MODULE: 1

INTRODUCTION: Data Communications: Components, Representations, Data Flow, Networks: Physical Structures, Network Types: LAN, WAN, Switching, Internet.

NETWORK MODELS: Protocol Layering: Scenarios, Principles, Logical Connections, TCP/IP Protocol Suite: Layered Architecture, Layers in TCP/IP suite, Description of layers, Encapsulation and Decapsulation, Addressing, Multiplexing and Demultiplexing, The OSI Model: OSI versus TCP/IP.

DATA-LINK LAYER: Introduction: Nodes and Links, Services, Categories of link, Sublayers, Link Layer addressing: Types of addresses, ARP. Data Link Control(DLC) services: Framing, Flow and Error Control, Data Link Layer Protocols: Simple Protocol, Stop and Wait protocol, Piggybacking.

INTRODUCTION :

DATA COMMUNICATIONS:-

During communication we are sharing information. This sharing can be local or remote. Local communication usually occurs face to face, while remote communication takes place over a distance.

The word "data" refers to information presented in whatever form is agreed upon by the parties creating and using the data.

Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable.

For effective communication, communicating devices must be a part of communication systems made up of a combination of hardware and software. Effectiveness of data communication depends of four fundamen-tal characteristics. They are:-

(i) Delivery : The system must deliver data to correct distination. Data must be recieved by the intended device or user.

(ii) Accuracy : The system must deliver the data accurately.

(iii) Timliness : System must deliver data in timely manner. Data delivered late are useless. In case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, without significant delay. This kind of delivery is called real-time transmission

(iv) Jitter: Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets.

Components:-

A data communication system has five components.

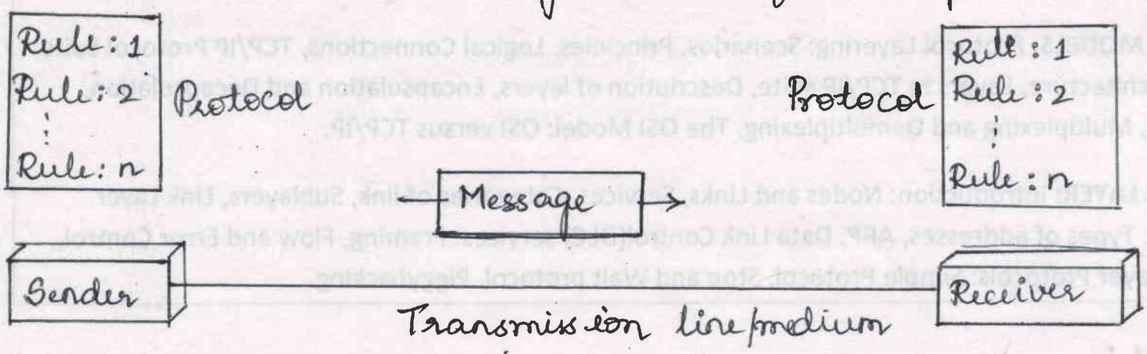


Figure 1.1: Five components of data Communication.

(i) Message:

The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio and video.

(ii) Sender:

The sender is the device that sends the data message. It can be computer, work station, telephone handset, video camera and so on.

(iii) Receiver:

The reciever is the device that receives the message. It can be a computer, workstation, telephone handset, television and so on.

(iv) Transmission medium:

The transmission medium is the physical path by which a message travels from sender to receiver. Transmission medium include twisted-pair wire, coaxial cable, fiber optic cable and radio waves.

(v) Protocol:

A protocol is a set of rules that govern data communication. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating.

Representations:-

The information comes in different forms such as text, numbers, images audio and video.

(i) Text :

Text is represented as a 'bit' pattern, a sequence of bits (0_s or 1_s) Different sets of bits patterns have been designed to represent text symbols. Each set is called 'code', and process of representing symbols is called 'coding'.

→ Prevalent coding system is called 'Unicode', which uses 32 bits to represent a symbol or character used in any language.

The 'American Standard Code for Information Interchange (ASCII)' constitutes of 127 characters in Unicode and is referred to as 'Basic Latin'

(ii) Numbers :

Numbers are also represented by bit patters. The number is directly converted to a binary number to simplify mathematical operations.

(iii) Images:

Images are also represented by bit patterns. In its simplest form, an image is composed of a matrix of pixels (picture elements), where each pixel is a small dot. The size of the pixel depends on the resolution.

After an image is divided into pixels, each pixels are assigned a pattern (bit). The size and value of the pattern depend on image.

There are several methods to represent color images. One method is called RGB, each color is made of a combination of three primary colors: red, green and blue. Another method is called YCM, in which the color is made of combination of three colors: yellow, cyan and magenta.

(iv) Audio :

Audio refers to recording or broadcasting of sound or music. It is continuous, not discrete. Even when we use microphone to change voice or music to an electrical signal, we create a continuous signal.

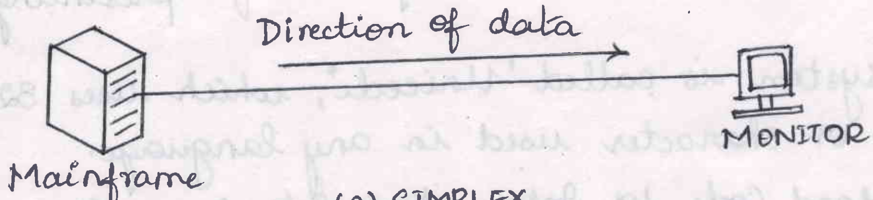
(v) Video :

Video refers to recording or broadcasting of a picture or movie. Video can either be produced as a continuous entity, or it can be a combination of images, each a discrete entity, arranged to convey the idea of motion.

Data Flow :-

Communication between two devices can be simplex, half-duplex or full-duplex as shown in figure.

(i) Simplex :



(a) SIMPLEX

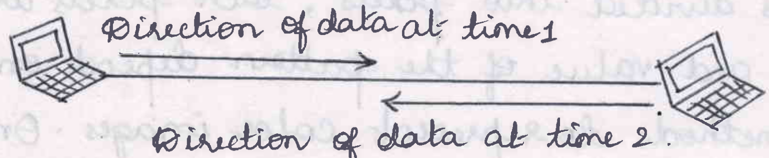
Simplex mode communication is unidirectional; Only one of the two devices on a link can transmit; other can only recieve.

Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output.

The simplex mode can use the entire ~~capatic~~ capacity of the channel to send data in one direction.

(ii) Half-Duplex:

(b) Half-duplex



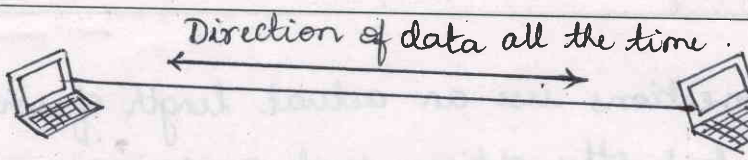
In half-duplex mode, each station can both transmit and recieve, but not at same time. When one device is sending, the other can only recieve and vice-versa.

In half-duplex transmission, the entire capacity of a channel is taken over by which of the two devices is transmitting at the time. Walkie-talkies and CB(citizens band) radios are both half-duplex systems.

The half-duplex mode is used in cases where there is no need for communication in both directions at the same time; the entire capacity of the channel can be utilized for each direction.

(iii) Full-Duplex :

In full-duplex (duplex), both stations can transmit and recieve simultaneously.



(C) Full-duplex

In full-duplex mode, signals going in one direction share the capacity of the link with signals going in the other direction. This sharing can occur in two ways; either the link must contain two physically separate transmission paths, one for sending and other for receiving; or the capacity of the channel is divided between signals travelling in both directions. Example of duplex communication is telephone network.

NETWORKS:-

(i) A network is the interconnection of a set of devices capable of communication. A device can be a host such as a large computer, desktop, laptop, workstation, cellular phone, or security system.

(ii) A device can also be a connecting device such as a router, which connects the network to other networks, a switch, which connects devices together, a modem (modulator - demodulator), which changes the form of data and so on.

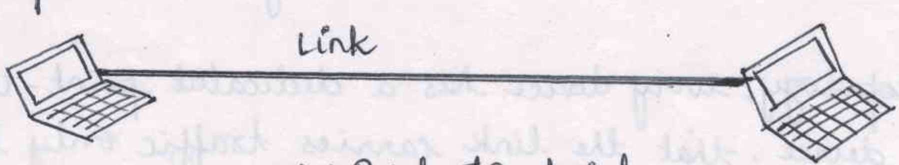
(iii) These devices in a network are connected using wired or wireless transmission media such as cable or air.

Physical Structures:-

(i) Type of connection:

A network is two or more devices connected through links. A link is a communications pathway that transfer data from one device to another. There are two possible types of communications:-

1) Point-to-point:



(a) Point-to-point.

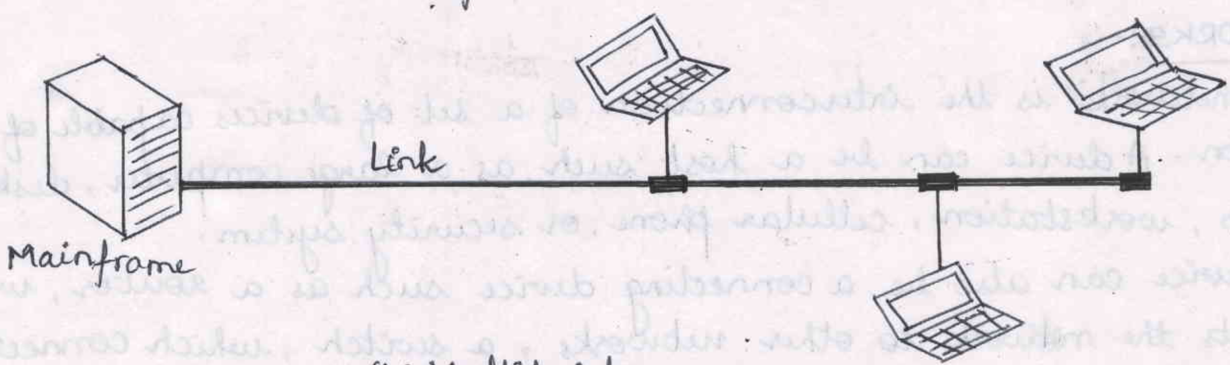
A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission

between those two devices.
Most point-to-point connections use an actual length of wire or cable to connect the two ends but other options such as microwave and satellite links are also possible.

Ex:- When we change television channels by infrared remote control, we are establishing a point-to-point connection between the remote control and the television's control system.

2) Multipoint:

A multipoint connection (multidrop) is one which more than two specific devices share a single link.



(b) Multipoint

In multipoint environment, the capacity of the channel is shared either spatially or temporally. If several devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a timeshared connection.

(ii) Physical Topology:

The term physical topology refers to the way in which a network is laid out physically. Two or more devices connect to a link; two or more links form a topology.

The topology of a network is the geometric representation of the relationship of all the links and linking devices (called nodes) to one another. There are four basic topologies possible: mesh, star, bus and ring.

1) Mesh topology:-

(i) In a mesh topology, every device has a dedicated point-to-point link to every other device, that the link carries traffic only between the two devices it connects.

(ii) To find the number of physical links in a fully connected mesh network with 'n' nodes, each node must be connected to every other node. Node 1 must be connected to (n-1) nodes, node 2 must be connected to (n-1) nodes, and finally node n must be connected to (n-1) nodes.

(iii) We need $n(n-1)$ physical links; if each physical link allows communication in both directions (duplex mode), we can divide the number of links by 2.

(iv) In a mesh topology, we need $\frac{n(n-1)}{2}$ duplex-mode links. To accomodate that many links, every device on the network must have (n-1) input/output (I/O) ports to be connected to the other (n-1) stations.

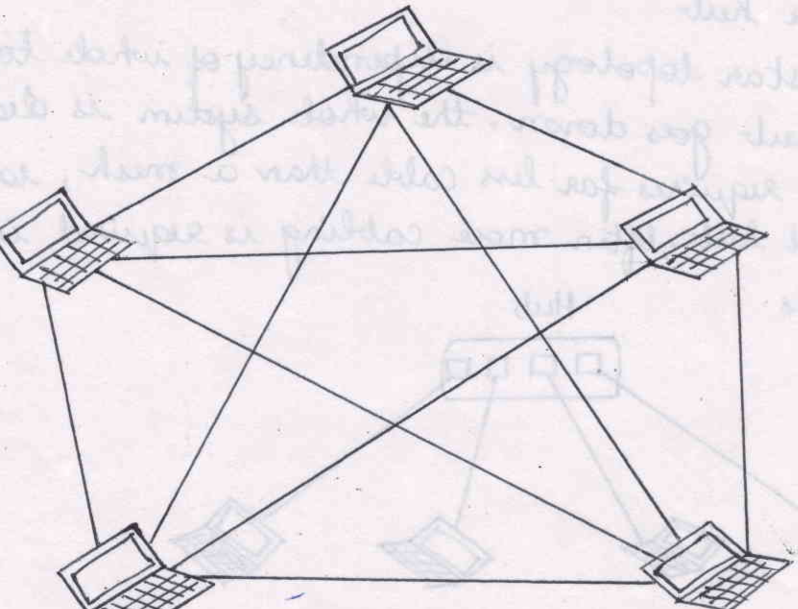
Advantages of Mesh topology:-

(i) The use of dedicated links guarantees that each connection can carry its own data load; this eliminating the traffic problems that can occur when links must be shared by multiple devices.

(ii) A mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.

(iii) There is advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages.

(iv) Point-to-point links make fault identification and fault isolation easy. Traffic can be routed to avoid links with suspected problems.



MESH. NETWORK $n = 5$
10 links.

Disadvantage of mesh topology:-

The main disadvantages of a mesh are related to the amount of cabling and the number of I/O ports required.

(i) Every device must be connected to every other device, installation and reconnection are difficult.

(ii) The sheer bulk of the wiring can be greater than the available space.

(iii) The hardware required to connect each link can be prohibitively expensive

Mesh topology is used as a backbone connecting the main computers of a hybrid network that can include several other topologies

Ex:- Mesh topology is used in the connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

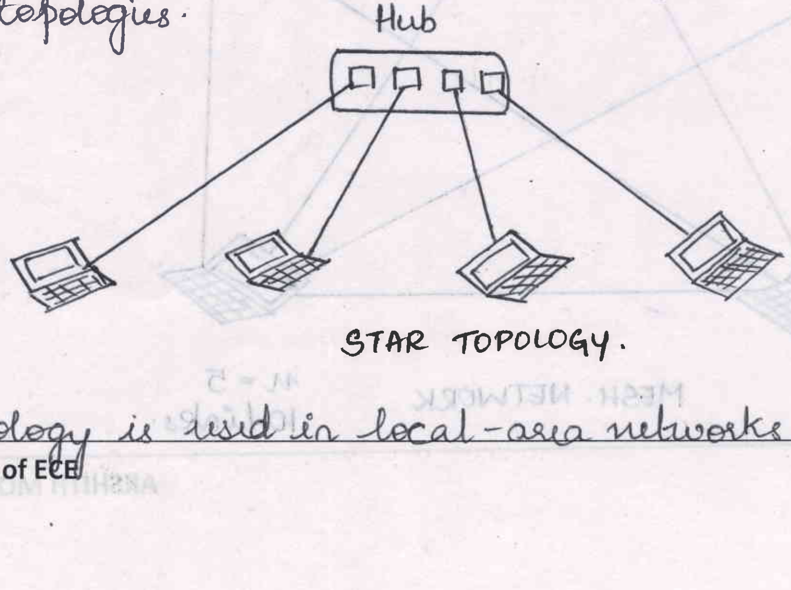
2) Star Topology:

(i) A star topology is less expensive than a mesh topology. Each device needs only one link and one I/O port to connect it to any number of others.

(ii) It is easy to install and configure. Less cabling needs to be housed and additions, moves, deletions involve only one connection: between that device and the hub

(iii) Disadvantage of star topology is dependency of whole topology on single point, the hub. If hub goes down, the whole system is dead.

Although a star requires far less cable than a mesh, each node must be linked to a central hub. Often more cabling is required in star than in some other topologies.

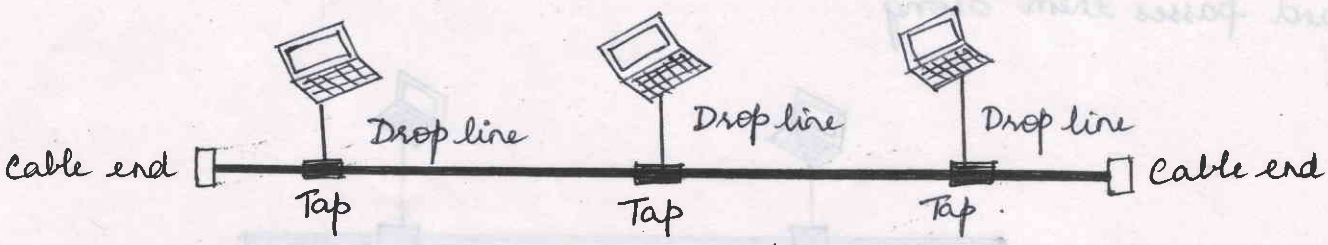


STAR TOPOLOGY.

Ex:- Star topology is used in local-area networks (LANs).

3) Bus Topology:

Bus topology has multipoint connection. One long cable acts as a backbone to link all the devices in a network.



BUS TOPOLOGY.

(i) Nodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and main cable. A tap is a connector that either splices into the main cable or punctures the sheathing ~~of a~~ to create a contact with the metallic core.

(ii) Signal travels along the backbone, some of its energy is transformed into heat. Thus, it becomes weaker and weaker as it travels farther. Thus there is a limit on the number of taps a bus can support and on the distance between the taps.

(iii) Advantages of bus topology include ease of installation. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths. Bus use less cabling than mesh or star topologies.

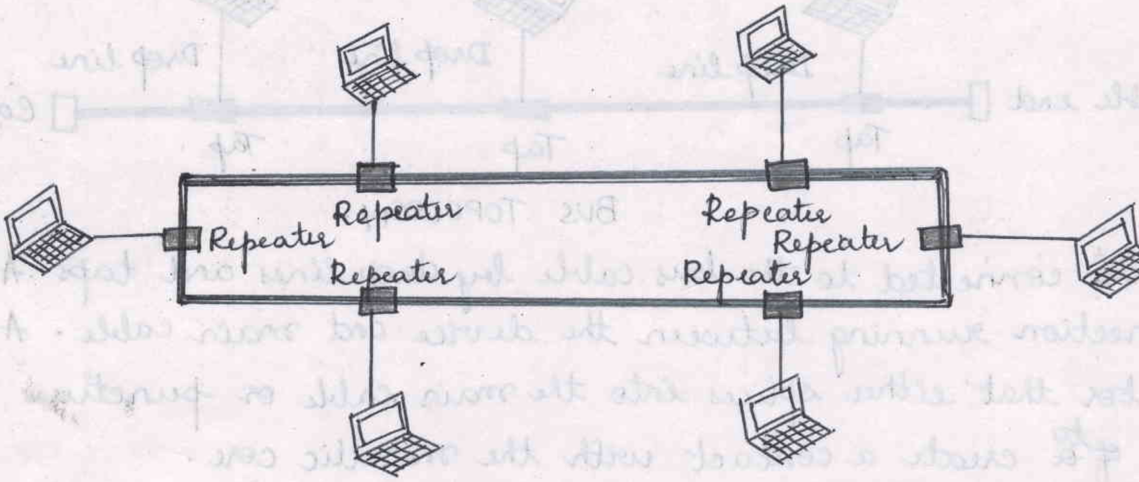
(iv) Disadvantages include difficult reconnection and fault isolation. Bus is usually designed to be optimally efficient at installation. Thus it is difficult to add new devices. Signal reflection at the taps can cause degradation in quality.

(v) A fault or break in the bus cable stops all transmission, even between devices on the same side of the problem. The damaged area reflects signals back in the direction of the ~~original~~ origin; creating noise in both directions.

4) Ring Topology:

(i) In ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device-to-device, until it reaches the destination.

(ii) Each device in a ring incorporates a repeater. when a device recieves a signal intended for another device, its repeater regenerates the bits and passes them along.



RING TOPOLOGY.

(iii) A ring is easy to install and reconfigure. Each device is linked to only its immediate neighbors. To add or delete a device requires changing only two connections.

(iv) Fault isolation is simplified. In a ring a signal is circulating at all times. If one device does not recieve a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.

(v) Unidirectional traffic is a disadvantage. In a simple ring, break in the ring can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break.

NETWORK TYPES:

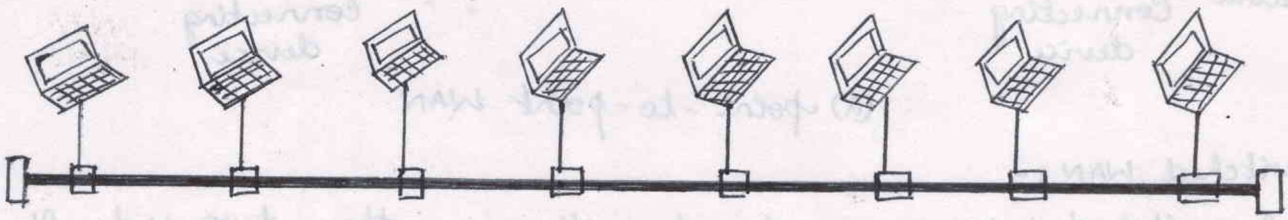
LOCAL AREA NETWORK (LAN):-

(i) A local area network (LAN) is usually privately owned and connects some hosts in single office, building or campus.

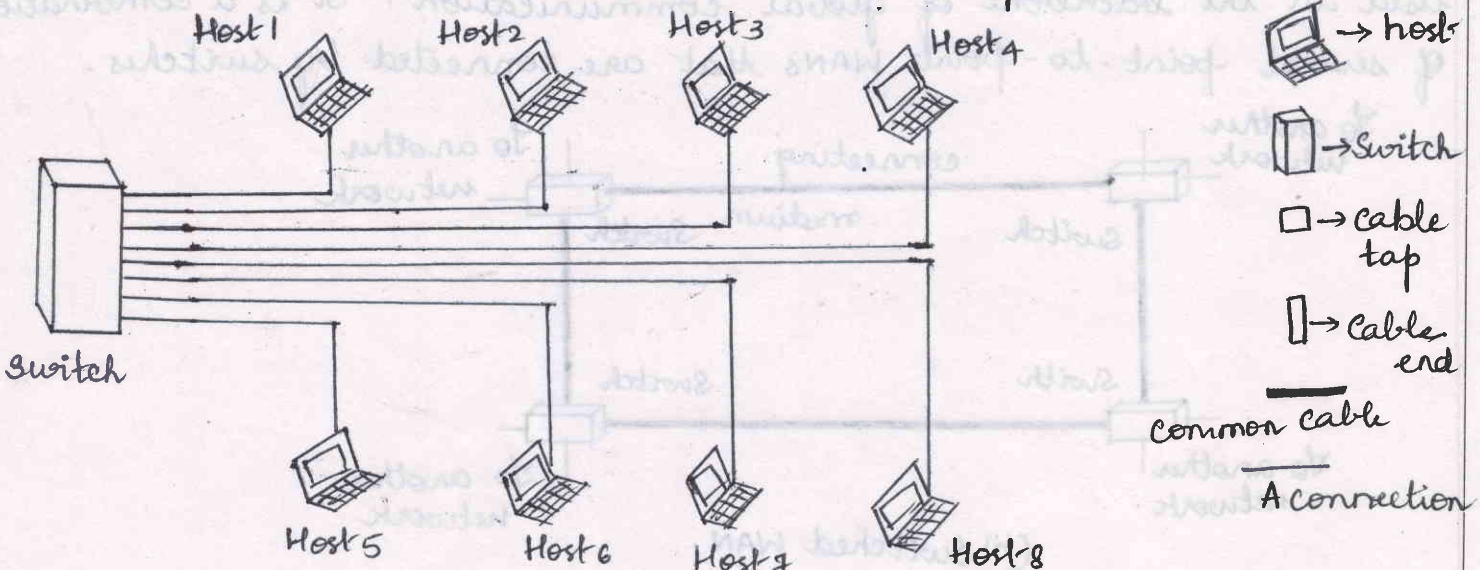
(ii) Each host in a LAN has an identifier, an address, that uniquely defines the host in the LAN. A packet sent by a host to another host carries both the source host's and destination host's addresses.

(iii) Previously, all hosts in a network were connected through a common cable, which meant that a packet sent from one host to another was recieved by all hosts. The intended recipient kept the packet, the others dropped the packet.

(iv) Now, most LANs use a smart connecting switch, which is able to recognize the destination address of the packet and guide the packet to its destination without sending it to all other hosts. The switch alleviates the traffic in the LAN and allows more than one pair to communicate with each other at the same time if there is no common source and destination among them.



(a) LAN with a common cable (past).



(b) LAN with a switch (today)

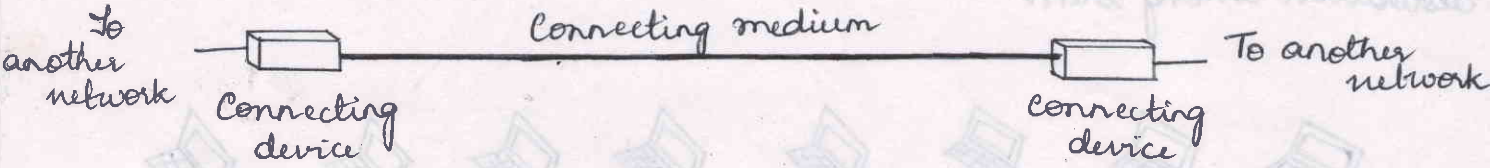
WIDE AREA NETWORK :- (WAN)

A wide area network is also an interconnection of devices capable of communication.

A LAN is normally limited in size, spanning an office, a building, or a campus; a WAN has wider geographical span, spanning a town a state, a country or even the world. A WAN interconnects connecting devices such as switches, routers or modems. It is normally created and run by communication companies and leased by an organization that uses it. Two types of WAN's are:-

(i) Point-to-point WANs:-

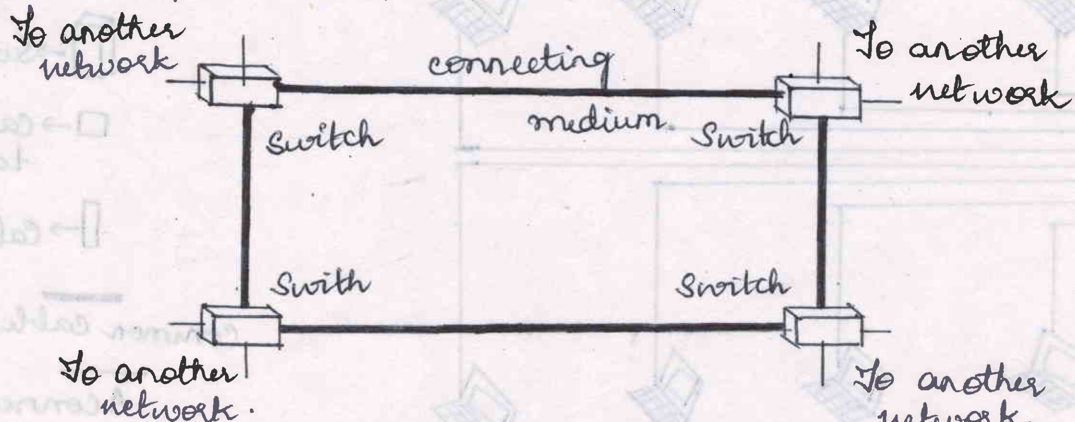
A point-to-point WAN is a network that connects two communica-ting devices through a transmission media (cable or air)



(a) point-to-point WAN.

(ii) Switched WAN:-

A switched WAN is a network with more than two ends. It is used in the backbone of global communication. It is a combination of several point-to-point WANs that are connected by switches.



(b) Switched WAN.

Switching:-

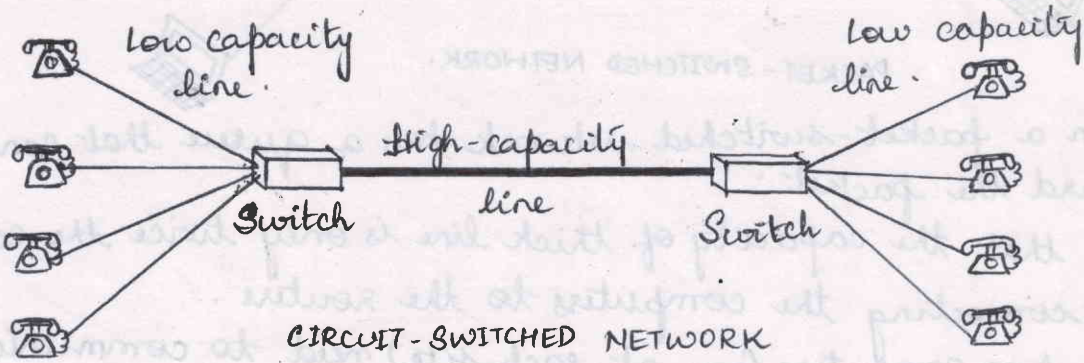
An internet is a switched network in which a switch connects at least two links together. A switch needs to forward data from a network to another network when required. The two most common types of switched networks are (i) circuit-switched and (ii) packet-switche-d networks.

Circuit-Switched Network :-

(i) In a circuit-switched network, a dedicated connection, called a circuit is always available between the two endsystems; the switch can only make it active or inactive.

(ii) The figure shows a simple switched network that connects four telephones to each end. Telephones are used instead of computers as end system because circuit switching was very common in telephone networks.

(iii) In the figure, the four telephones at each side are connected to a switch. The switch connects a telephone set at one side to a telephone set on the other side. The thick line connecting two switches is a high-capacity communication line that can handle four voice communications at the same time; the capacity can be shared between all pairs of telephone sets.



CIRCUIT-SWITCHED NETWORK

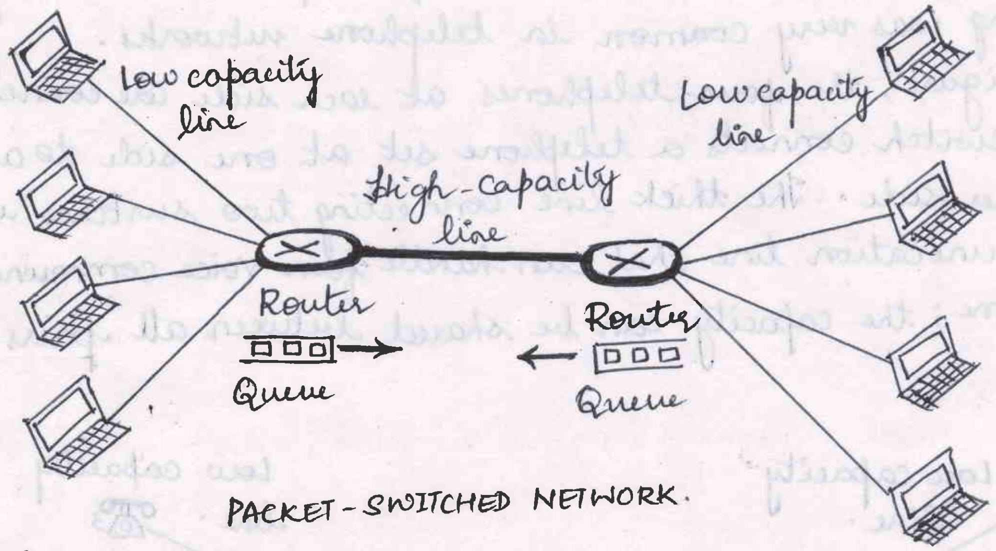
1) Let us consider two cases; In the first case, all telephone sets are busy; four people at one site are talking with four people at the other site, the capacity of the thick line is fully used.

2) In second case, only one telephone set at one side is connected to a telephone set at the other side; only one-fourth of the capacity of the thick line is used. This means that a circuit-switched network is efficient only when it is working at its full capacity, most of the time, it is inefficient because it is working at partial capacity.

Packet-Switched Network :

In a computer network, communication between the two ends is done in blocks of data called packets. Instead of continuous communicat-ion we see between two telephone sets when they are being used, we see the exchange of individual data packets between the two computers. This allows us to make the switch function for both storing and forwarding because a packet is an independent entity that can be stored and sent later.

The figure shows a small packet-switched network that connects four computers at one site to four computers at the other site.



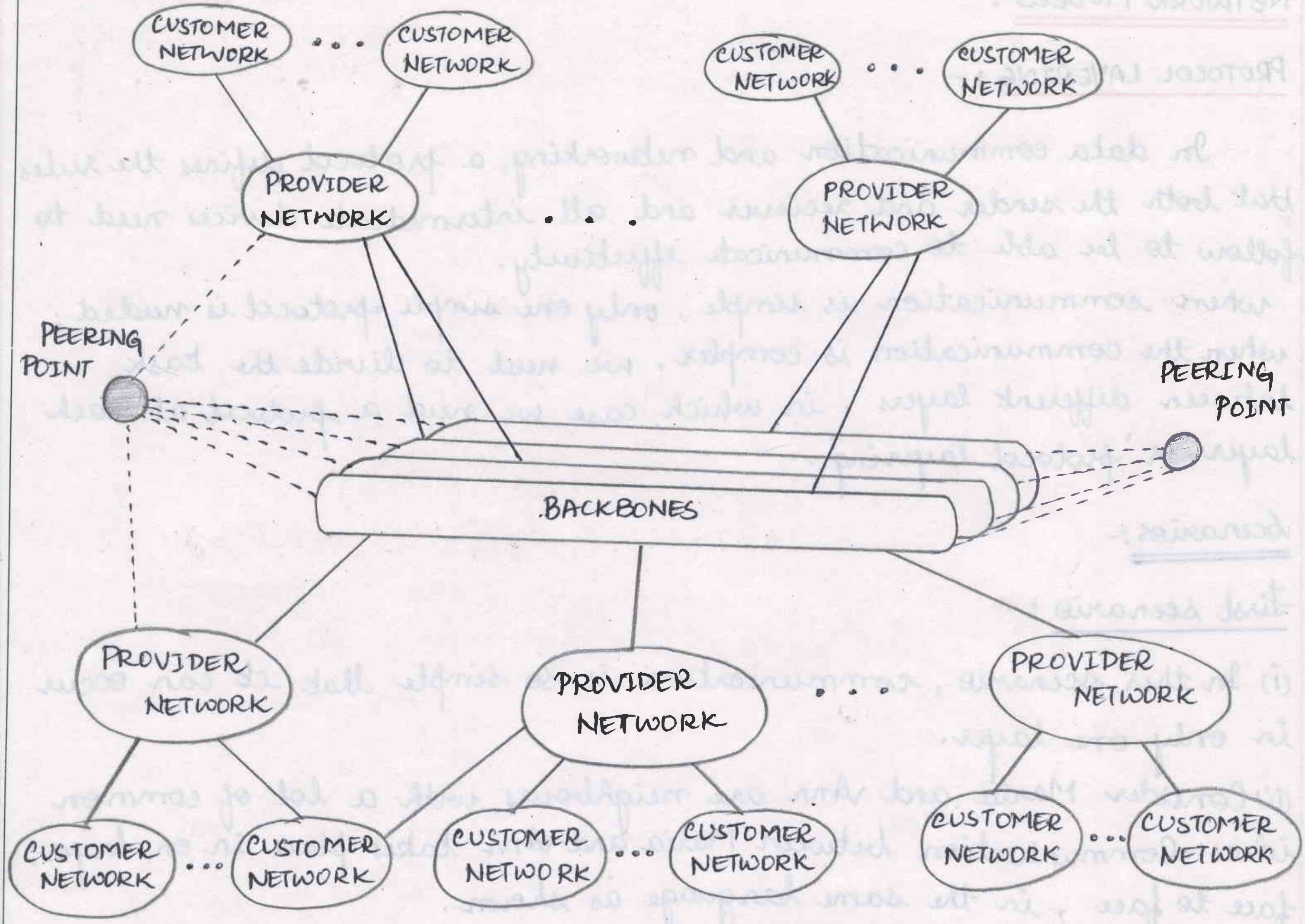
PACKET-SWITCHED NETWORK.

1) Router in a packet-switched network has a queue that can store and forward the packet.
2) Assume that the capacity of thick line is only twice the capacity of data line connecting the computers to the routers.
3) If only two computers (one at each site) need to communicate with each other, there is no waiting for the packets.
4) If packets arrive at one router when the thick line is already working at its full capacity, the packets should be stored and forwarded in the order they arrive.
5) This shows that packet-switched network is more efficient than a circuit-switched network, but packets may encounter some delay.

Internet :-

An 'internet' is two or more networks that can communicate with each other. The most notable internet is called the "Internet", and is composed of thousands of interconnected networks.

The figure shows the conceptual view of the "Internet"



CONCEPTUAL VIEW OF INTERNET.

(i) The Internet has several backbones, provider networks and customer networks

(ii) At the top level, the backbones are large networks owned by some communication companies such as Sprint, Verizon (MCI), AT&T and NTT.

(iii) The backbone networks are connected through some complex switching systems, called peering points

(iv) At the second level, there are smaller networks, called provider networks, that use the services of the backbones for a fee.

(v) The provider networks are connected to backbones and sometimes to other provider networks.

(vi) The customer networks are are networks at the edge of the Internet that actually use the services provided by the Internet. They pay fees to provider network for recieving services.

(vii) Backbones and provider networks are also called Internet Service Providers (ISPs). Backbones are often referred as international ISP and provider networks are regional/national ISPs.

NETWORK MODELS :

PROTOCOL LAYERING :-

In data communication and networking, a protocol defines the rules that both the sender and reciever and all intermediate devices need to follow to be able to communicate effectively.

when communication is simple, only one simple protocol is needed; when the communication is complex, we need to divide the task between different layers, in which case we need a protocol at each layer; or 'protocol layering'.

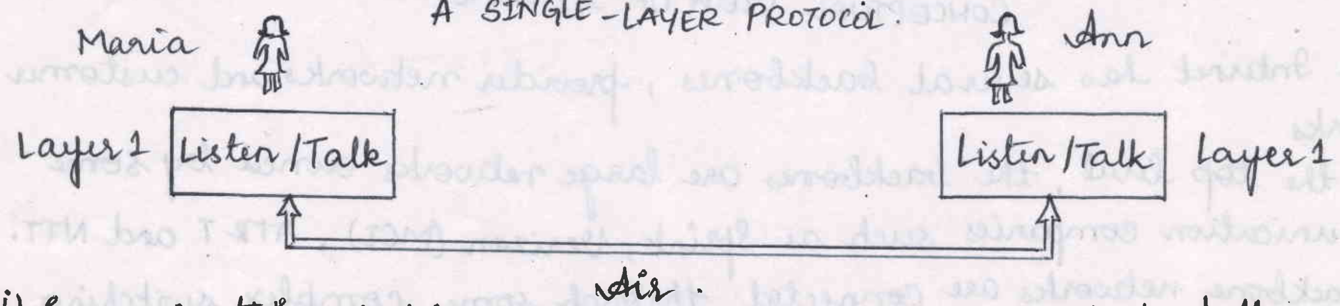
Scenarios :-

First Scenario :

(i) In this scenario, communication is so simple that it can occur in only one layer.

(ii) Consider Maria and Ann are neighbours with a lot of common ideas. Communication between Maria and Ann takes place in on layer, face to face, in the same language as shown.

A SINGLE-LAYER PROTOCOL.



(iii) Even in this simple scenario, a set of rules needs to be followed.

First, Maria & Ann know that they should greet each other when they meet. Second, they know that they should confine their vocabulary to the level of their friendship. Third, each party knows that she should refrain from speaking when the oxther party is speaking.

(iv) Fourth, each party knows that the conversation should be a dialog, not a monolog: both should have the opportunity to talk about the issue. Fifth, they should exchange some nice words when they leave.

(v) We can see that the protocol used by Maria and Ann is different from communication b/w student and professor.

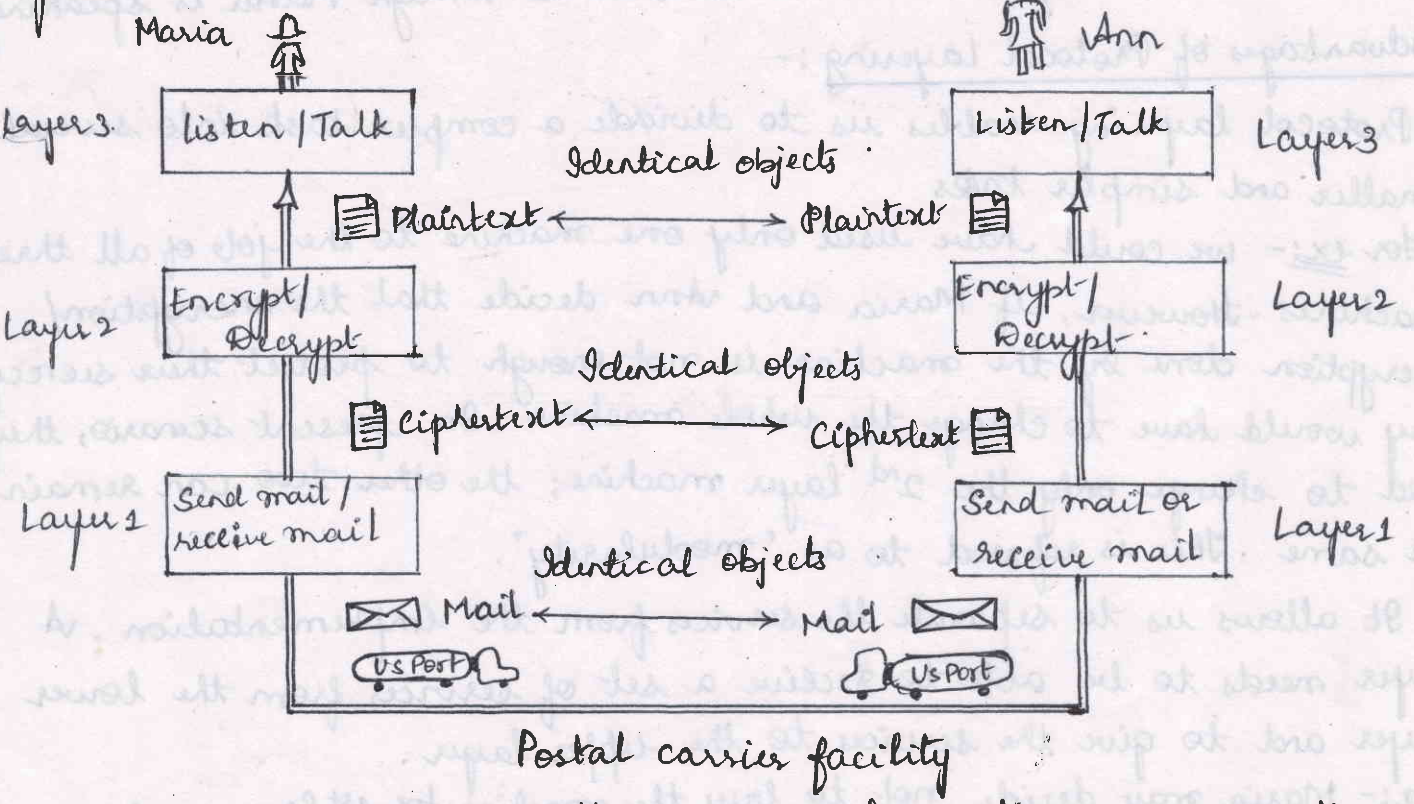
Second Scenario:

(i) In second scenario, we assume Ann is offered a higher-level position in her company, but needs to move to another branch located in a city very far from Maria. The two friends still want to continue their communication and exchange ideas because they have come up with an innovative project to start a new business when they both retire.

(ii) They decide to continue their conversation using regular mail through the post office. However, they do not want their ideas to be revealed by other people if the letters are intercepted.

(iii) They agree on an encryption / decryption technique. The sender of the letters encrypts it to make it unreadable by an intruder; the receiver of the letter decrypts it to get original letter.

(iv) Now communication between Maria and Ann takes place in three layers.



We assume that Ann and Maria each have three machines that can perform the task at each layer.

(i) Let us assume that Maria sends the first letter to Ann. Maria talks to the machine at the third layer as though the machine is Ann and is listening to her

(ii) The 3rd layer machine listens to Maria and creates the plain text (a letter in English), which is passed to 2nd layer machine.

(iii) The 2nd layer machine takes the plain text and encrypts it, and creates the ciphertext, which is passed to first layer machine.

(iv) The 1st layer machine takes the ciphertext, puts it in an envelope, adds the sender and receiver address, and mails it.

(v) At Ann's side, the 1st layer machine picks up the letter from Ann's mail box, recognizing the letter from Maria by the sender address.

(vi) The machine takes out the ciphertext from the envelope and delivers it to the 2nd layer machine.

(vii) The 2nd layer machine, decrypts the message, creates a plaintext, and passes the plaintext to the third-layer machine. The third layer machine takes the plaintext and reads it as though Maria is speaking

Advantages of Protocol Layering :-

(i) Protocol layering enables us to divide a complex task into several smaller and simpler tasks

For ex:- we could have used only one machine to the job of all three machines. However, if Maria and Ann decide that the encryption/decryption done by the machine is not enough to protect their secrecy, they would have to change the whole machine. In present scenario, they need to change only the 2nd layer machine; the other two can remain the same. This is referred to as 'modularity'.

(ii) It allows us to separate the services from the implementation. A layer needs to be able to receive a set of services from the lower layer and to give the services to the upper layer.

Ex:- Maria may decide not to buy the machine for 1st layer, she can do the job herself. As long as Maria can do the tasks provided by the first layer, in both directions, the communication system works.

(iii) When we discuss protocol layering in the Internet, communication does not always use only two end systems; there are intermediate systems that need only some layers, but not all. If protocol layering is not used, we would have to make each intermediate system as complex as the end systems, which makes the whole system more expensive.

Principles of Protocol Layering:-

First Principle:-

The first principle dictates that if we want bidirectional communication, we need to make each layer so that it is able to perform two opposite tasks, one in each direction

For example; the 3rd layer task is to listen (in one direction) and talk (in other direction). The 2nd layer needs to be able to encrypt and decrypt. The 1st layer needs to send and recieve mail.

Second Principle:-

The second principle is that we need to follow in protocol layering is that the two objects under each layer at both sites should be identical.

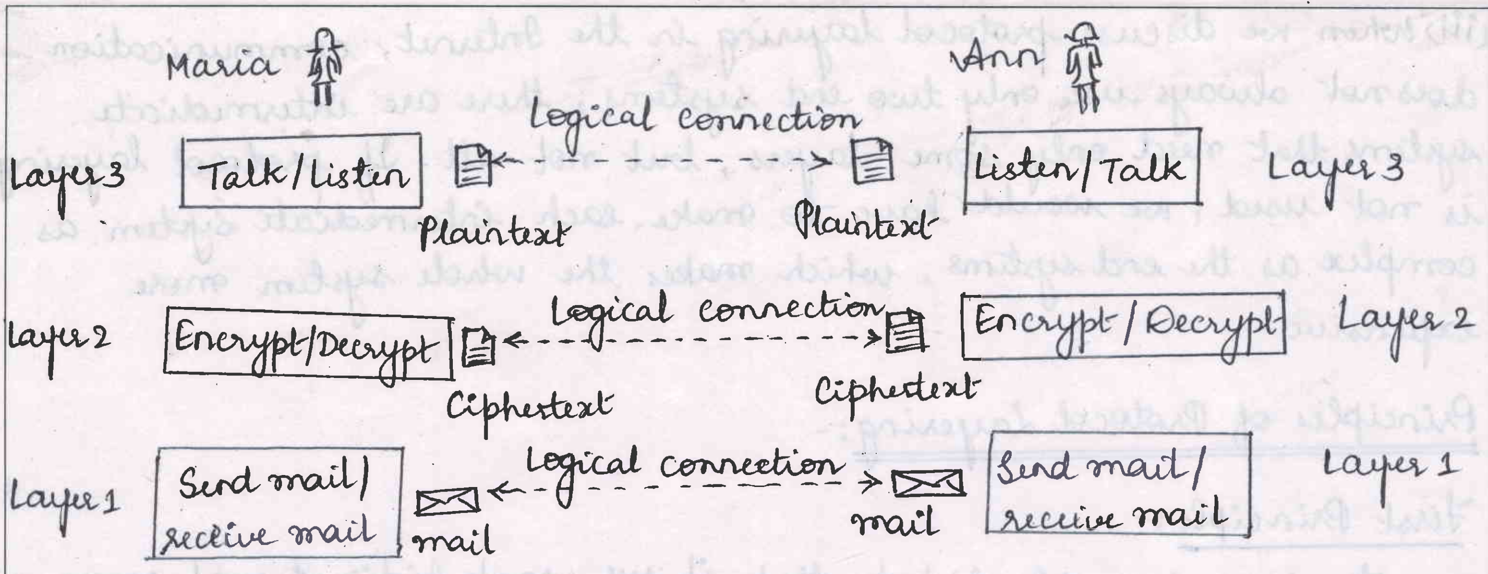
For example; the object under layer 3 at both sides should be a plain text letter. The object under layer 2 at both sides should be ciphertext letter. The object under layer 1 at both sides should be a piece of mail.

Logical Connections:-

Logical connections between each layer is as shown in figure. This means that we have layer-to-layer communication.

Maria and Ann can think that there is a logical (imaginary) connection at each layer through which they can send the object created from that layer.

(P.T.O)



LOGICAL CONNECTION BETWEEN PEER LAYERS.

TCP/IP Protocol Suite :-

TCP/IP (Transmission Control Protocol/Internet Protocol).

TCP/IP is a protocol suite (a set of protocols organized in different layers) used in Internet.

It is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality.

The upper level protocol is supported by services provided by one or more lower level protocols. TCP/IP is a five-layered model.

Layered Architecture :

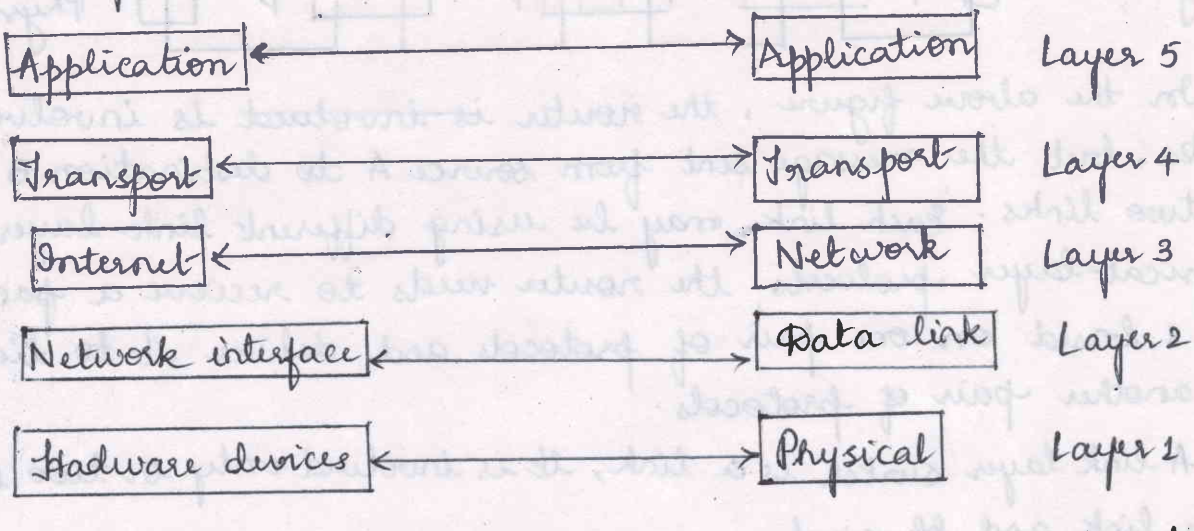
To understand how the layers in the TCP/IP protocol suite are involved in communication between two hosts, we assume we want to use the suite in a small internet made up of three LANs (links), each with a link-layer switch. The links are assumed to be connected by one router as shown in the figure.

(i) Consider, computer A communicates with computer B. We have 5 communicating devices in this communication: source host (computer A), the link-layer switch in link 1, the router, the link-layer switch in link 2 and the destination host (computer B).

(ii) Each device is involved with a set of layers depending on the role of the device in internet.

(iii) The two hosts are involved in all five layers, the source host needs to create a message in the application layer and send it down the layers so that it is physically sent to the destination host.

(iv) The destination host needs to recieve the communication at the physical layer and then deliver it through the other layers to the application layer.



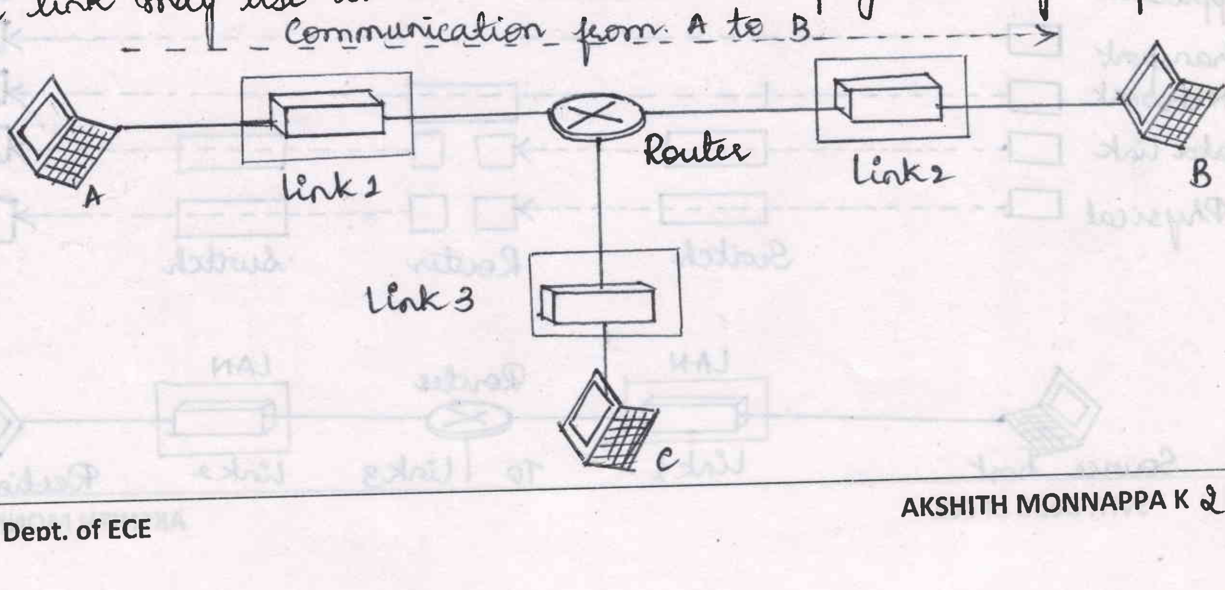
(a) Original layers

(b) Layers used in the book.

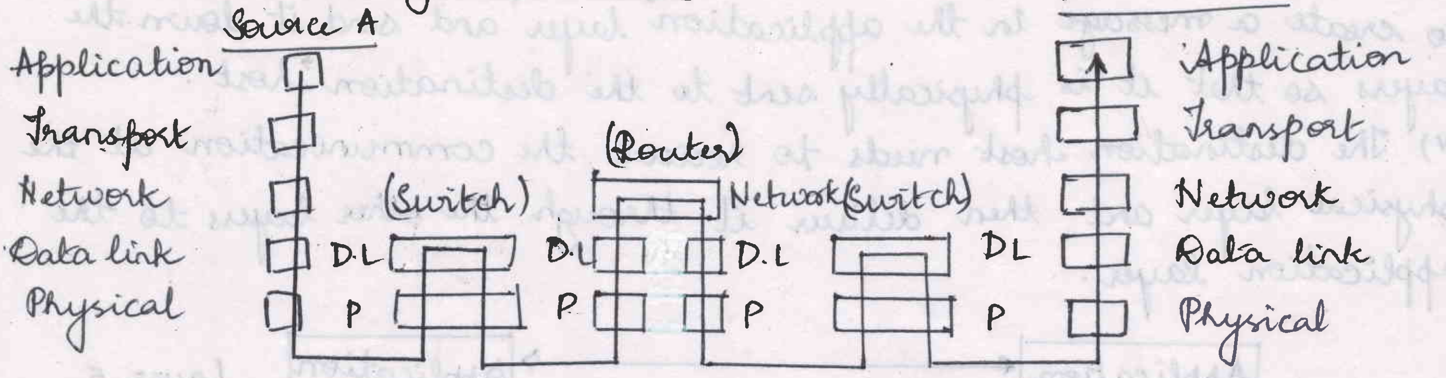
LAYERS IN TCP/IP PROTOCOL SUITE

(V) The router is involved in only three layers; there is no transport or application layer in a router as long as the router is used only for routing.

(VI) Although a router is always involved in one network layer, it is involved in n combinations of link and physical layers in which n is the number of links the router is connected to. The reason is that each link may use its own data-link or physical ~~layers~~ protocol.



Communication through an internet :



(vii) In the above figure, the router ~~is involved~~ is involved in three links, but the message sent from source A to destination B is involved in two links. Each link may be using different link-layer and physical-layer protocols, the router needs to recieve a packet from link 1 based on one pair of protocols and deliver it to link 2 based on another pair of protocols.

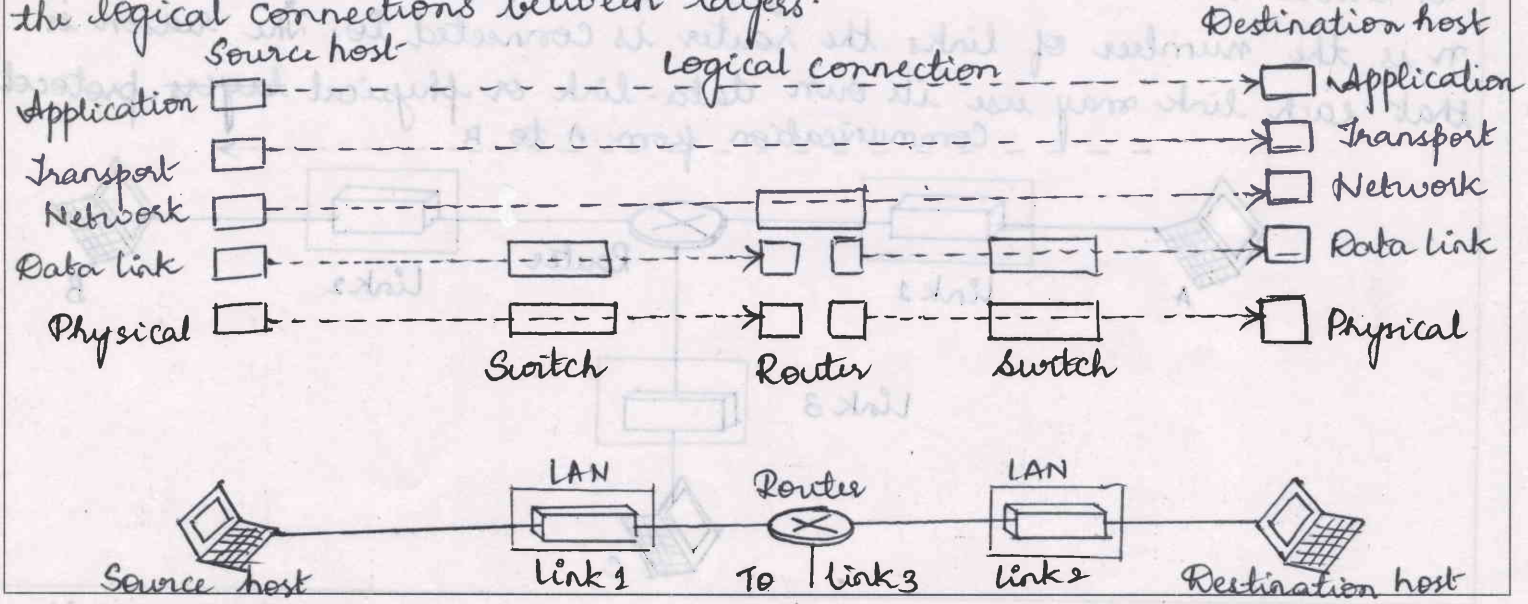
(viii) A link layer switch is a link, it is involved only in two layers, data-link and physical.

(ix) Although each switch in the above figure has two different connections, the connections are in the same link, which uses only one set of protocols

(x) unlike a router, a link-layer switch is involved only in one data-link and one physical layer.

Layers in the TCP/IP Protocol Suite

To understand the duties of each layer, we need to think about the logical connections between layers.



(i) As the figure shows, the duty of the application, transport and network layers is end-to-end.

(ii) The duty of the data-link and physical layers is hop-to-hop, in which a hop is a host or router.

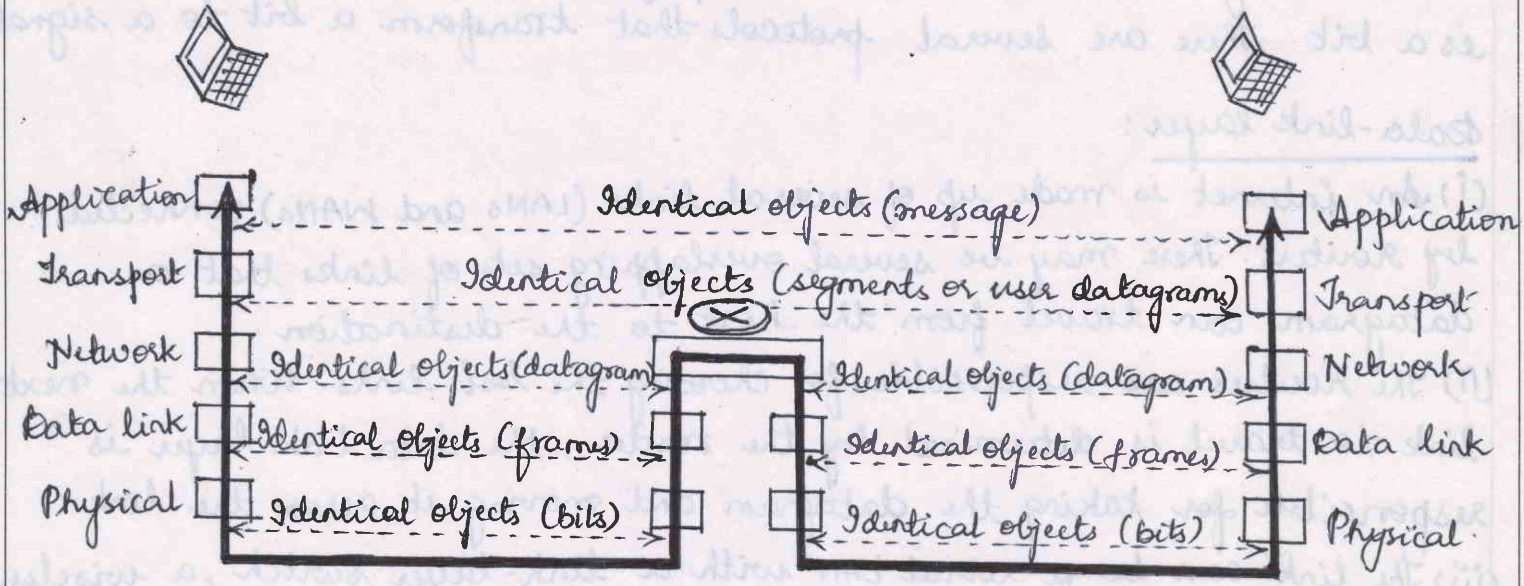
(iii) The domain of duty of the top three layers is the internet, and the domain of duty of the two lower layers is the link.

(iv) ~~As the~~ Another way of thinking of the logical connections is to think about the data unit created from each layer.

(v) In the top three layers, the data unit (packets) should not be changed by any router or link-layer switch.

(vi) In the bottom two layers, the packet created by the host is changed only by the routers, not by the link-layer switches.

The figure shows the second principle discussed previously for protocol layering. We show the identical objects below each layer related to each device.



Although the logical connection at the network layer is between the two hosts, identical objects exist between two hops in this case because a router may fragment the packet at the network layer and send more packets than recieved. Link between two hops does not change the object.

(P.T.O)

Description of Layers :-

Physical Layer:

(i) The physical layer is responsible for carrying individual bits in a frame across the link.

(ii) The physical layer is the lowest level in the TCP/IP protocol suite, the communication between two devices at the physical layer is still a logical communication because there is another, hidden layer, the transmiss-ion media, under the physical layer.

(iii) Two devices are connected by a transmission medium (cable or air). The transmission medium does not carry bits; it carries electrical or optical signals.

(iv) So the bits received in a frame from the data-link layer are transformed and sent through the transmission media, but we can think that the logical unit between two physical layers in two devices is a bit. There are several protocols that transform a bit to a signal.

Data-link layer:

(i) An internet is made up of several links (LANs and WANs) connected by routers. There may be several overlapping sets of links that a datagram can travel from the host to the destination.

(ii) The routers are responsible for choosing the best links. When the next link to travel is determined by the router, the data link layer is responsible for taking the datagram and moving it across the link.

(iii) The link can be a wired LAN with a link-layer switch, a wireless LAN, a wired WAN, or a wireless WAN.

(iv) TCP/IP does not define any specific protocol for the data link layer. It supports all the standard and proprietary protocols. Any protocol that can take a datagram and carry it through the link suffices for the network layer. The data link layer takes a datagram and encapsulates it in a packet called a 'frame'.

(v) Each link layer protocol may provide a different service. Some provide complete error detection and correction.

Network Layer:

(i) The network layer is responsible for creating a connection between the source computer and the destination computer. The communication at the network layer is host-to-host.

(ii) Since there can be several routers from the source to the destination, the routers in the path are responsible for choosing the best route for each packet.

(iii) The network layer in the Internet includes the main protocol, Internet Protocol (IP), that defines the format of the packet, called a datagram at the network layer.

(iv) IP defines the format and the structure of addresses used in this layer. It is responsible for routing a packet from its source to its destination which is achieved by each router forwarding the datagram to the next router in its path.

(v) IP is connectionless protocol that provides no flow control, no error control and no congestion control services. If any of these services are required for an application, it should rely on transport layer protocol.

(vi) The network layer also includes unicast (one-to-one) and multicast (one-to-many) routing protocols. A routing protocol does not take part in routing (it is the responsibility of IP), but creates forwarding tables for routers to help them in the routing process.

(vii) The network layer also has some auxiliary protocols that help IP in its delivery and routing tasks.

(viii) The Internet Control Message Protocol (ICMP) helps IP to report some problems when routing a packet. The Internet Group Management Protocol (IGMP) is another protocol that helps IP in multitasking. The Dynamic Host Configuration Protocol (DHCP) helps IP to get the network-layer address for a host. The Address Resolution Protocol (ARP) is a protocol that helps IP to find link-layer address of a host or a router when its network-layer address is given.

Transport Layer:

(i) The logical connection at the transport layer is also end-to-end. The transport layer at the source host gets the message from the application layer; encapsulates it in a transport layer packet (called a segment or a user datagram in different protocols) and sends it through the logical (imaginary) connection, to the transport layer at the destination host.

(ii) The transport layer is responsible for giving services to the application layer: to get a message from an application program running on the source host and deliver it to the corresponding application program on the destination host.

(iii) There are a few transport layer protocols in the Internet, each designed for some specific task. The main protocol, Transmission Control Protocol (TCP), is a connection-oriented protocol that first establishes a logical connection between transport layers at two hosts before transferring data. It creates a logical pipe between two TCPs for transferring a stream of bytes.

(iv) TCP provides flow control (matching the sending data rate of the source host with the receiving data rate of the destination host to prevent overwhelming the destination); error control (to guarantee that the segments arrive at the destination without error and resending the corrupted ones), and congestion control to reduce the loss of segments due to congestion in the network.

(V) The other common protocol, User Datagram Protocol (UDP), is a connectionless protocol that transmits user datagarms without first creating a logical connection.

(Vi) In UDP, each user datagram is an independent entity without being related to the previous or the next one. UDP is a simple protocol that does not provide flow, error, or congestion control.

(Vii) Its simplicity, means small overhead, is attractive to an application program that needs to send short messages and cannot afford the retransmission of the packets involved in TCP, when a packet is corrupted or lost.

(Viii) Stream Control Transmission Protocol (SCTP) is designed to respond to new applications that are emerging in the multimedia.

Application Layer:

(i) The logical connection between the two application layers is end-to-end. The two application layers exchange messages between each other as though there were a bridge between the two layers.

(ii) Communication at the application layer is between two process (2 programs running at this layer). To communicate, a process sends a request to the other process and receives a response.

(iii) Process-to-process communication is the duty of the application layer. The application layer in the Internet includes may predefined protocols, but a user can also create a pair of processes to be run at the two hosts.

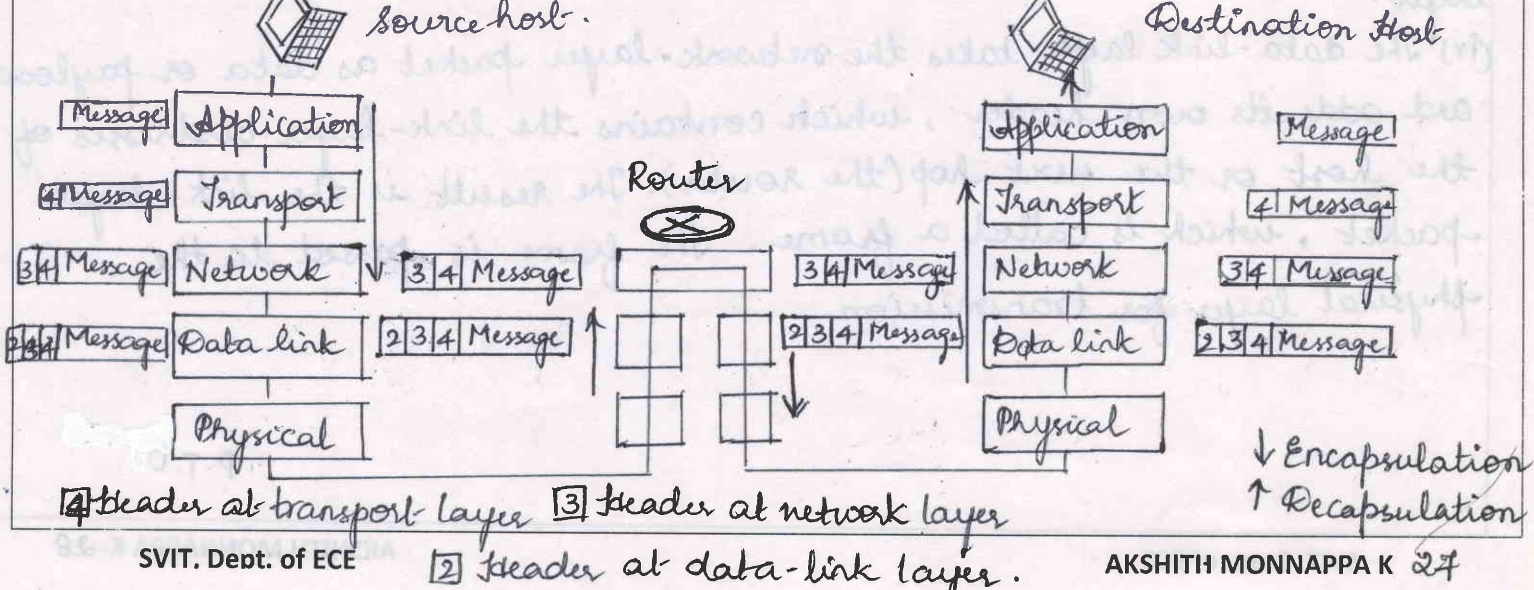
(iv) The Hypertext Transfer Protocol (HTTP) is a vehicle for accessing the World Wide Web (WWW). The Simple Mail Transfer Protocol (SMTP) is the main protocol used in electronic mail (email) service.

(v) The File Transfer Protocol (FTP) is used for transferring files from one host to another. The Terminal Network (TELNET) and Secure Shell (SSH) are used for accessing the site remotely.

(vi) The Simple Network Management Protocol (SNMP) is used by an administrator to manage the Internet at global and local levels. The Domain Name System (DNS) is used by other protocols to find the network-layer address of a company computer. The Internet Group Management Protocol (IGMP) is used to collect membership in a group.

Encapsulation and Decapsulation:-

One of the important concepts in protocol layering in the Internet is encapsulation / decapsulation.



4 Header at transport layer 3 Header at network layer
2 Header at data-link layer.

The figure shows, the encapsulation at source host, decapsulation in the destination host, and encapsulation and decapsulation in the router.

Encapsulation at the Source Host:

At source, we have only encapsulation.

(i) At the application layer, the data to be exchanged is referred to as a message. A message normally does not contain any header or trailer, but if it does, we refer to the whole as the message. The message ~~to~~ is passed to the transport layer.

(ii) The transport layer takes the message as the payload, the load that the transport layer should take care of. It adds the transport layer header to the payload, which contains the identifiers of the source and destination application programs that want to communicate plus some more information that is needed for the end-to-end ~~layers~~ delivery of the message, such as information needed for flow, error control or congestion control. The result is the transport layer packet, which is called the segment (in TCP) and the user datagram (in UDP). The transport layer then passes the message to the network layer.

(iii) The network layer takes the transport-layer packet as data or payload and adds its own header to the payload. The header contains the addresses of the source and destination hosts and some more information used for error checking of the header, fragmentation information, and so on. The result is the network-layer packet called a datagram. The network layer then passes the packet to the data-link layer.

(iv) The data-link layer takes the network-layer packet as data or payload and adds its own header, which contains the link-layer addresses of the host or the next hop (the router). The result is the link-layer packet, which is called a frame. The frame is passed to the physical layer for transmission.

P.T.O.

Decapsulation and Encapsulation at the Router :-

At router, both decapsulation and encapsulation is present because it is connected to two or more links.

(i) After the set of bits are delivered to the data-link layer, this layer decapsulates the datagram from the frame and passes it to the network layer.

(ii) The network layer only inspects the source and destination addresses in the datagram header and consults its forwarding table to find the next hop to which the datagram is to be delivered. The contents of the datagram should not be changed by the network layer in the router unless there is a need to fragment the datagram if it is too big to be passed through the next link. The datagram is then passed to the data-link layer of the next link.

(iii) The data-link layer of the next link encapsulates the datagram in a frame and passes it to the physical layer for transmission.

Decapsulation at the Destination Host :-

At the destination host, each layer only decapsulates the packet received, removes the payload, and delivers the payload to the next-higher layer protocol until the message reaches the application layer. It is necessary to say that decapsulation in the host involves error checking.

Addressing :-

(i) We have logical connections between pairs of layers in the model. Any communication that involves two parties needs two addresses: source address and destination address.

(ii) Although it looks like we need five pairs of addresses (one pair per layer), we have only four because the physical layer does not need addresses.

(iii) The unit of data exchange at the physical layer is a bit, which cannot have an address. The figure shows the addressing at each layer.

(iv) As the figure shows, there is a relationship between the layer, the address used in that layer, and the packet name at that layer.

P.T.O.

Packet names	Layers	Address
Message	Application layer	Names
Segment/User datagram	Transport Layer	Port numbers
Datagram	Network Layer	Logical addresses
Frame	Data-Link Layer	Link-layer addresses
Bits	Physical Layer	

ADDRESSING IN TCP/IP PROTOCOL SUITE.

(iv) At the application layer, we use names to define the site that provides services; such as someorg.com or the email address, ex:- somebody@coldmail.com

(v) At transport layer, the addresses are called port numbers, and these define the application-layer programs at the source and destination. Port numbers are local addresses that distinguish between several programs running at the same time.

(vi) At the network-layer address uniquely defines the connection of a device to the Internet. The link-layer addresses, called as MAC address, are locally defined addresses, each of which defines a specific host or router in a network (LAN or WAN).

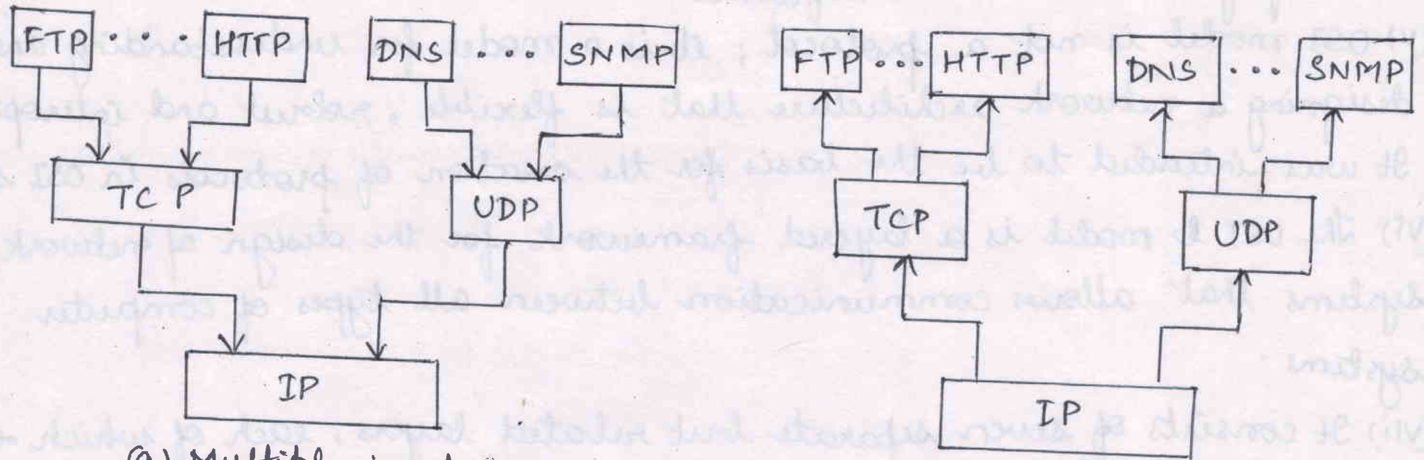
Multiplexing and Demultiplexing:-

(i) Since the TCP/IP protocol suite uses several protocols at some layers, there is multiplexing at the source and demultiplexing at the destination.

(ii) Multiplexing means that a protocol at a layer can encapsulate a packet from several next-higher layer protocols (one at a time).

(iii) Demultiplexing means that a protocol can ~~de~~ decapsulate and deliver a packet to several next-higher layer protocols (one at a time).

Figure shows the concept of multiplexing and demultiplexing at the three upper layers.



(a) Multiplexing at source

(b) Demultiplexing at destination

(iv) To multiplex and demultiplex, a protocol needs to have a field in its header to identify to which protocol the encapsulated packets belong.

(v) At the transport layer, either UDP or TCP can accept a message from several application-layer protocols.

(vi) At the network layer, IP can accept a segment from TCP or a user datagram from UDP.

(vii) IP can also accept a packet from other protocols such as ICMP, IGMP etc

(viii) At data link layer, a frame may carry the payload coming from IP or other protocols such as ARP.

The OSI Model:

(i) TCP/IP protocol suite is not the only suite of protocols defined. Established in 1947, the International Organization for Standardization (ISO) is a multinational body dedicated to worldwide agreement on international standards.

(ii) An ISO standard that covers all aspects of network communications is the "Open Systems Interconnection" (OSI) model. It was introduced in 1970s.

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

(iv) The purpose of OSI model is to show how to facilitate communicati between different systems without requiring changes to the logic of th underlying hardware and software.

(v) OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust and interoperabl It was intended to be the basis for the creation of protocols in OSI stac

(vi) The OSI ~~&~~ model is a layered framework for the design of network systems that allows communication between all types of computer systems.

(vii) It consists of seven separate but related layers, each of which ~~is defined~~ defines a part of the process of moving information across the network.

Layer 7	APPLICATION
Layer 6	PRESENTATION
Layer 5	SESSION
Layer 4	TRANSPORT
Layer 3	NETWORK
Layer 2	DATA LINK
Layer 1	PHYSICAL

THE OSI MODEL

OSI versus TCP/IP :-

When we compare the two models, we find two layers, session and presentation, are missing from TCP/IP protocol suite.

The application layer in the suite is usually considered to be a combination of three layers in the OSI model.

(i) The TCP/IP has more than one transport-layer protocol. Some of the functionality of the session-layer are available in some of transport layer protocols.

(ii) The application layer is not only one piece of software. Many applicati[ons] can be developed in this layer. If some of the functionalities mentione[d] in the session and presentation layers are needed for a particular application, they can be included in the development of that piece of software.