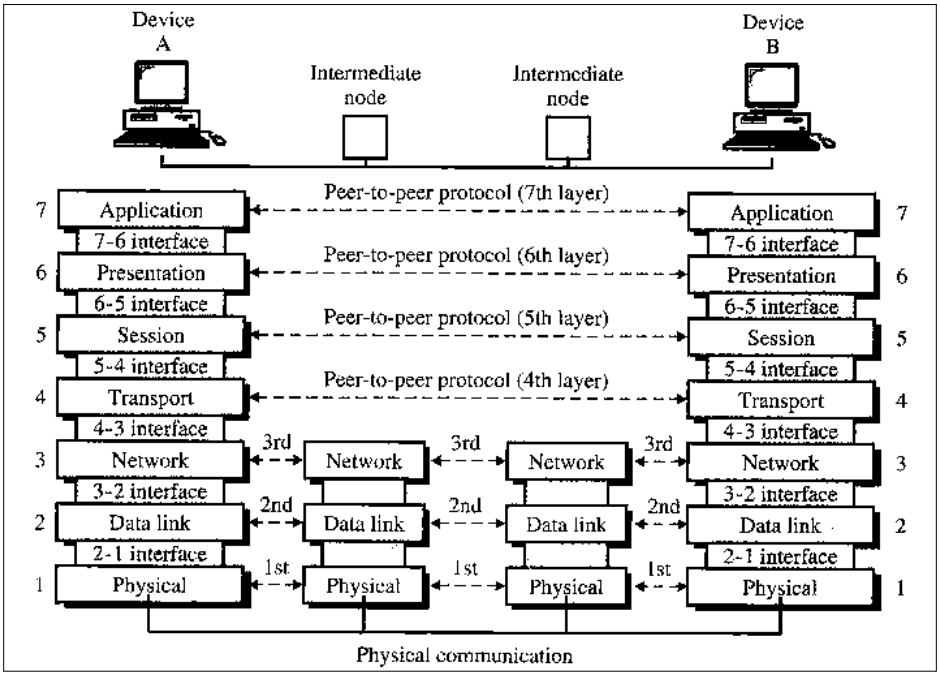
12. A list of protocols used by a certain system, one protocol per layer, is called a protocol stack.

13. Now let's consider the technical example of 7-layer network. A message M is produced by Host A in layer 7. The message M is passed from layer 7 to layer 6 according to definition of layer 6/7 interface. Layer 6 transforms the message in certain ways for example text compression. Then it passes the new message M to layer 5 across layer 5/6 interface. Layer 5 just regulates the direction of flow.

14. In many networks, layer 4 does not have restrictions or limits to the size of the message. But layer 3 may have limits. So layer 4 breaks up the message into smaller units, by writing a header to each unit. Header allows reconnecting the message in the original form at distinction machine. Header contains the sequence

The OSI Reference Model

The OSI model is based on a proposal developed by the International Standards Organization as a first step towards international standardization of the protocols used in the various layers. The model is called the ISO – (International Standard Organization – Open Systems Interconnection) Reference Model because it deals with connecting open systems – that is, systems that follow the standard are open for communication with other systems, irrespective of a manufacturer.



The OSI model has seven layers shown in Figure.

The principles that were applied to arrive at the seven layers are as follows:

1. Each layer should perform a well-defined function.
2. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
3. The layer boundaries should be chosen to minimize the information flow across the interfaces.

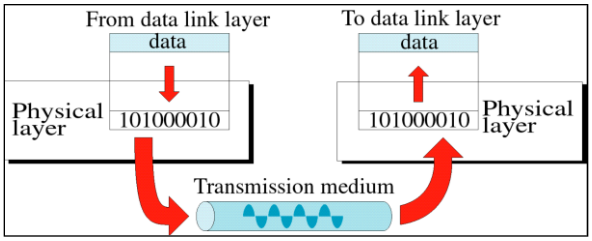
The set of rules for communication between entities in a layer is called protocol for that layer

1) Physical layer: -

i. It is the bottom layer of OSI Model.
ii. It is responsible for the actual physical connection between the devices. Such physical connection may be made by using twisted pair cable.

Function:-

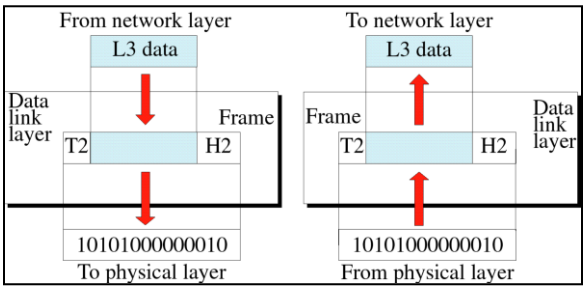
a) **Physical characteristics of interfaces and media: -** Defines type of transmission medium.
b) **Data (bit) representations**: - Data consists of bit stream (0's and 1's). To be transmitted bits must be encoded into signals-electrical or optical. The physical layer defines the type of encoding



c) **Data rate**:- It defines the transmission rate(number of bits sent per seconds)
d) **Synchronization of bits**: - Provides synchronization of bits by a clock i.e sender and receiver clock must be synchronized
e) **Physical Topology**:- It defines how devices are connected to make a network. For example:- star, ring, bus etc.
f) **Transmission mode**:- It defines the direction of transmission For example:-simplex,half-duplex, full-duplex
g) **Transmission medium**: - It defines the type of transmission media for ex: - wire cable, optical cable, microwave, telephone line.

2) Data Link Layer: - It is responsible for node-to-node delivery of data.

i. It receives the data from network layer and creates FRAMES, add physical address to these frames & pas them to physical layer
ii. It consist of 2 layers: Logical Link Layer (LLC) : Defines the methods and provides addressing information for communication between network devices.
iii. Medium Access Control (MAC): establishes and maintains links between communicating devices.

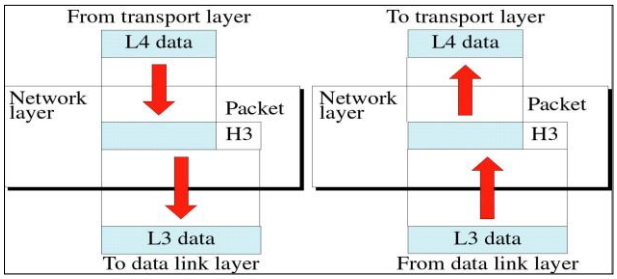


Function:-

a) **Framing**: DLL divides the bits received from N/W layer into frames. (Frame contains all the addressing information necessary to travel from S to D).
b) **Physical addressing**: After creating frames, DLL adds physical address of sender/receiver (MAC address) in the header of each frame.
c) **Flow Control**: DLL prevents the fast sender from drowning the slow receiver.
d) **Error Control**: - It adds reliability to the physical layer by adding mechanism to detect and retransmit damaged or lost frames. It also prevents duplication of frames.
e) **Access control**:- When two or more devices are connected to the same link, data link layer protocols determines which device has control over the link at any given time.

3) Network Layer:-

i. It is responsible for the source to destination delivery of a packet across multiple networks.



ii. If two systems are attached to different networks with devices like routers, then N/W layer is used.

iii. Thus DLL overseas the delivery of the packet between the two systems on same network and the network layer ensures that the packet gets its point of origin to its final destination.

Functions of Network Layer

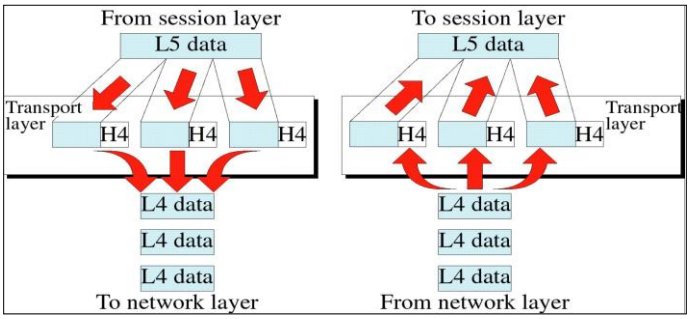
a) **Internetworking**: It provides Internetworking.

b) **Logical Addressing**: When packet is sent outside the network, N/W layer adds Logical (network) address of the sender & receiver to each packet. Network addresses are assigned to local devices by n/w administrator and assigned dynamically by special server called DHCP (Dynamic Host Configuration Protocol)

c) **Routing**: When independent n/w is connected to create internetwork several routes are available to send the data from Source to Destination. This n/w is interconnected by routers & gateways that route the packet to final destination.

4) Transport Layer

i) It is responsible for process-to-process delivery of the entire message.



ii) TL looks after the delivery of entire message considering all its packets & make sure that all packets are in order. On the other hand n/w layer treated each packet independently.

iii) At the receiver side, TL provides services to application layer & takes services form n/w layer.

iv) At the source side, TL receives message from upper layer into packets and reassembles these packets again into message at the destination.

v) Transport Layer provides two types of services:

(1) Connection Oriented Transmission: In this type of transmission the receiving devices sends an acknowledge back to the source after a packet or group of packet is received. It is slower transmission method.

(2) Connectionless Transmission: In this type of transmission the receiving devices does not sends an acknowledge back to the source. It is faster transmission method.

Functions of Transport Layer

a) **Segmentation and Reassemble:-**Segmentation of message into packet & reassembly of packets into message.

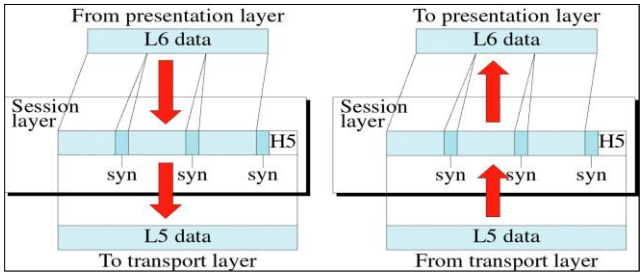
b) **Port addressing**: Computers run several processes. TL header includes a port address with each process.

c) **Flow Control**: Flow control facility prevents the source form sending data packets faster than the destination can handle.

d) **Error control**: TL ensures that the entire message arrives at the receiving TL without error.

5) Session Layer

i. It has the responsibility of beginning, maintaining and ending the communication between two devices, called session.



ii. It also provides for orderly communication between devices by regulating the flow of data.

Functions of Session Layer

a) **Establishing, Maintaining and ending a session:** When sending device first contact with receiving device, it sends syn (synchronization) packet to establish a connection & determines the

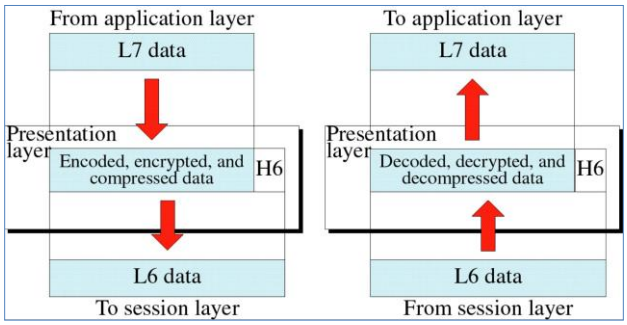
order in which information will be sent. Receiver sends ack (acknowledgement). So the session can be set & end.

b) **Dialog Control**: This function determines that which device will communicate first and the amount of data that will be sent.

c) **Dialog separation**: Process of adding checkpoints & markers to the stream of data is called dialog separation.

6) Presentation Layer

i. It is concerned with the syntax & semantics of the information exchanged between the two devices.



ii. It was designed for data encryption, decryption and compression.

Functions of Presentation Layer

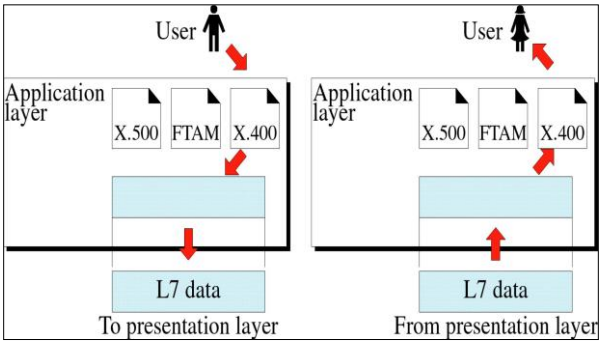
b) **Data Presentation or Translation**: Because different computers use different encoding systems. It ensures that the data being sent is in the format that the recipient can process.

c) **Data Encryption**: PL provides this facility by which hides the information from everyone except the person who originally sent the information & the intended recipient. When encrypted data arrives at destination, PL decrypts the message.

d) **Data Compression**: PL shrinks large amount of data into smaller pieces i.e. it reduces the size of data.

7) Application Layer

i. It enables the user to access the network.



ii. It provides user interface & supports for services such as e-mail, file transfer, access to the World Wide Web.

iii. So it provides services to different user applications.

Functions of Application Layer

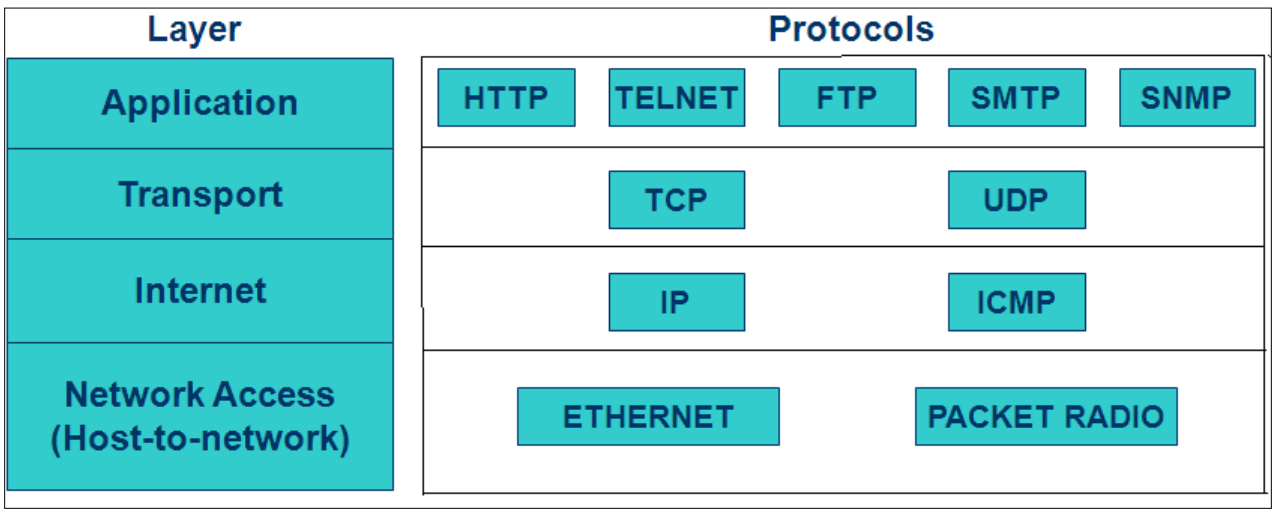
b) Mail Services: This application provides various email services.

c) File transfer & Access: It allows users to access files in a remote host, to retrieve files from remote computer for use etc.

d) Remote log-in: A user can log into a remote computer and access the resources of that computer.

e) Accessing the World Wide Web: Most common application today is the access of the World Wide Web

TCP/IP Reference Model:-



1) The late-60s The Defense Advance Research Projects Agency (DARPA) originally developed Transmission Control Protocol/Internet Protocol (TCP/IP) to interconnect various defense department computer networks.
2) The Internet, an International Wide Area Network, uses TCP/IP to connect networks across the world.
3) The TCP/IP layer has four Layer model which are as follows:

a) **The network access layer**

i) Concerned with all of the issues that an IP packet requires to actually make the physical link. All the details in the OSI physical and data link layers.
(1) Electrical, mechanical, procedural and functional specifications.
(2) Data rate, Distances, Physical connector.
(3) Frames, physical addressing.
(4) Synchronization, flow control, error control.

ii) Protocol Used in Internet layer:-
(1) Ethernet
(a) Uses CSMA/CD
(2) Token Ring

b) **The internet layer.**

i) Send source packets from any network on the internetwork and have them arrive at the destination independent of the path and networks they took to get there.
(1) Packets, Logical addressing.
(2) Internet Protocol (IP).
(3) Route , routing table, routing protocol

ii) **Protocol** :-
(1) IP:-
(a) Path selection
(b) routing and addressing
(2) ICMP (Internet Control Message Protocol)
(a) sends error messages relying on IP
(b) a requested service is not available
(c) a host or router could not be reached

c) Transport Layer:-

i) The transport layer deals with the quality-of-service issues of reliability, flow control, and error correction.
(1) Segments, data stream, datagram.
(2) Connection oriented and connectionless.
(3) Transmission control protocol (TCP).
(4) User datagram protocol (UDP).
(5) End-to-end flow control.
(6) Error detection and recovery.
(7) Allows end-to-end communication
(8) Connection establishment, error control, flow control
(9) Two main protocols at this level
(i) Transmission control protocol (TCP),
1. Connection oriented
a. Connection established before sending data

b. Reliable

(ii) user datagram protocol (UDP)

1. Connectionless

a. Sending data without establishing connection
b. Fast but unreliable

d) Application Layer:-

i) Handles high-level protocols, issues of representation, encoding, and dialog control.

ii) The TCP/IP combines all application-related issues into one layer, and assures this data is properly packaged for the next layer.

(1) FTP, HTTP, SMNP, DNS ...
(2) Format of data, data structure, encode …
(3) Dialog control, session management

iii) Protocols at the application layer

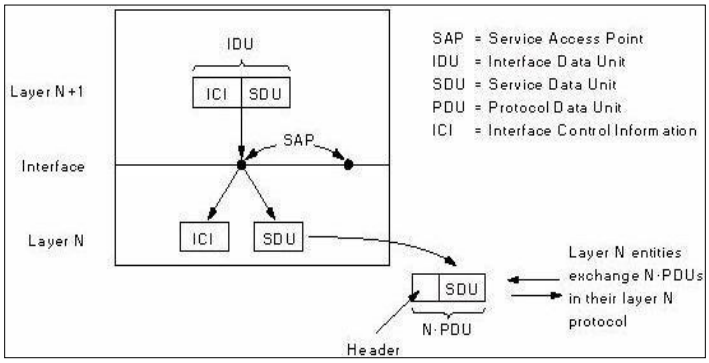
(1) HTTP:
(a) Browser and web server communication.
(2) FTP :
(a) file transfer protocol
(3) TELNET:
(a) remote login protocol
(4) POP3: Retrieve email
(a) POP3 is designed to delete mail on the server as soon as the user has downloaded it
(b) IMAP (Internet Message Access Protocol)
(c) Retrieve emails,
(d) retaining e-mail on the server and for organizing it in folders on the serve

Comparison of the OSI & the TCP/IP Reference Models

OSI Reference Model	TCP/IP Reference Model
1. Seven layers	1. Four layer
2. It distinguishes between service, interface, and protocol	2. Does not clearly distinguish between service, interface and protocol
3. Firstly description of model and protocol came next.	3. Protocol comes first and description of model later.
4. Both have Network.	4. Transport and Application layer.
5. Supports connectionless and connection oriented communication in network layer and only connection-oriented communication in transport layer.	5. TCP/IP has only one mode in Network layer (connection less) but supports both modes in Transport layer.
6. Protocol in OSI model are better hidden and can be replaced relatively easily (No Transparency)	6. Protocols in TCP/IP are not hidden and thus cannot be replaced easily (Transparency).

SAP:-

1. **Service:** - It is formally specified by a set of operations or primitives available to a user process to achieve some task.
   a. These primitives are normally system calls of the operating system.
   b. These primitives tell services to take some action or report taken by the entity.
2. **Entities**: Tea active elements in each layer are called entities. An entity can be a software entity (such as a process), or a hardware entity (such as an intelligent I/O chip).



3. **Peer entities**: Entities in the same layer on different machines.
4. **Service provider:** - It is the layer which provides the services to its upper layer.
5. **Service user**: It is the layer which uses the services to the its lower layer
    a. The entities in layer n implement a service used by layer n+1. In this case n is called the service provider and layer n+1 is called the service user.
6. **Services are available at SAPs (Service Access Points)**:- Each sap has an address that uniquely identifies. It is the pace where service provider layer offers services to service user layer. This place is nothing but the points. These points are called as the Service accesses point.
    a. **IDU (Interface Data Unit**):-At a typical interface, the layer n+1 entity passes an IDU to the layer n entity through the SAP.
        The IDU consists of an
        i. SDU (Service Data Unit):-.The SDU is the information passed across the network to the peer entity and then up to layer n+1.This is the virtual communication between the service users of sender and receiver machines. It is added as a header to data unit.
        ii. Interface control information (ICI):- It is needed to help the lower layer that means service provider to do function or services.
            A. *PDU (Protocol Data Unit):*-In order to transfer the SDU, the layer n entity may have to fragment it into several pieces, each of which is given a header and sent as separate PDU (Protocol Data Unit) such as a packet. The PDU headers are used by the peer entities to carry out their peer protocol. They identify which PDUs contain data and which contain control information, provide sequence numbers and counts. Generally it identify
                I. Information: - Using which its peer entity can assemble the packets into one message.
                II. It is also has the information passed to peer entity through which it can perform virtual communication.

Connection-oriented and Connection less services:-

A) Connection –oriented Services

1.Connection-oriented services must first establish a connection between the two end-points (sending/receiving) before passing any data traffic between them.
2. An example of a connection-oriented service is Frame Relay, where a VC (virtual connection) is required between both end-points before data traffic can be exchanged.
3.Connection-oriented service involves three phases:
    i. **Connection establishment**: - A sender wants the service to do some communication. Here entity invokes service provider to do some function by this primitive. That function may be either established the connection or send the data. That means it sends request for to establish connection.
    ii. **Data transfer**: - Sender is connected with the receiver and now they can exchange their information using the connection between them.
    iii. **Connection termination**: - When the communication is the over then sender and receiver wants to terminate the connection
4.Connection-Oriented service is based on telephone. As you pick up the phone, dial the number, talk and then hang up.
5. Here the bits arrive in order. In some cases when a connection is established, the receiver, sender, and subnet conduct a negotiation about parameters to be used, such as quality of service required, as maximum message size, and other issues.
6.Each message carries the complete destination address, and is routed through the system independent of all the others. When two messages are sent to the same destination, the one sent first will be the first one to arrive but there could be a possibility that the first one sent can be delayed.

7.There are two types of connection orienteer services:-

8. A reliable service is one in which the message is never lost.

d) Reliable connection-oriented: -

i. This system gives the guarantee of data such that all the data is delivered successfully without error at receiver.

ii. It is compulsion on receiver to send acknowledgement receipt for each message during the communication.

iii. Reliable connection-oriented service will be having two variations:

A. Message sequences: - In the message sequence the message boundaries are preserved for example. If two 8-byte messages are sent, they received as two different b-byte messages and but notes one of16-byte message.

B. Byte Stream:- In the bytes stream the connection is simply a stream of bytes, with no message boundaries i.e. 2048 bytes arrive at the receiver as one

e) **Unreliable connection-oriented services**:-

i. This system does not give any guarantee of data. So here there is no compulsion on receiver to send acknowledgement receipt for each massage during the communication.

9. Advantages:

a.Buffers can be reserved in advance

b.Sequencing can be guaranteed**.**

c.Short headers**.**

10. **Disadvantages:**

a.No alternate routing around congestion**.**

b.Vulnerability to router failures along the path**.**

c.Requirement of table spaces at the routers**.**

d.Difficult to implement if one of the networks involved is an unreliable datagram network**.**

B) Connectionless Services:-

1. Connectionless services can send data without requiring an established connection
2. This system is similar to the poster system. Each message is carrying full address of the destination.
3. Each message is routed or travels independently. Because of this reason there may be possibility that the message go out of order at the receiver side.
4. In this method virtual connection is established in between sender and the receiver.
5. It uses packets switching techniques are many switching offices which can establishing between the sender and receiver
   a. In packet switching techniques there are many switching offices which can establish physical connection between them and root the packets.
   b. Each packet has full address of destination. So they can travels independently from one office to another office.
   c. These packets are referred as a datagram.

6. Connectionless Services has two types:-

Electronic junk mail (third class mail as advertisements) - this service is moreover unreliable (meaning not acknowledged). Such connectionless services are often called datagram services.

a. **Acknowledged datagram services** - connectionless datagram services with acknowledgment.
b. **Request-reply service** - the sender transmits a single datagram containing a request. The reply contains the answer. Request-reply is commonly used to implement communication in the client-server model.

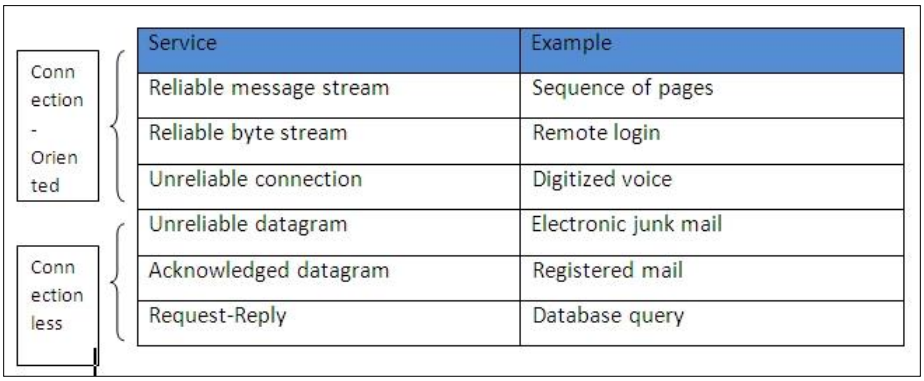
7.Advantages:

a. Can be used to connect subnets without VC's inside**.**
b. Robust to router failures**.**
c. More potential for adapting congestion

8. Disadvantages:

a. No sequencing**.**
b. Longer headers**.**

Six different types of Services:



	Service	Example
Connection-Oriented	Reliable message stream	Sequence of pages
	Reliable byte stream	Remote login
	Unreliable connection	Digitized voice
Connectionless	Unreliable datagram	Electronic junk mail
	Acknowledged datagram	Registered mail
	Request-Reply	Database query

Connection-oriented	**Connectionless**
It establishes Physical link between Sender and receiver.	There is no direct link between sender and receiver.
It follows three mode of communication: a) Establish connection. b) Data communication c) Terminate connection	Whenever sender wants to transmits data sender can transmit the data.
It is very time consuming	It is very fast.
Maximum time is required to establish the connection between the sender and the receiver and very less time is required for actual data communication.	It will not requires any connection so no time is wasting in establishing connection thus very less time is required for data transfer.
It is very costly system.	It is not costly.
Bandwidth of physical line is wasted if sender and receivers are not communicated with each other.	Bandwidth of channel is not wasted at all.
Other computers could not share the line till sender or receiver not terminates the connection.	Very small time is allocated for data transmission so line is not shared during one switching office to other switching office.
It is not required data sequencing process.	It requires data sequencing algorithms at receiver's side because data does not come sequentially.