Computer Networks

Module 1

① Explain the four basic topologies used in networks. List advantages and disadvantages of each of them.

→ The four basic topologies are:

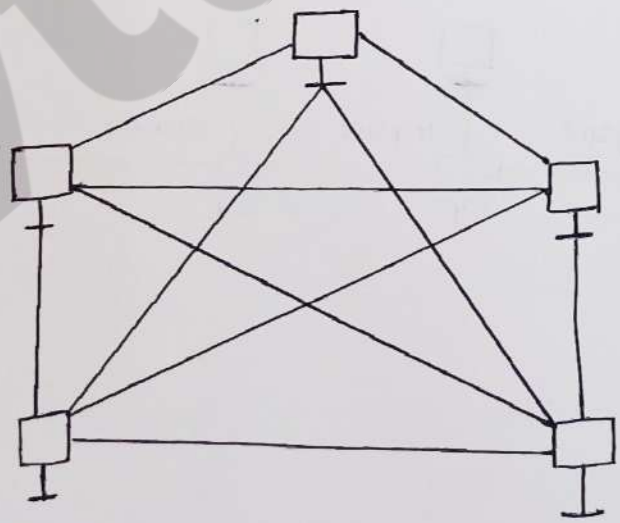
i) Mesh topology:

a) In mesh topology every device is connected to other device, requiring $n(n-1)/2$ links for n devices.

b) Node 1 must be connected to n-1 node, node 2 must be connected to n-2 node, and finally node n must be connected to n-1 nodes. We need $n(n-1)$ physical links. However, if each physical link allows communication in both direction, we can divide the number of links by 2. Therefore we need $n(n-1)/2$ duplex-mode links.

c) Advantages: Dedicated links, fault isolation, secure

d) Disadvantages: Expensive, complex installation, excessive cabling.
Eg: Telephone network between regional offices.



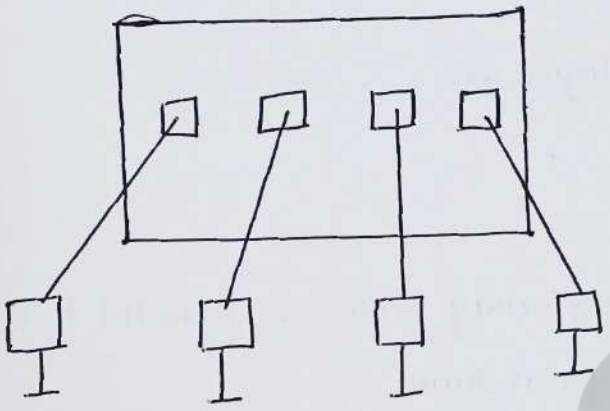
2) Star topology

1) Each devices is connected to a central hub, which manages communication

2) Advantages: Easy installation and fault isolation, if a link fails, only the device is affected

3) Disadvantages: Entire system fails if the hub goes down.

Eg: LAN



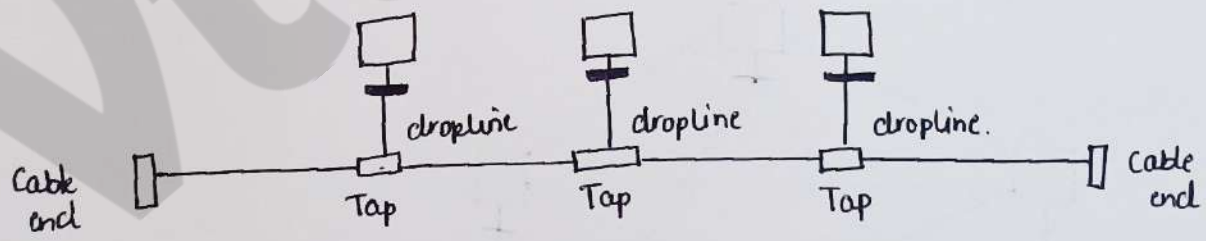
3) Bus topology:

a) All devices are connected to a single backbone cable.

b) Advantages: Easy installation, less cabling than mesh

c) Disadvantages: Difficult to add device, fault in the backbone disrupt the entire network.

Eg: Early ethernet LANS.



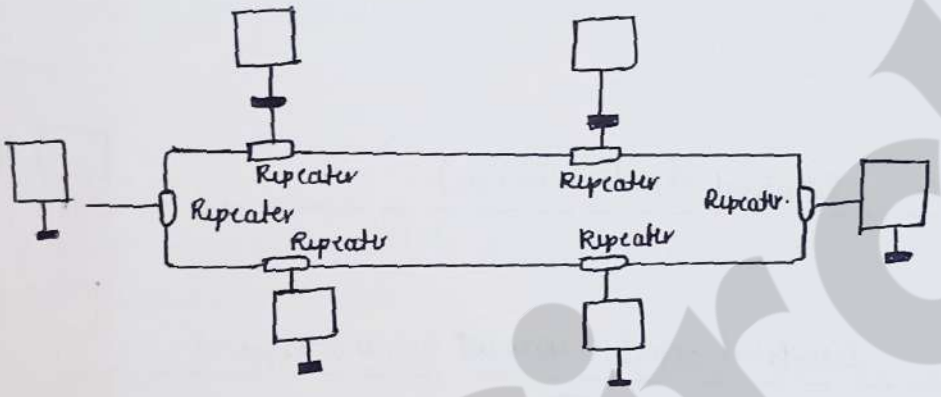
4) Ring topology:

a) Devices are connected in loop, with signals travelling in one direction through repeaters.

b) Advantages: easy to installation, simple fault detection.

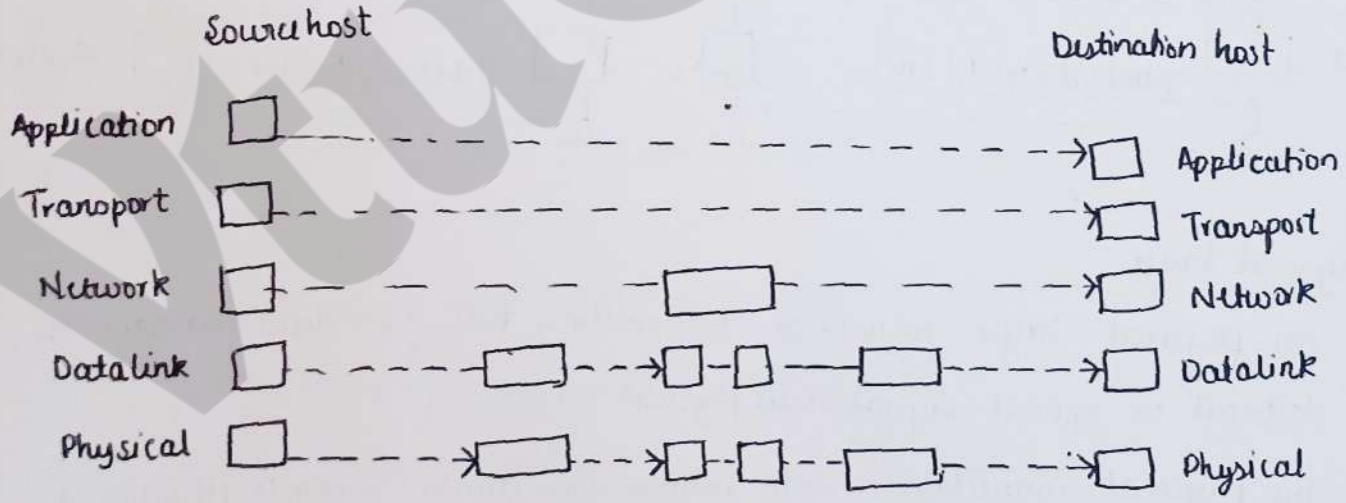
c) Disadvantage: A break in ring can disable the entire network.

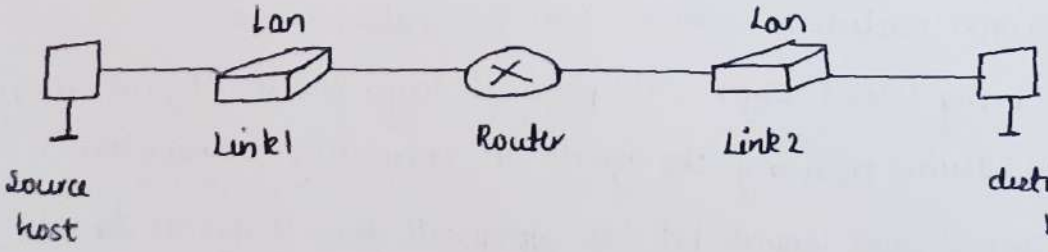
Eg: IBM's token ring LANs



(2) What is meant by logical connection in TCP/IP. Explain with diagram how the identical object interact.

→

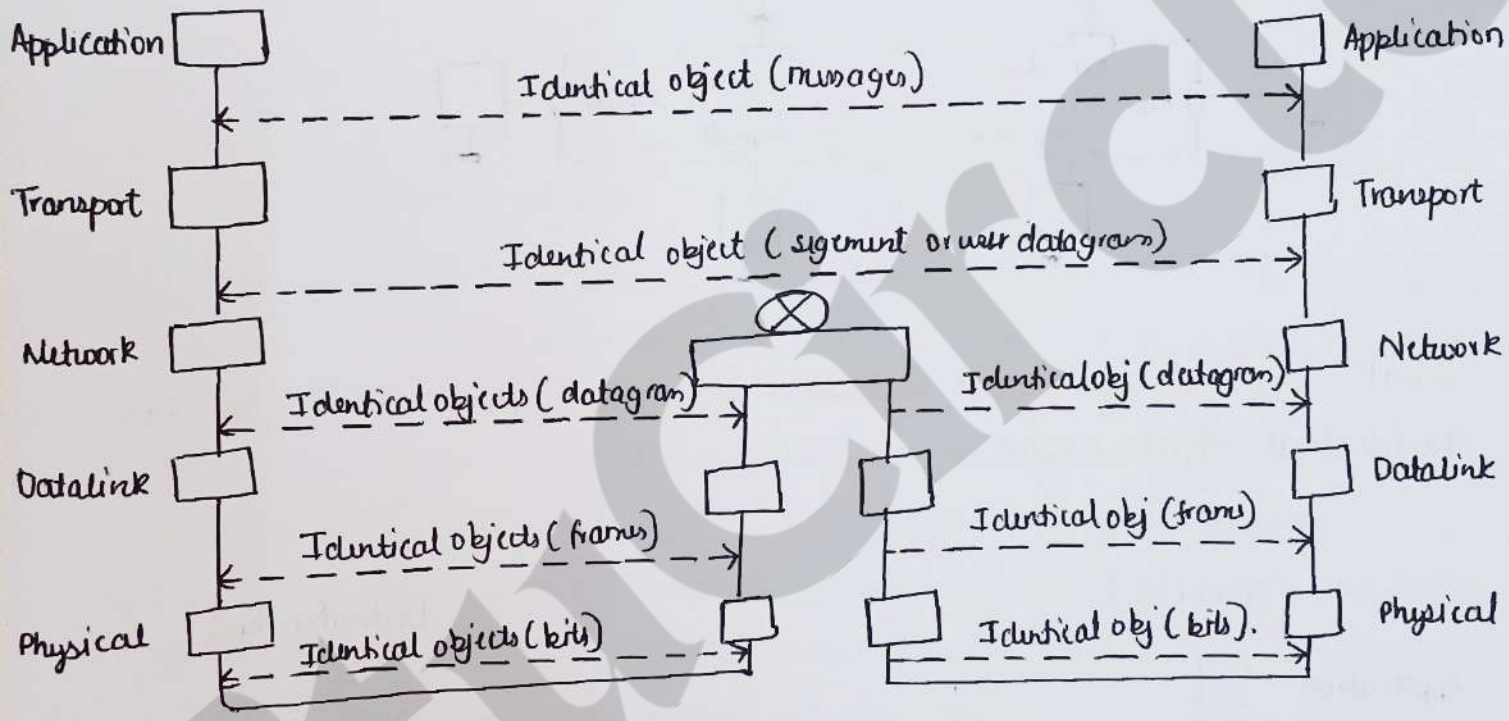




The application, transport and network layers are responsible for end to end communication, meaning they manage data from one end device to other across the network.

The data-link and physical layer on the other hand, handle communication on a hop to hop basis, where each "hop" refers to a host or router.

Identical object interact in TCP/IP protocol suite



1) Physical layer:

* The physical layer focuses on transmitting bits from data link layer as electrical or optical signal over physical medium.
* The physical connection made between two devices is made through a transmission medium which can be cables or air.
* Despite being lowest layer, the physical layer enables logical communication between devices ensuring the signals are accurately transmitted.
* The physical layer converts bit into appropriate forms of signals depending on the medium level.

2) Datalink layer:

* We have seen that an internet is made up of several links connected by routers.
* These routers are responsible for choosing the best links. However when the next link to travel is determined by the router, the data link layer is responsible for taking datagram and moving it across the link.
* The link can be wired LAN with a link layer switch, a wired LAD, a wired WAN or wireless WAN.
* In each case, the datalink layer is responsible for moving the packet through the link
* The data link layer takes a datagram and encapsulates it in a packet called frame.

3) Network Layer:

* The network layer is responsible for creating a connection between the source computer and destination computer.
* The communication at the network layer is host-to-host. However since there are several routers from the source to destination, the router in the path are responsible for choosing the best path for each packet.
* The network layer in the Internet include the main protocol, Internet protocol that defines the format of the packet, called a datagram at network layer.
* IP also defines the formaat and the structure of addresses used in this layer
* IP is also responsible for routing a packet from its sources to destination
* IP is a connectionless protocol that provides no flow control, no error control, and no congestion control services.
* The network layer also has some auxiliary protocols such as Dynamic Host configuration protocol, Address Resolution Protocol, these help IP in its delivery and routing tasks.

(4) Transport layer:

* The logical connection at the transport layer is end to end.
* The transport layer at the source host get the messages from application layer, encapsulates it in a layer packet and sends it through the logical connection, to the transport layer at the destination host

* The main protocol, Transmission control protocol, is a connection oriented protocol that first establishes a logical connection between transport layers at two host before transferring data. It creates a logical pipe between two TCP for transferring a stream of bytes. TCP provides flow control, error control and congestion control to reduce the loss of segments due to congestion in network.
* The transport layer should be independent of application layer.
* UDP is a connectionless protocol that transmit use datagram without first creating a logical connection.

(5) Application layer:

* The two application layers exchange messages between each other as though there were a bridge between two layers.
* Communication at application layer is between two processes. To communicate a process sends a request to other process and receive a response. Process to process communication is the duty of application layer.

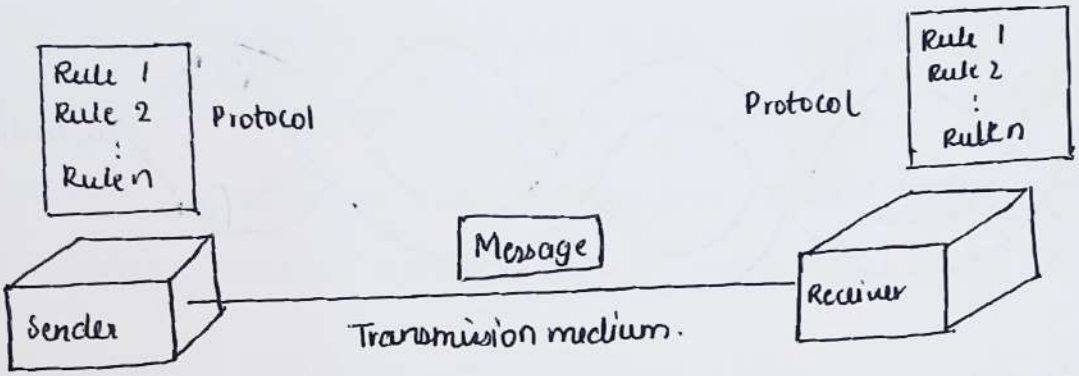
(3) What is data communication? Explain its characteristics and components.

→ Data communication: Data communication is the exchange of data between two devices via some form of transmission medium such as wire cable.

Characteristics:

1) Delivery: The system must deliver data to correct destination. Data must be received by the intended device or user and only by that device or user.
2) Accuracy: The system must deliver data accurately. Data that have been altered in transmission and left uncorrected are unusable.
3) Timeliness: The system must deliver data in timely manner. Data delivered late are useless.
4) Jitter: Jitter refers to the variation in packet arrival time. It is the uneven delay of audio or video packets.

Components in data communication.



1) Message: The message is the information to be communicated. Popular form of information include text, number, pictures etc

2) Sender: The sender is a device that sends the data message. It can be computer workstation, video camera.

3) Receiver: The receiver is a device that receives the message. It can be computer, workstation, television.

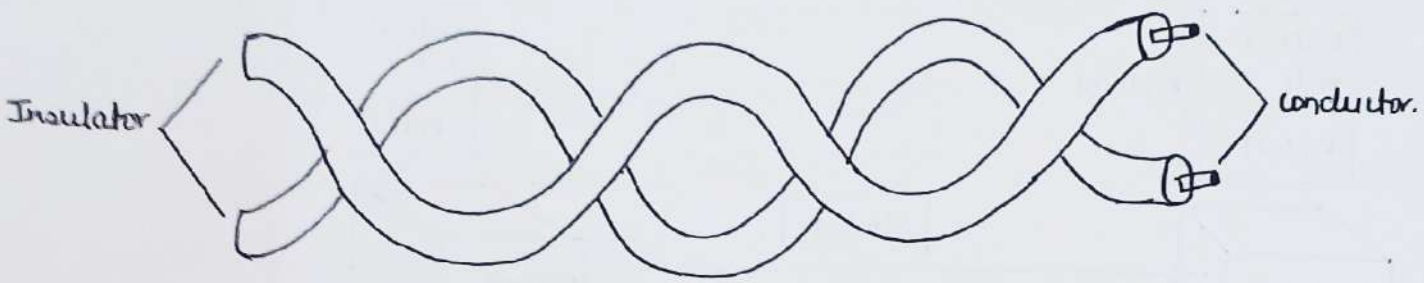
4) Transmission medium: The transmission medium is a physical path by which a message travels from sender to receiver. Eg: twisted pair wire, coaxial cable, fibre optic cable.

5) Protocal: A protocol is a set of rules that govern the data communication. It represents an agreement between two communicating devices.

(4) ~~Explain~~ What are guided transmission media? Explain twisted pair cable in detail.

→ Guided transmission media: Guided media are the types of communication channels that provide a specific path to travel from one device to another device. These include Twisted pair cable, Coaxial Cable, fibre optic cable.

Twisted pair cable:



1) A twisted pair cable consist of two insulated copper conductors twisted together.

2) Each wire in the pair serves a different function: one carries the signal to the receiver, and other act as ground.

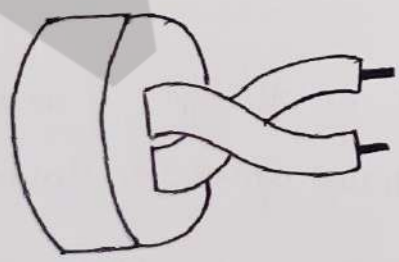
3) The twisted pair cables are mainly designed to minimize the impact of noise and cross talk.

4) When the wires are parallel, noise or cross talk can effect each wire differently. By twisting the cables maintain a balance.

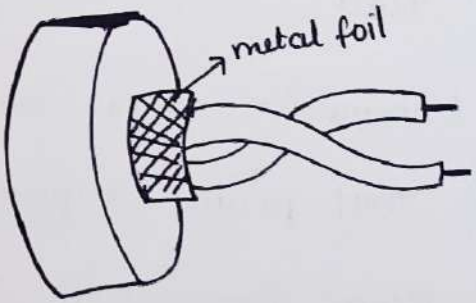
5) Shielded and Unshielded twisted pair cables.

Unshielded Twisted pair: The most common type used in communication

Shielded Twisted pair: The cable have additional metal foil or braided mesh covering each pair of conductors. The shielding reduces interference and improves signal quality.



unshidded



Shielded

6) The RJ45 connector is the most common connector for UTP cables.

7) The performance of twisted pair cables is often assessed by measuring attenuation in relation to frequency and distance.

8) Although twisted pair cable can handle a broad range of frequencies, attenuation increases significantly at frequencies above 100kHz.

9) Applications: Telephone lines, DSL lines, LAN's.

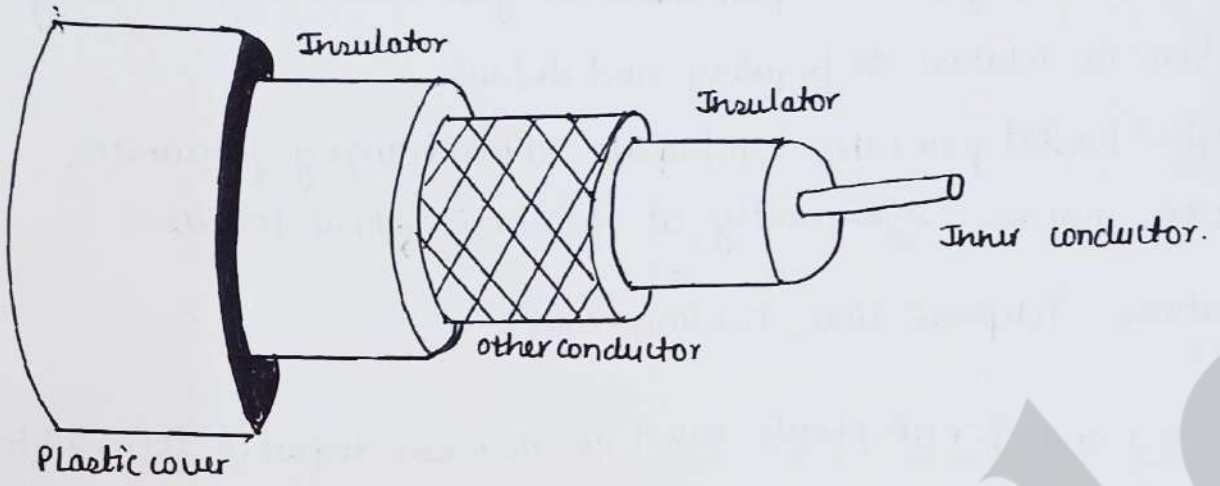
⑤ Compare OSI and TCP/IP Models. What are the reasons ~~to fail~~ for OSI model to fail?

→ OSI Model	TCP/IP model
1) Open system interconnection model	Transmission control protocol/ Internet protocol
2) Developed By ISO	Developed by U.S. Department of defense.
3) Number of layers are 7	Number of layers are 5
4) Top down approach	Bottom up approach
5) Independent of protocols	Protocol dependent.
6) Conceptual model	Practical model.
7) More detailed error handling	Simplified error handling.

The Reason for OSI model to fail

1) First, the OSI model was completed when TCP/IP was fully in place and a lot of time and money had been spent on the suite, changing it would cost lot
2) Seconds, some layers in the OSI model were never fully defined.
3) Third, when OSI was implemented by an organization in different application it did not show a high enough level of performance to entice the internet authority to switch from TCP/IP to OSI model.

(6) Explain Coaxial cable and fibre optic cable.



1) Coaxial cable carries signals of higher frequency ranges than those in twisted pair cable.

2) Instead of having two wires, coaxial have a central core conductor of solid enclosed in an insulating sheath, encased in an outer conductor of metal foil or combination of two.

3) The outer metallic wrapping serves both as a shield against noise and as the second conductor which complete the circuit.

4) The outer conductor is also enclosed in an insulating sheath and the whole cable is protected by plastic cover.

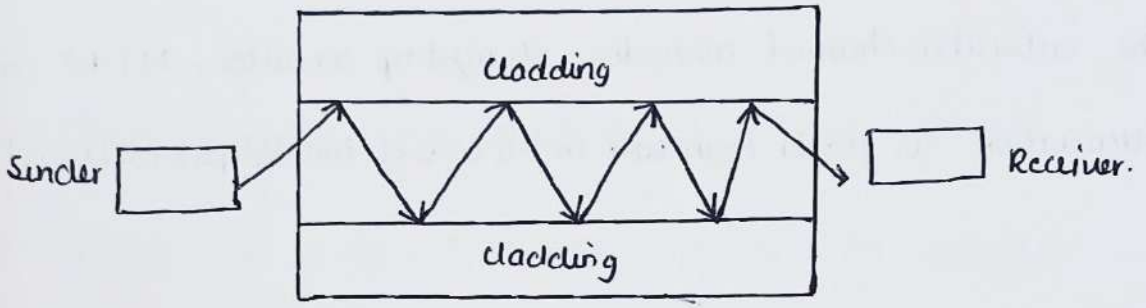
5) Coaxial Cables are categorized by the goverment of India, Radio Goverment. Each RG number denotes a unique set of physical specification, including the wire gauge of inner conductor, thickness and type of insulator, and size and type of outer casting.

6) The most common type of connector used in Coaxial Cable are Bayonet Neill-Concelman connector.

7) The ~~attes~~ attenuation is much higher in coaxial cable than in twisted pair.

8) Applications : TV cable, telephone network.

Fibre optic cable:



1) A fibre optic cable is made of glass or plastic and transmits signals in form of light.

2) Optical fibres use reflection to guide light through a channel. A glass or a plastic core is surrounded by cladding of less dense glass or plastic.

3) The different in the density of the two materials must be such that beam of light moving through the core is reflected off the cladding instead of be being refracted into it.

4) Current technology provides two modes ie Multimode and Single mode.

5) In multimode multiple beams from a light source move through the core in different path. There are two types in multimode ie step index and graded index.

6) In multimode step index fibre, the core density is constant causing light to travel in straight line. until it hits lower density cladding.

7) In multimode graded index fibre reduces this distortion by gradually decreasing the core density from center to edge, allowing light to bend smoothy and reduce signal distortion.

8) Single mode fibre uses step index fibre with a very narrow core and focused light source. This setup limit light beams to nearly horizontal path. The fibre small diameter and lower density create critical angle of 90°,

ensuring that the beam travels almost parallel.

9) Optical fibre are defined by ratio of diameter of core and diameter of cladding.

10) The subscriber channel connector, straight tip connector, MT-RJ connector.

11) Attenuation is flatter than case in the case of twisted pair cable and coaxial.

(7) Explain unguided media.

→ unguided media refers to communication channels that use wireless signals to transmit data. These signals travel through air or without any physical conductor.

Unguided medias are of 3 types: Radio waves, micro waves and infrared waves.

1) Radio waves:

* Radio waves have frequency range from typically from 3khz to 1GHz.
* Radio waves are mostly omnidirectional, meaning they spread out in all directions from transmitting antenna.
* The sending and receiving antenna's don't need to be aligned for sucessfull communication, as any receiving antenna in range can pick up the signal.
* Radio waves especially propagate in the sky mode can travel long distances.
* Radio waves, particularly those with low and medium frequencies that can penetrate walls.
* The Radio wave band is relatively narrow, just under 1GHz, when divided into subbands, the limited width of these subband result in low data rates for digital communication.

* Application: AM and FM radio, Television broadcasting, cordless phones.

2) Microwaves.

1) Microwaves have frequency range from typically 1GHz to 300GHz

2) Microware require line of sight transmission, meaning the transmitter and receiver must be directly visible to each other. ~~They are~~

3) They are less effective in penetrating obstacles like buildings.

4) Application: Satellite communication, radar system, microwave oven.

3) Infrared waves:

1) Infrared waves have frequency range from typically 300GHz to 400THz

2) Infrared signals are used for short range communication and do not penetrate walls, making them suitable for indoor use.

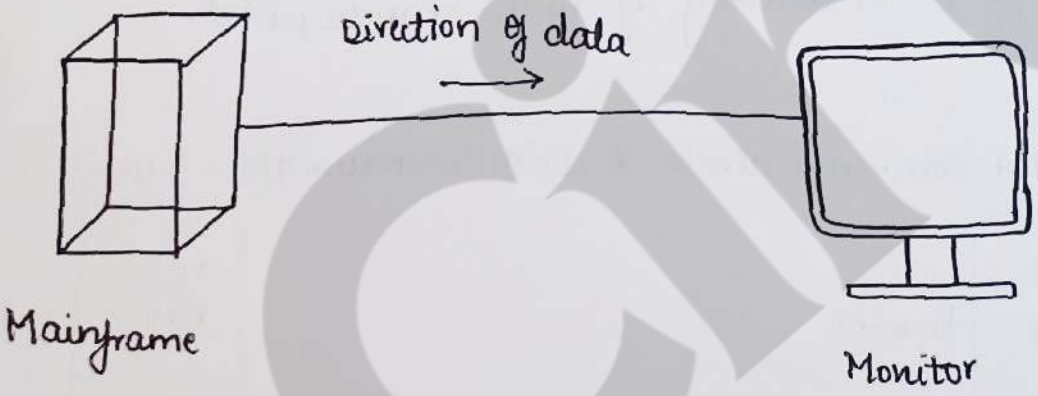
3) They are highly directional and require line of sight transmission.

4) Application: Remote control, short range data transmission, medical devices.

(8) What is data flow? Explain simplex, half duplex and full duplex with diagram.

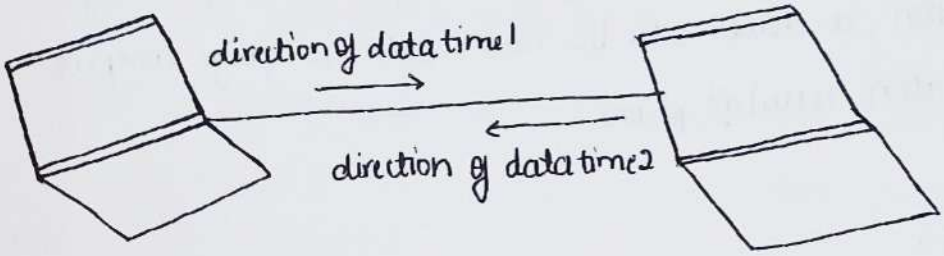
→ Communicating between two devices can be simplex, half duplex or full duplex is called as data flow.

1) Simplex:



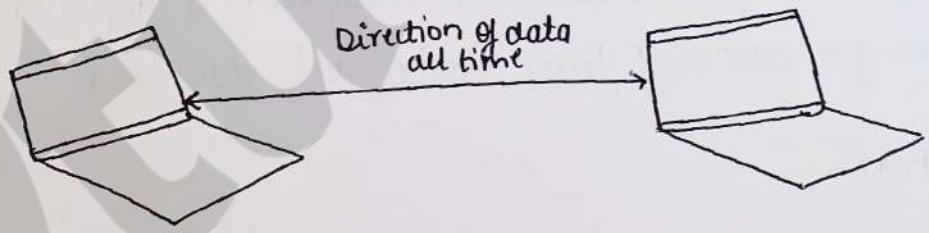
1) In simplex mode, the communication is unidirectional, as on a oneway street
2) Only one of two devices on a link can transmit, the other can only receive.
3) Keyboards and traditional monitors are the examples of simplex devices. The keyboard can only introduce input and monitor can only accept output

2) Half Duplex:



1) In half duplex mode, each station can both transmit and receive, but not at the same time. When one devices is sending, the other can only receive and vice versa.
2) The half duplex mode is like a one-lane road with traffic allowed in both directions.
3) In half duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time.

3) Full duplex:



1) In full duplex mode, both station can transmit and receive simultaneously.
2) The full duplex mode is like a two way street with traffic flowing in both directions at same time.
3) In full duplex mode, signals going in one direction share the capacity of the link with signals going in other direction.

⑨ What is network? Explain network criteria and type of connection.

→ A network is the interconnection of a set of devices capable of communication. In this defination, a device can be host such as large computer, desktop, laptop, workstation, cellular phone.

Network criteria:

1) Performance: Pefermance can be measured in many ways, including transist time and response time. Pefermance is often evaluated by two networking metrics: throughput and delay.

We often need more throughput and less delay. However, these two criteria are often contradictory.

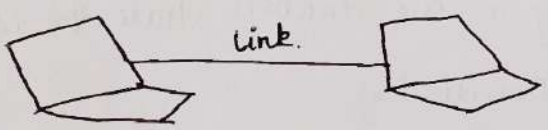
2) Reliability: Network reliability is measured by the frequency of failure the time it takes a link to recover from a failure. and the network robustness in a catastrophe.

3) Security: Network security issues include protecting data from unauthorized access, protecting data from damage. & development & implementing policies. and procedures for recovery from breaches and data losses.

Types of connection:

1) 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 of the point to point connections we can actual length of wire or cables to connect the two ends.

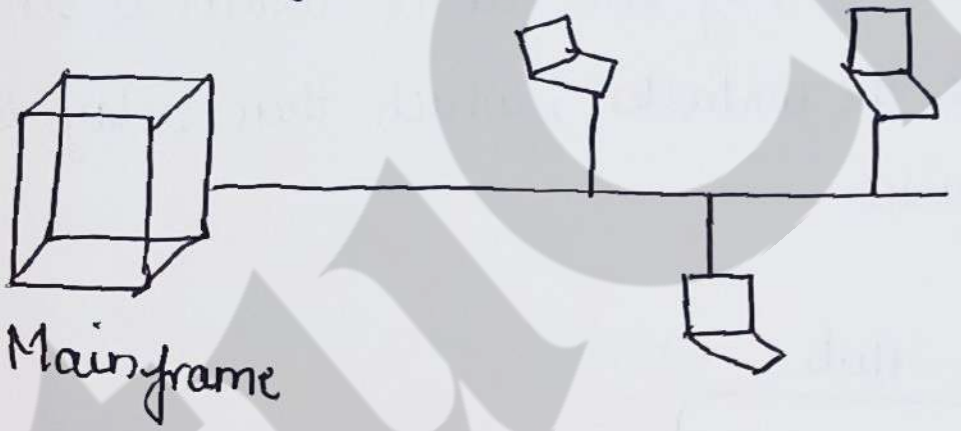


(17)

(5)

2) Multipoint : A multipoint connection is one in which more than two specific devices share a single link

In multipoint environment, the capacity of the channel is shared, either spatially or temporally.



(15) What is computer networking? Explain local area network in detail with neat diagram.

→ Computer networking: Computer networking is the process of connecting two or more computing devices and allowing them to share resources and exchange data.

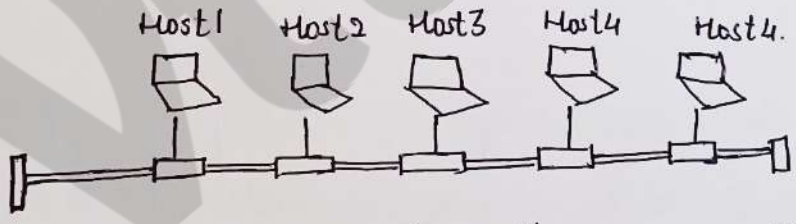
Local Area Network (LAN):

1) A local area network is usually privately owned and connects some host in a single office., building or campus.

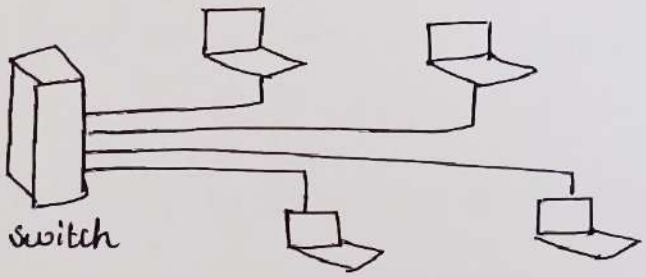
2) Depending on the needs of an organization, a LAN can be as simple as two PC's and a printer in someones home office, or it can extend throughout a company and include audio and video devices.

3) 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 to another host carries both the source hosts and the destination host's addresses.

4) In past all host network were connected through a common cable, which meant that a packet sent from one host to another was received by all hosts.



Lan with common cable.



Lan with a switch.

Module 2

① Explain flow control and error control.

→ Flow control:

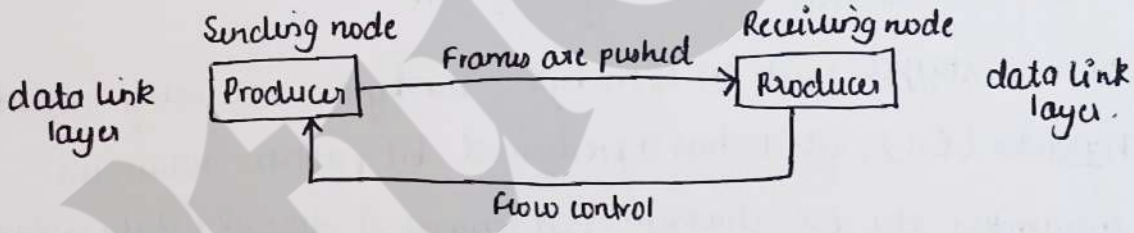
1) Flow control coordinates the amount of data that can be sent before receiving an acknowledgment.

2) In communication at data link layer, we are dealing with four entities, network and data link layer are at the sending node and network and data link layers at receiving node.

3) The data link layer at the sending node tries to push frames toward the data-link layer at receiving node.

4) If the receiving node cannot process and deliver the packet to its network at the same rate the frames arrive, it becomes overwhelmed with frames

5) Flow control in this case can be feedback from the receiving node to the sending node to stop or slow down pushing frames.



Error control

1) Error control is both error detection and error correction.

2) It allows receiver to inform the sender of any frames lost or damaged in transmission and coordinates the retransmission of those frames by sender.

3) In datalink layer, the term error control refers primarily to method of error detection and retransmission.

4) Error control in datalink layer is often implemented simply: Any time an error is detected in an exchange, specified frames are retransmitted. This process is called automatic repeat request.

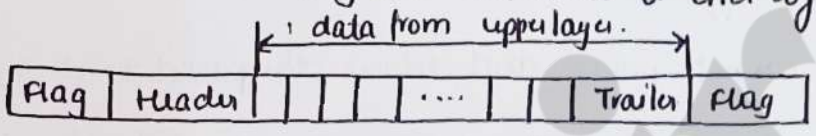
② What is framing? Explain byte and bit stuffing in detail.

→ Framing in the datalink layer seprates a message from one source to a destination, or from other messages to other destination, by adding a sender address and a destination address.

* Byte stuffing (Character-oriented protocols):

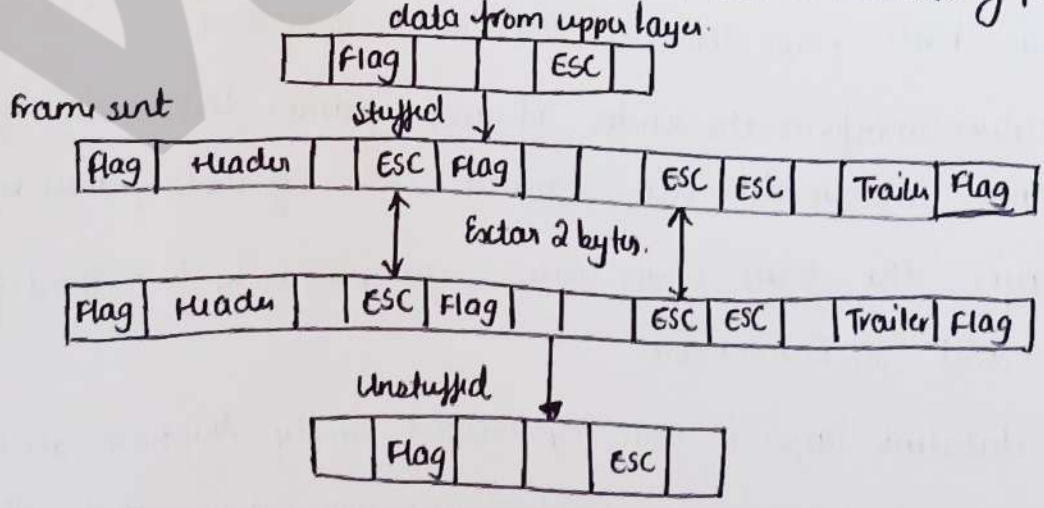
1) In a character-oriented protocol, data to be carried are 8 bit characters ~~by data link layer~~. from a coding system such as ~~ASC~~ ASCII

2) To seprate one frame from the next, an 8 bit flag is added at the beginning and the end of the frame. The flag is composed of protolol dependent special characters, signals the start or end of a frame.



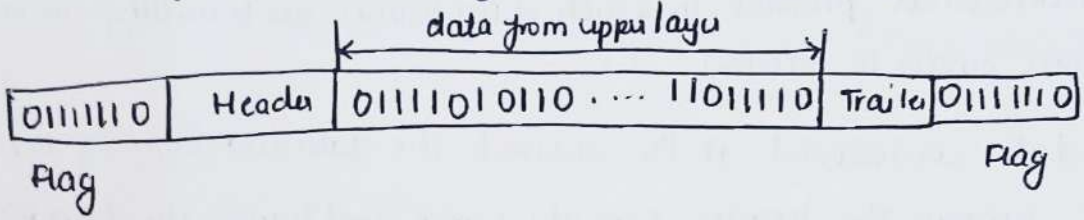
3) Any pattern for the flag could also be part of the information. If this happens, the receiver, when it encounters this pattern in the middle of the data, thinks it has reached the end of the frame.

4) The data section is stuffed with an extra byte. The byte is usually called the escape character (ESC), which has a predefined bit pattern. Whenever the reciever encounters the ESC character, it removes it from the data section and treats next character as data, not a delimiting flag.



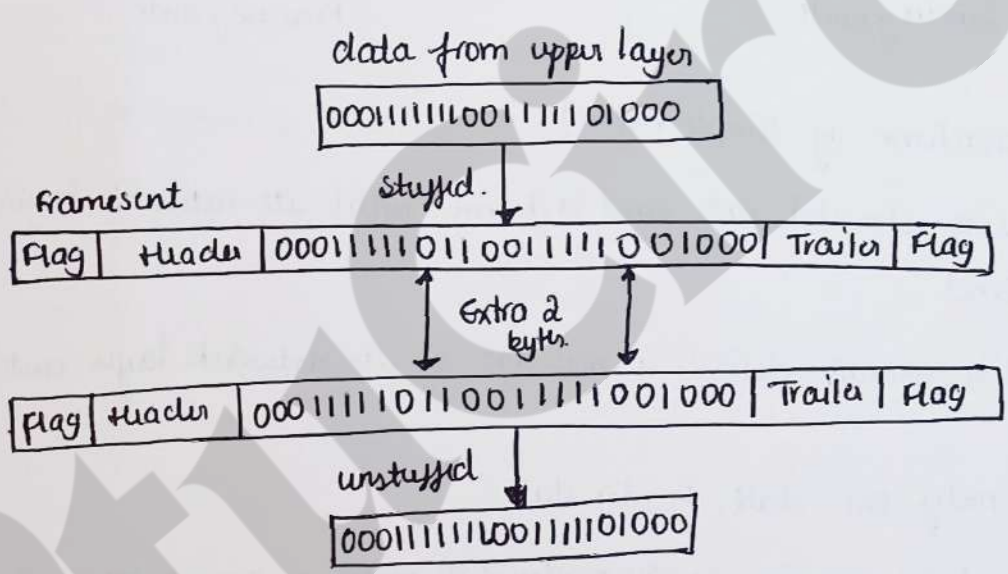
★ Bit stuffing: (Bit oriented protocol):

1) Most of the protocols use a special 8-bit pattern flag 01111110 as the delimiter to define the beginning and the end of the frame.



2) If the flag pattern appears in the data, we need to somehow inform the receiver that it is not the end of the frame.

3) This is done by stuffing 1 sigle bit, if we encounter 0 followed by five 1's instead of ESC byte.

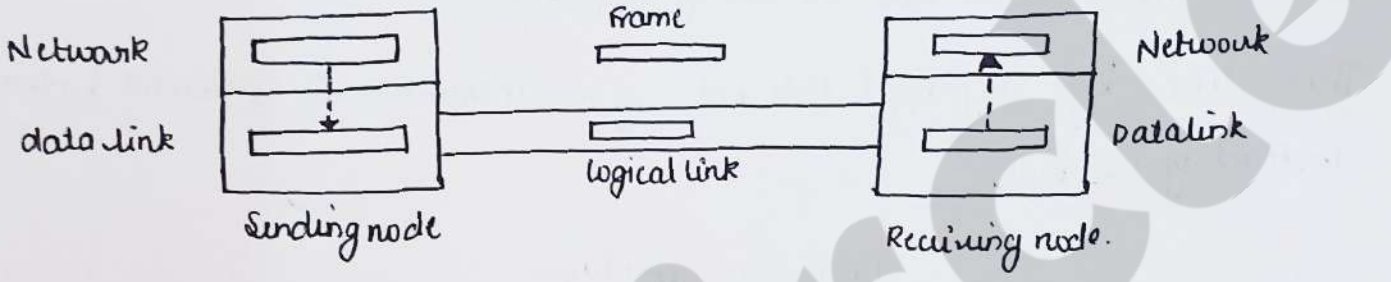


(3) Explain data link layer protocol (Simple, stop and wait, piggybacking)

→ Simple protocol:

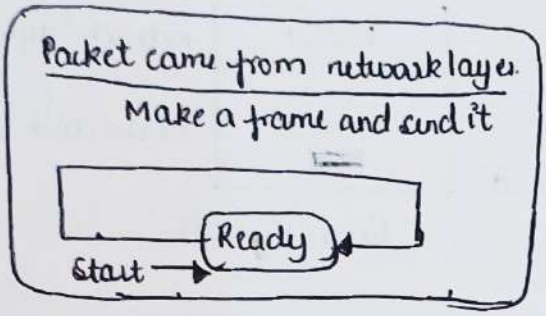
1) It is a unidirectional protocol in which data frames are travelling in only one direction from sender to receiver.

2) Once the data is received at the received the data link layer of the receiver immediately removes the header from the frame and hands the data packet to its network layer, which can also accept the packet immediately.

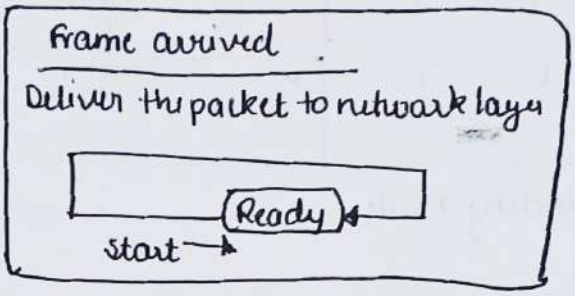


Finite state machine of Simple Protocol:

1) The sender site should not send a frame until its network layer has a message to send.
2) The receiver site cannot deliver a message to its network layer until a frame arrives.
3) Each FSM has only one state: Ready state.
4) The sending machine remains in the ready state until a request comes from the process in the network layer.
5) When the event occurs, the sending machine encapsulates the message in a frame and sends it to ~~network layer~~ receiving machine
6) The receiving machine remain in ready state until a frame arrives from the sending machine
7) When the event occurs, the receiving machine decapsulates the message out of the frame and delivers it to the process at the network layer.

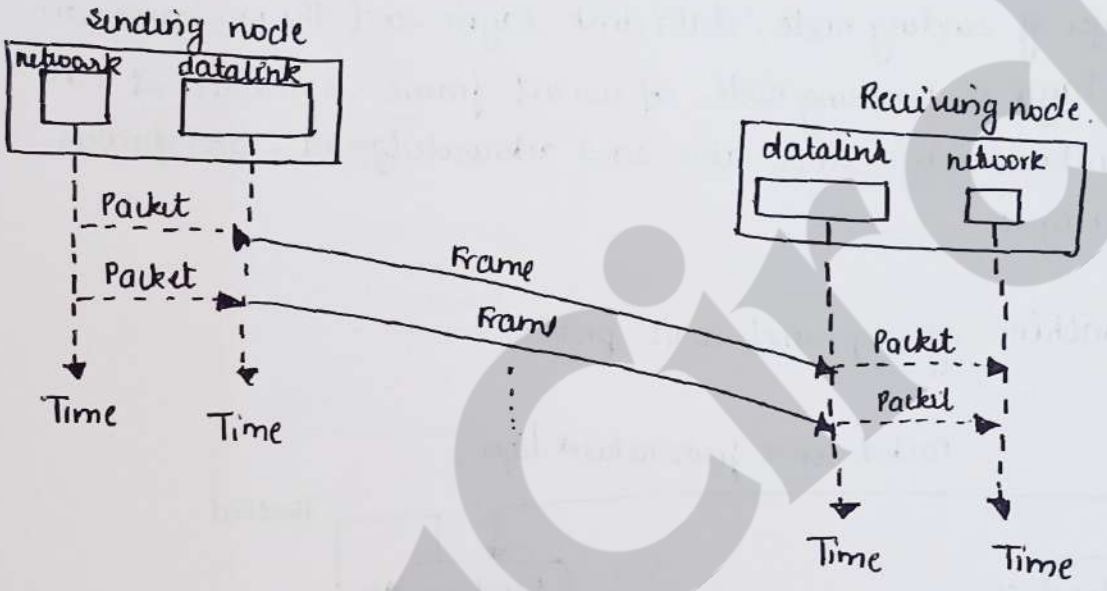


Sending Node

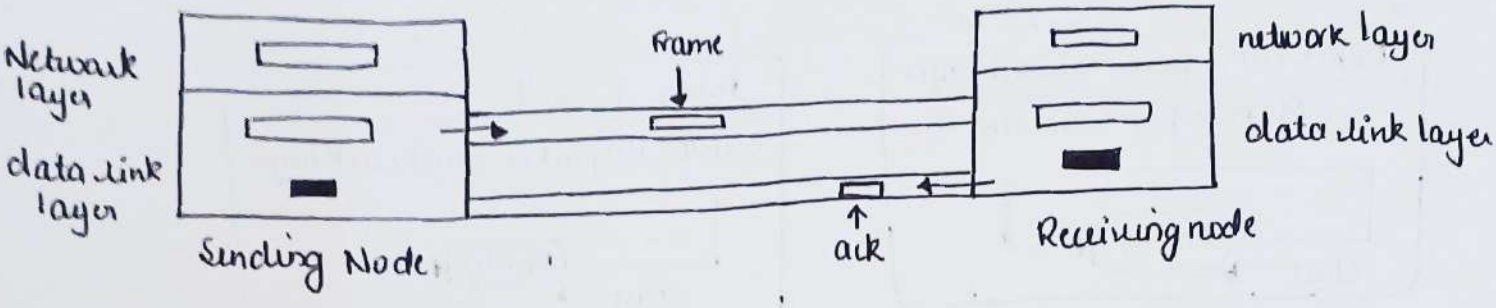


Receiving node.

Flow diagram:



* Stop and wait protocol.

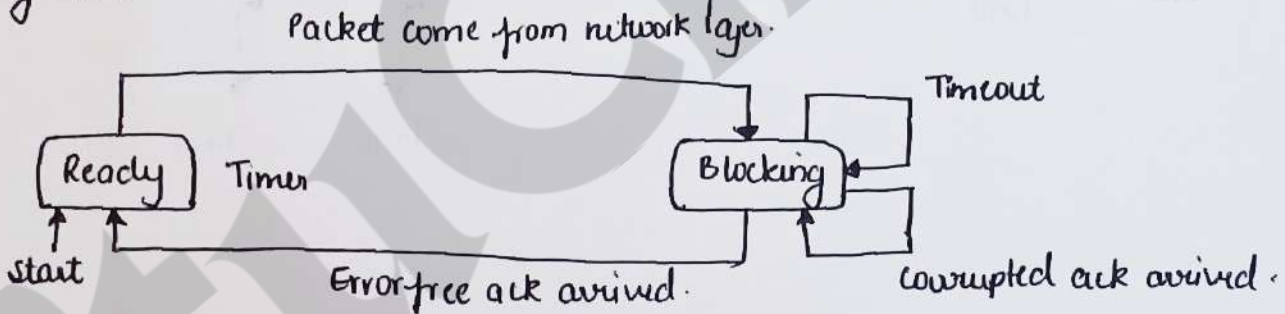


Stop and wait protocol supports both flow and error control.

The network layer from the sending node prepare some packet and send to data link layer of sending node, data link layer send the pkt frame to the datalink layer of Receiving node, if correct frame is received it will forward to network layer and also send acknowledgment, and further continues the cycle.

Finite state machine of stop and wait protocol.

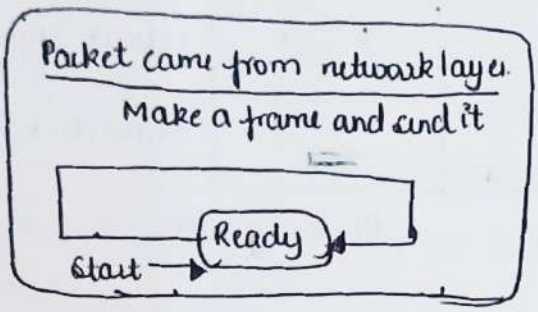
* Sending node.



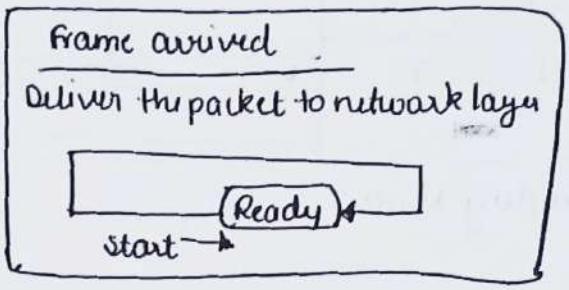
1) Sending nodes has two states: Readystate, and Blocking state.

2) In Ready state it receive frame from network layer and make frame and saves a copy and sets timer.

3) In Blocking state: 1) When Timeout occurs it resends the frame
   2) Corrupted acknowledgment arrives it discards the acknowledgment
   3) If the error free acknowledgment arrives it stop the timer.

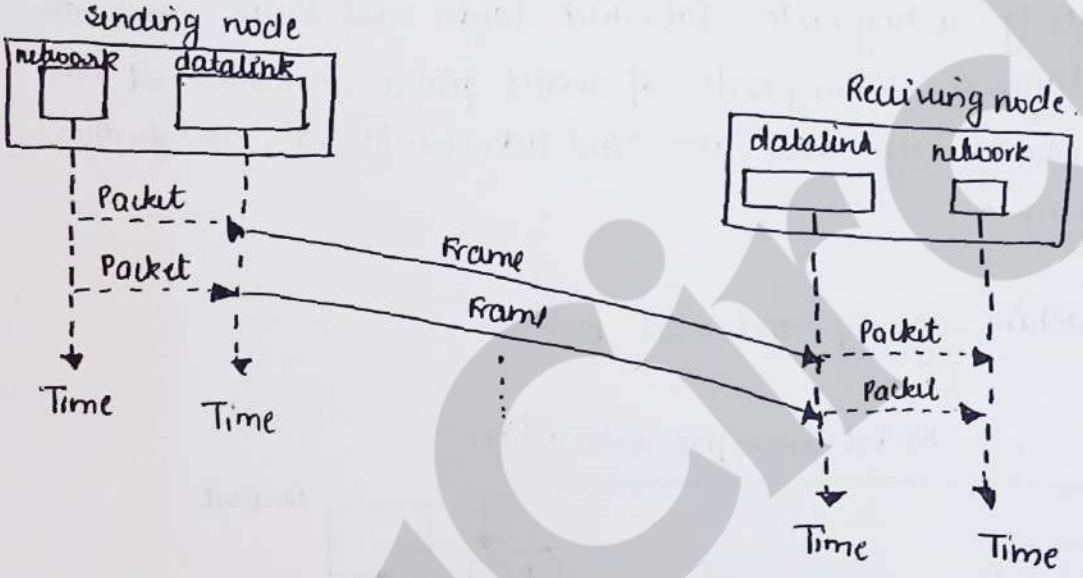


Sending Node

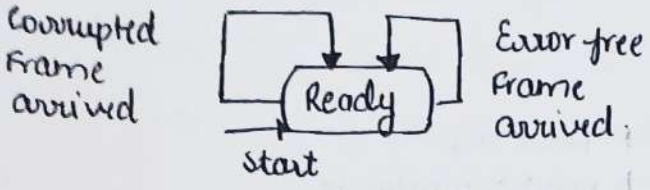


Receiving node.

Flow diagram:

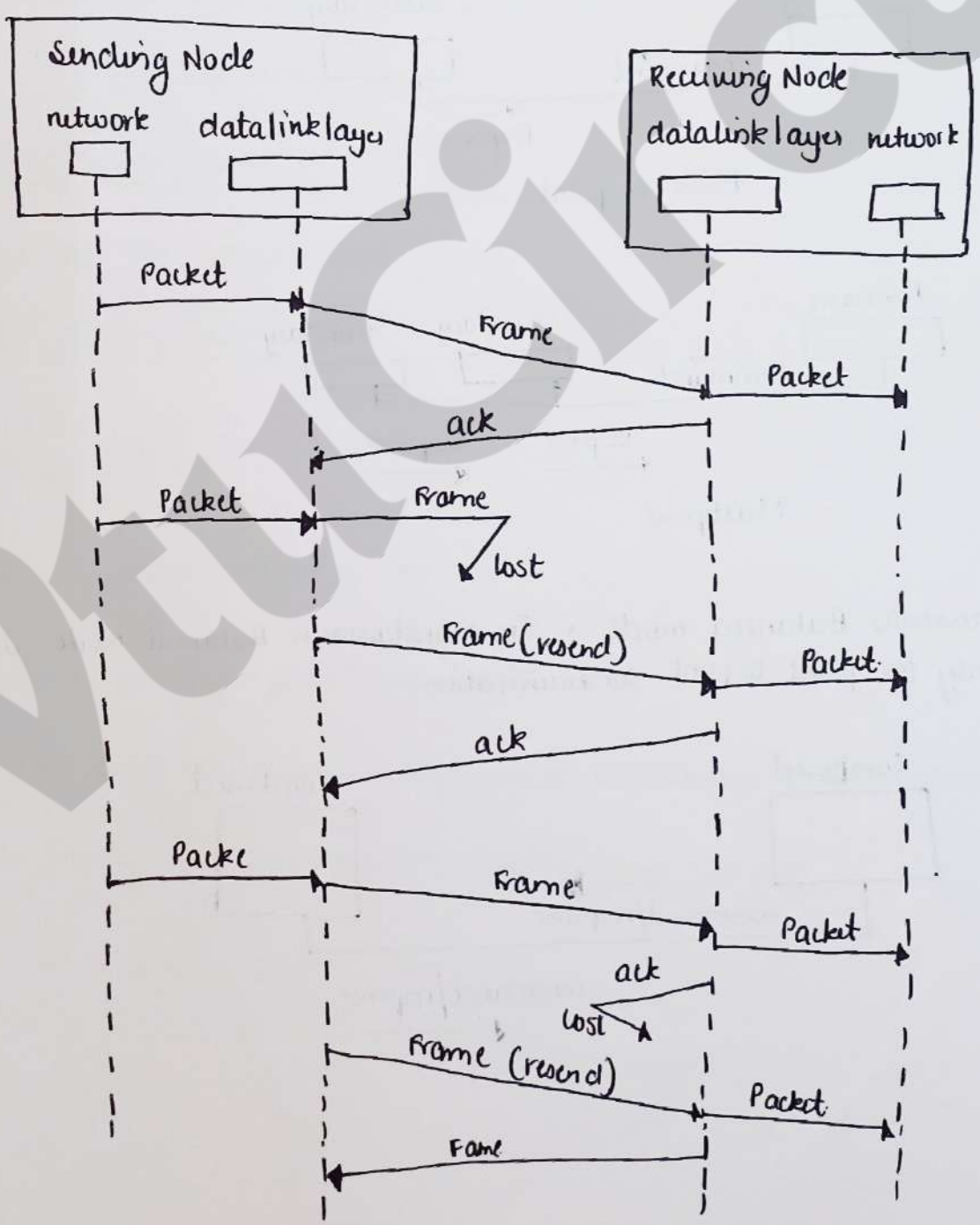


* Receiving node



1) In Receiving node it performs two action
   a) If error free frame arrives it deliver packet to next upper layer
   b) If corrupted frame arrive it discards the layer.

Flow diagram.



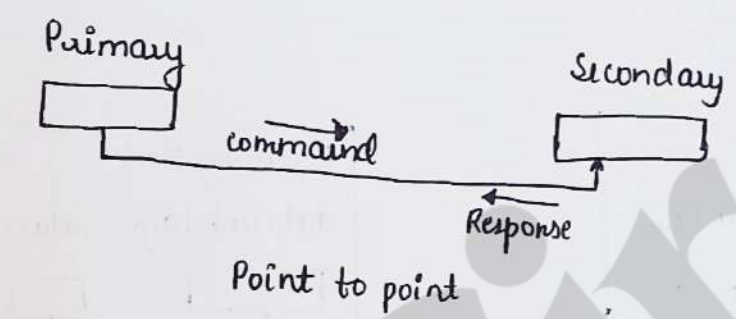
(4) Explain in detail HDLC protocol. (8)

→ High level data link control.

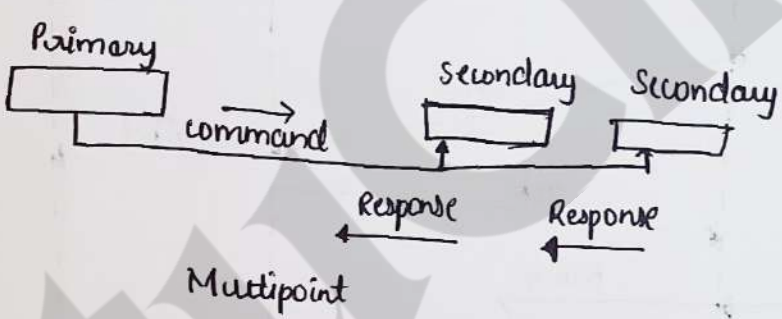
1) HDLC is bit oriented protocol → point to point
→ point to multipoint

2) HDLC protocol provides two Transfermodes i) Normal Response mode
ii) Asynchronous Balanced mode

i) Normal Rspose mode: In normal Response mode the station configuration is unbalanced.

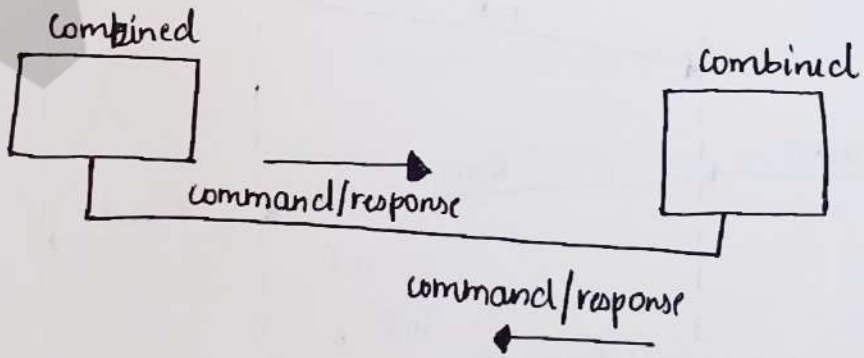


Point to point



Multipoint

2) Asynchronous Balanced mode. : In asynchronous Balanced mode it can be used only for point to point communication

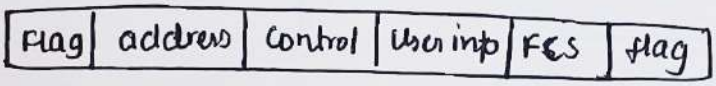


* Framing: In HDLC it provide three types of frame:

1) Information Frame → user data information
2) Supervisory Frame → control information
3) Unnumbered Frame → system management

Structure of a frame

1) HDLC frame for Information frame.



2) HDLC frame for Supervisory frame

3) HDLC frame for unnumbered frame.

* 1) Flag: 01111110

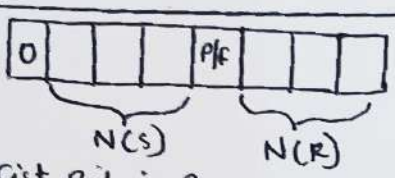
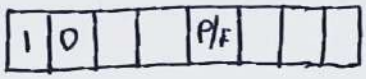
2) Address: It contain address of stations.

3) Control field: Used for flow / error control

4) Information field: Contain user information or Management information

5) FCS: Frame check sequence :→ identify error detection.

* Control field format.

Information frame	Supervisor frame	Unnumbered frame.
		
1) Fist Bit is 0 2) Neext 3 bit: N(S) 3) Last 3 bit: N(R) 4) Bit B/w N(S) & N(R) is P/F	1) First two bit is 10 2) Last 3 bit - N(R) 3) 5th bit: P/F 4) 3rd & 4th bit: code	1) First two bit = 11 2) Neext 3rd & 4th bit - code 3) 5th bit = P/F 4) Last 3 bits - N(R).

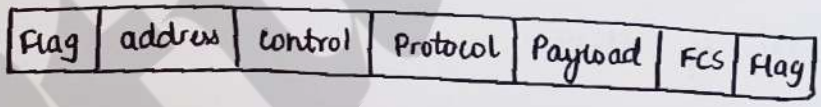
(5) Explain in detail point to point protocol.

→

1) The services provided in point to point protocol are ~~Aun~~ Authentication and frames and also multilink.

2) The services not provided in point to point protocol are flow control, it will support only error control.

3) Framing in point to point protocol



Flag: 01111110

address: The address field in this protocol is a content value and set of 11111111

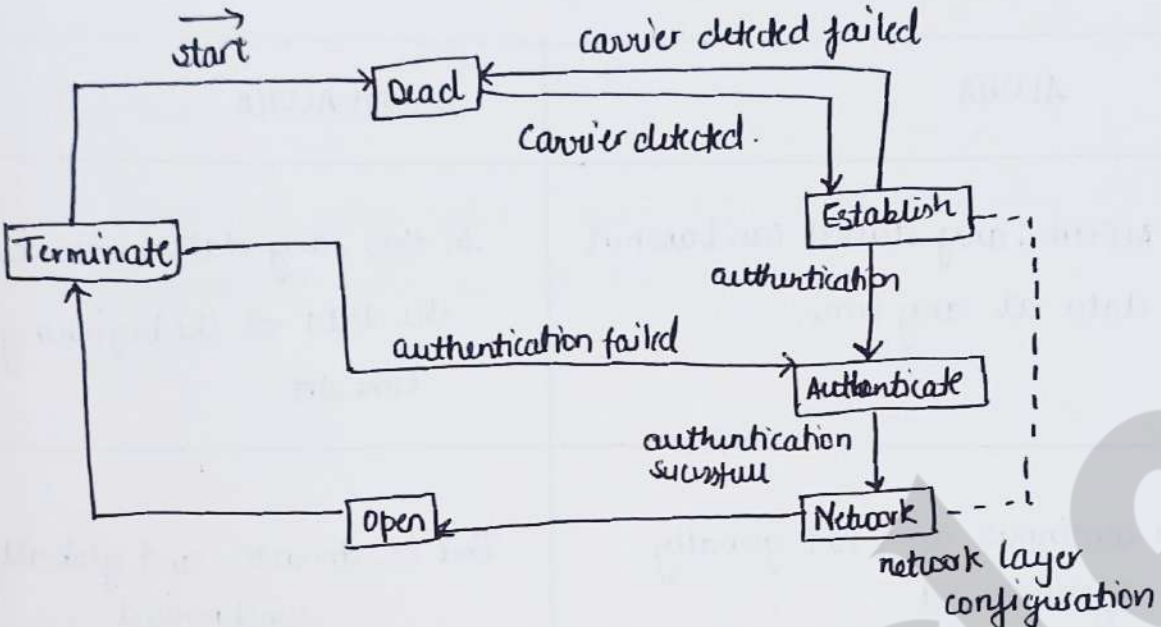
Control: This field is set to constant value 11000000

Protocol: The protocol field defines what is being carried in data field.

Payload: Payload contain actual data of 1500 bytes.

FCS: Frame check sequence is simply a 2byte or 4byte standard CRC

4) Transition phases.



1) Dead state: In dead phase the link is not being used. There is no active carrier and the line is quiet.

2) Establish: when the node starts communication, the connection goes into this phase, in this phase if the negotiation is sucessfull the system goes to authentication or directly to networking phase.

3) Authenticate: The authentication phase is optional, if the result is sucessful the connection goes to networking phase otherwise it goes to termination phase.

4) Network: In network phase, negotiation for the network layer takes place and the PPP supports multiple protocols at network layer.

5) Open: In open Phase data transfer takes place. When a connection reaches this phase, the exchange of data packets can be started.

6) Terminate: In termination phase, the connection is terminated.

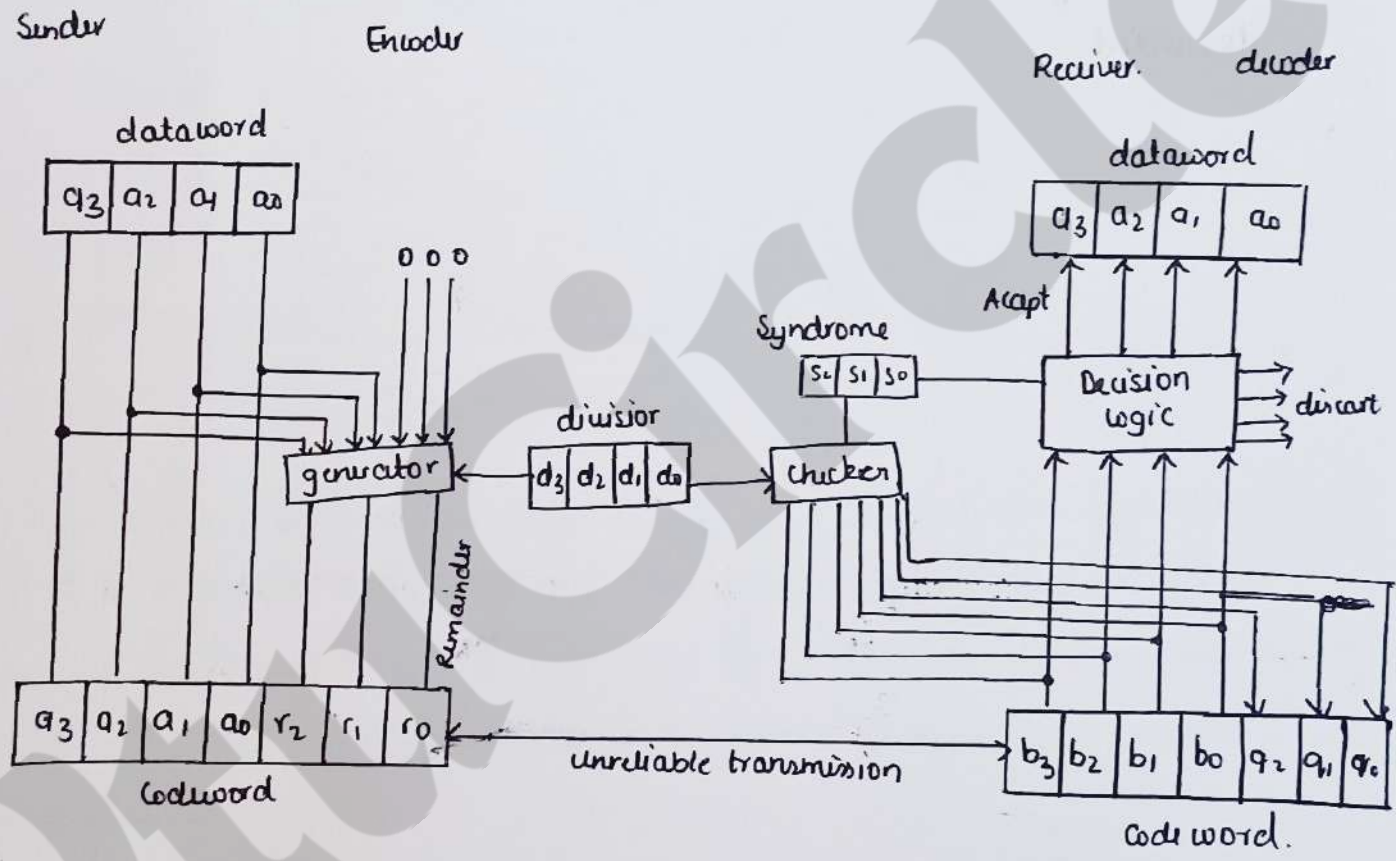
(6) What is the difference between ALOHA and slotted ALOHA.

→ ALOHA	Slotted ALOHA
1) In the ALOHA, any station can transmit the data at any time	In this, any station can transmit the data at the beginning of any time slot.
2) Time is continous and not globally synchronized	Time is discrete and globally synchronized.
3) Vulnerable time for aloha = $2 \times Tt$	Vulnrable time for ~~stand~~ slotted aloha = Tt
4) Probability of sucessfull transmission of data packet = $G \times e^{-2G}$	Probability of sucessfull transmission of data packet = $G \times e^{-G}$
5) Maximum efficiency = 18.4%.	Maximum efficiency is 36.8%.
6) Pure aloha doesn't reduce the number of collision to half	Slotted aloha reduces the number of collision to half and doubles the efficiency of aloha.

(7) Explain CRC encoder and decoder for 4 bit dataword.

→ Cyclic Redudancy check

It is a subset of cyclic codes called the cyclic redudancy check, which is used in networks such as LAN and WANs



In encoder:

1) The dataword has k bits (4), and the codeword has n bits (7)
2) The size of the dataword is agumented by adding n-k (3 here) 0s to the right hand side of the word. The n bit result is fed into generator.
3) The generator uses a divisior n-k+1 (4 here), predefined and agreed upon. The generator divides the agumented dataword by divisior (modulo 2 division)
4) The quotient of division is discarded, the remainder (r_2, r_1, r_0) is appended to dataword to create codeword.

In decoder

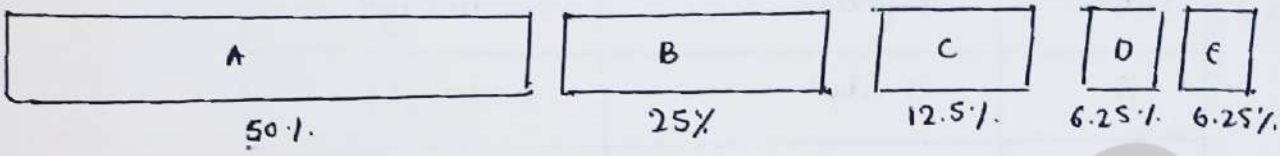
1) Receives the possibly corrupted codeword
2) A copy of all n bits is fed to the checker which is replica of generator.
3) The remainder produced by the checker is a syndrome of n-k (3here) bits, which is fed to decision logic analyzer.
4) The analyzer has a simple function. If the syndrome bits are all as, the 4 left most bit of codeword are accepted as the dataword, otherwise 4 bits are discarded.

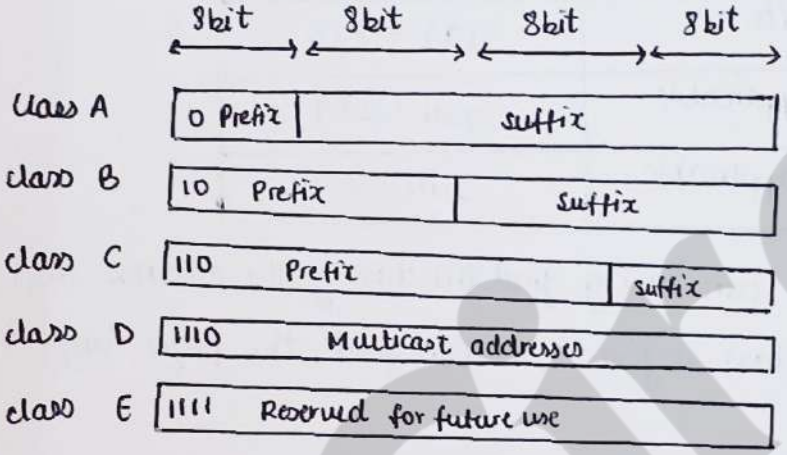
Module 3

Computer Networks

(1) Explain classful addressing system with a neat diagram.

→





1) When the Internet started, an IPv4 address was designed with a fixed length prefix, but to accomodate both small and large networks, three fixed length prefix were designed instead of one (n = 8 , n = 16 and n = 24). The whole address space was divided into five classes (class A, B, C, D, E). This scheme is reffered to as classful addressing.

2) In class A, the network length is 8 bits, but since the first bit which is 0, defines the class, we can have only seven bits as network identifier. This means there are only $2^7 = 128$ networks in the world that can have a class A address.

3) In class B, the network length is 16 bits, but since the first two bit which are $(10)_2$ define the class. we can have only 14 bits as network identifier. This means there only $2^{14} = 16,384$ networks in the world that can have a class B address.

4) In class C, the network length is 24 bits, but since the first three bit which are $(110)_2$ defines the class, we can have only 21 bit as network identifier. This means there are only $2^{21} = 2,097,152$ networks in the world that can have a class C address.

5) Class D is not divided into prefix and suffix. It is used for multicast addresses. All addresses that start with 1111 in binay belong to class E. As in class D, class E is not divided into prefix and suffix and is used to reserve.

6)

Class	Prefixes	First byte
A	n = 8 bits	0 - 127
B	n = 16 bits	128 - 191
C	n = 24 bits	192 - 223
D	Not applicable	224 - 239
E	Not applicable	240 - 255

7) In classful address we can easily find the class of the address and since the prefix length for each class is fixed, we can find the prefix length immediately.

(2) Write Dijkstra's algorithm to compute shortest path with an example.

→ Dijkstra's algorithm computes the least cost path from one node to all other nodes in the network.

D(v): cost of the least path from the source node to destination v as of this iteration of algorithm.

P(v): previous node along current least cost path from the source to v

N': subset of nodes.

Initialization
N' = {u}
for all nodes v
if v is a neighbor of u
then D(v) = c(u,v)
else D(v) = ∞

Loop
find w not in N' such that D(w) is a minimum

add w to N'

update D(v) for each neighbor v of w and not in N'

$D(v) = \min(D(v), D(w) + c(w,v))$

until N' = N.

Ex: Consider a network graph with nodes A, B, C, D and the following weights

From	To	weight
A	B	1
A	C	4
B	C	2
B	D	6
C	D	3
C	E	5
D	E	2

step 1: Initialization

Node	Distance from A	Previous Node
A	0	-
B	∞	-
C	∞	-
D	∞	-
E	∞	-

step2: Start at A

Node	Distance from A	previous node
A	0	-
B	1	A
C	4	A
D	∞	-
E	∞	-

step3 : visit B

Node	Distance from A	Previous node
A	0	-
B	1	A
C	3	B
D	7	B
E	∞	-

step4: visit C:

Node	Distance from A	previous node
A	0	-
B	1	A
C	3	B
D	6	C
E	8	C

step5: visit D

Node	Distance from A	Previous node
A	0	-
B	1	A
C	3	B

D E	6 8	C D

Final shortest path:

A → B = 1

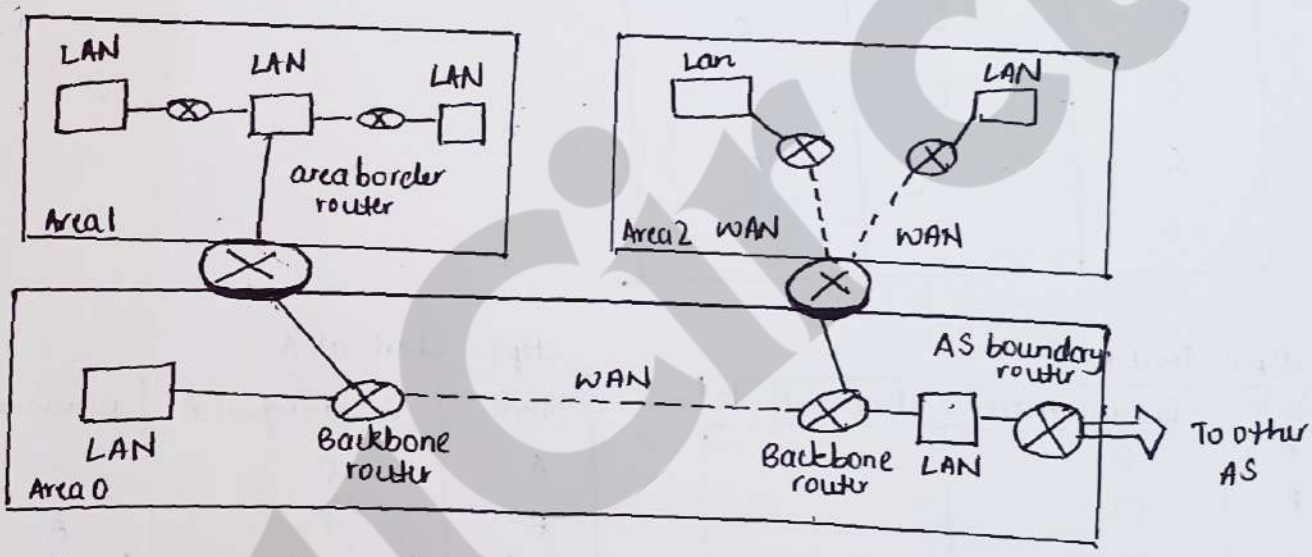
A → C = 3

A → D = 6

A → E = 8

(3) Explain open shortest path first protocol with an example.

→



1) OSPF is an internal routing protocol
2) OSPF is based on linkstate routing
3) For handling the routing efficiently and in a timely manner, the OSPF divides an autonomous system into areas.
4) OSPF uses dijkstra's algorithm to create forwarding table.
5) Unlimited hop count
6) OSPF calculates the cost of reaching destination from a source by considering link weights, which can vary based on the the other type of service.
7) OSPF messages are encapsulated in IP datagrams with a protocol field value of 89
8) OSPF uses 5 message types:

a) HELLO Message (Type1): Used by routers to introduce themselves and announce their own neighbour.

b) Database description Message (Type2): Sent in response to Hello messages, allowing routers to acquire the full LSDB

c) Link State Request (Type3): Sent when a router requires a specific LS information

d) Link State Update (Type 4): The primary message used to build the LSDB, with the version for each type of link.

e) Link state acknowledgment (Type5): Provides reliability by confirming receipt of link state updates.

Example

Routers R1, R2, R3, R4

Links: R1 - R2 : cost 10
R1 - R3 : cost 5
R2 - R4 : cost 15
R3 - R4 : cost 10

Dijkstra's algorithm from R1

Shortest Path to R2 = R1 → R2 ⇒ cost 10
Shortest Path to R3 : R1 → R3 ⇒ cost 5
Shortest Path to R4
via R2 - R1 = cost 25
via R3 - R1 = cost 15
Choosen path : R1 → R3 → R4 = Cost 15

Routing table for R1

Destination R2: Next to hop R2 : cost 10
Destination R3 : Next to hop R3 : cost 5
Destination R4 : Next to hop R4 : cost 15.

(4) Expain DHCP protocol. (6)

→

1) DHCP stands for dynamic host configuration protocol.
2) DHCP works on a client-server mode
3) DHCP protocol automatically assigns IP addresses to devices present in network
4) It simplifies network management by eliminating the need for manual IP configuration.

Working of DHCP protocol

1) DHCP DISCOVER

When a new device connects to a network, it broadcasts a DHCP DISCOVER message to find a DHCP server. This is sent because the device doesn't yet have an IP address.

2) DHCP OFFER

DHCP server on the network receives an DHCP DISCOVER request and responds with a DHCP OFFER message. Message contain an available IP address, subnet mask and other network configuration.

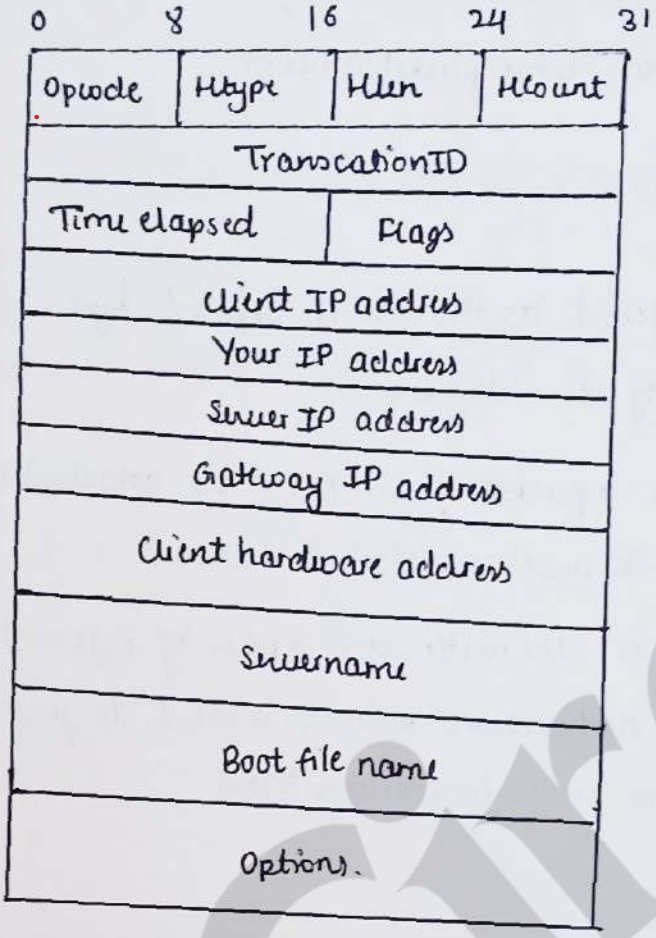
3) DHCP REQUEST

client has selected a specific server's offer and replies with a DHCP REQUEST message to indicate acceptance of the IP address offered.

4) DHCP acknowledgement: DHCP PACK

The DHCP server responds with a DHCP PACK message and officially assigns the IP address to the client for a specific lease duration. The client can now use the IP address.

DHCP message format.



Importance:

1) Centralized management of IP addresses
2) Ease of adding new clients to network
3) Reuse of IP addresses reduces total number of IP address that are required.

(5) Define and explain routing and forwarding in network layer.

→ Routing:

1) The network layer is responsible for routing the packet from its source to destination.
2) A physical network is a combination of network and router to connect them.
3) The network layer is responsible for finding the best one among these possible routes. The network layer has specific strategies to to define best route.

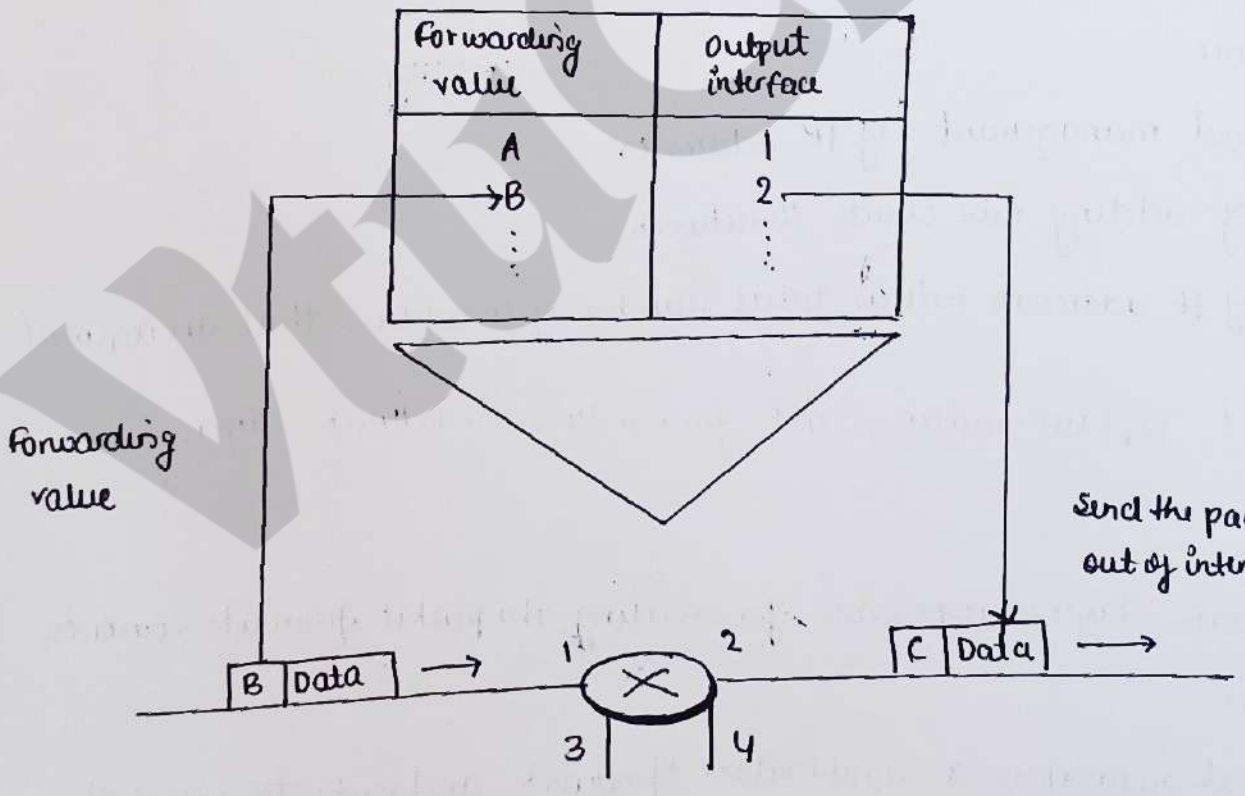
4) In internet today, this is done by some routing protocols to help the routers to coordinate their knowledge about their neighborhood and to come up with consistent table to be used when packet arrives.

Forwarding

1) Forwarding can be defined as the action applied by each router when a packet arrives at one of its interfaces.

2) When a router receives a packet from one of its attached networks, it needs to forward the packet to another attached network.

3) To make this decision, the router uses a piece of information in packet header, which can be destination address or a label, to find the corresponding output interface number in the forwarding table.

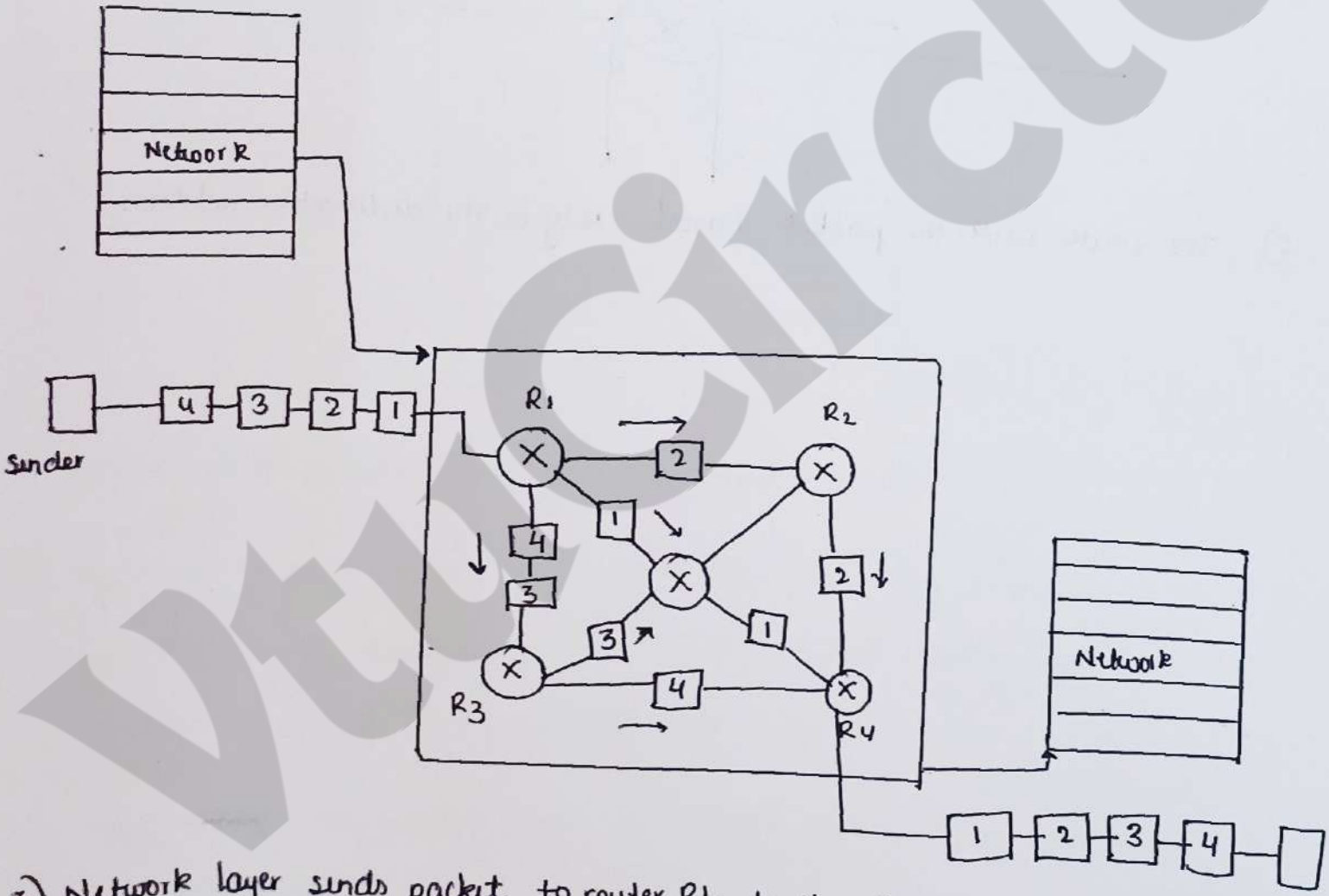


(6) Explain network layer packet switching (Datagram approach, Virtual circuit) (9)

→ Datagram approach

1) Router: A Router is a switch that creates a connection between in an input port and output port.

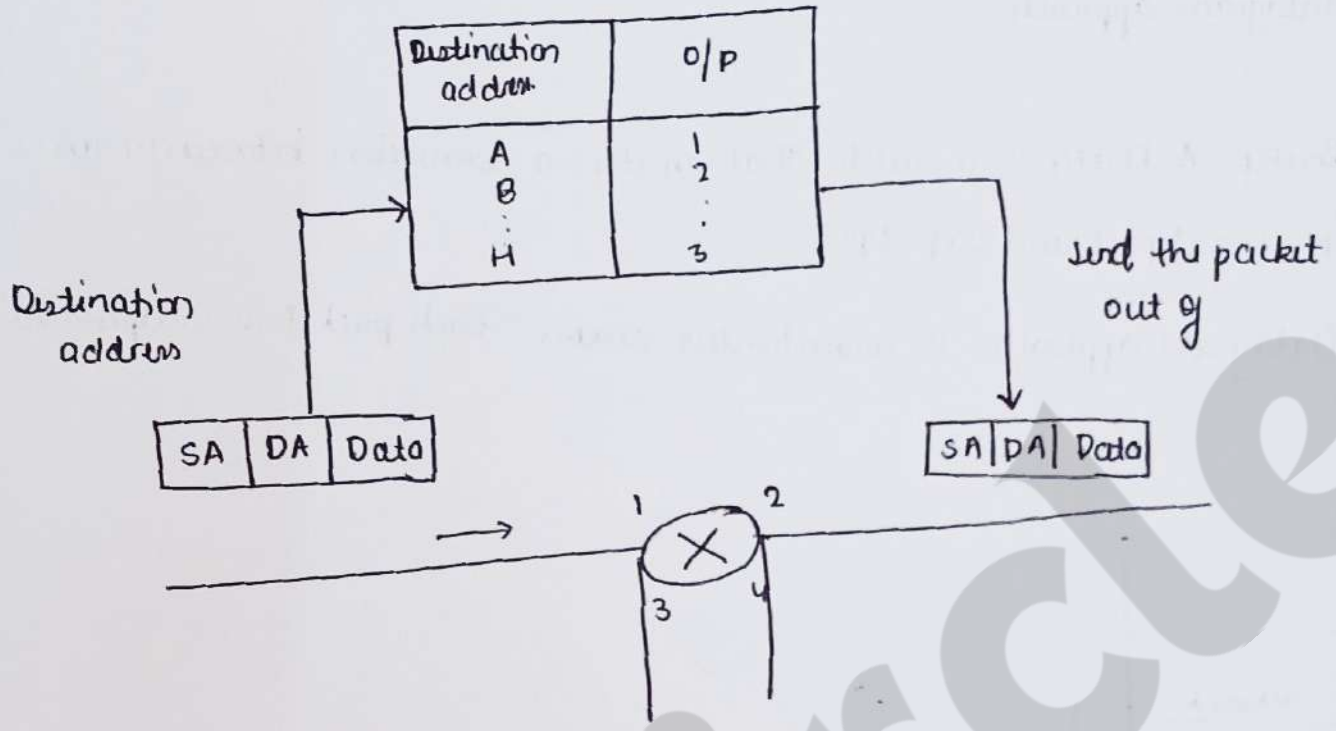
2) Datagram approach is connectionless service: Each packet is independent



3) Network layer sends packet to router R1, further the router R1 will send packet to any other ports. Somehow the packet are received at receiver and then it transfers to network layer.

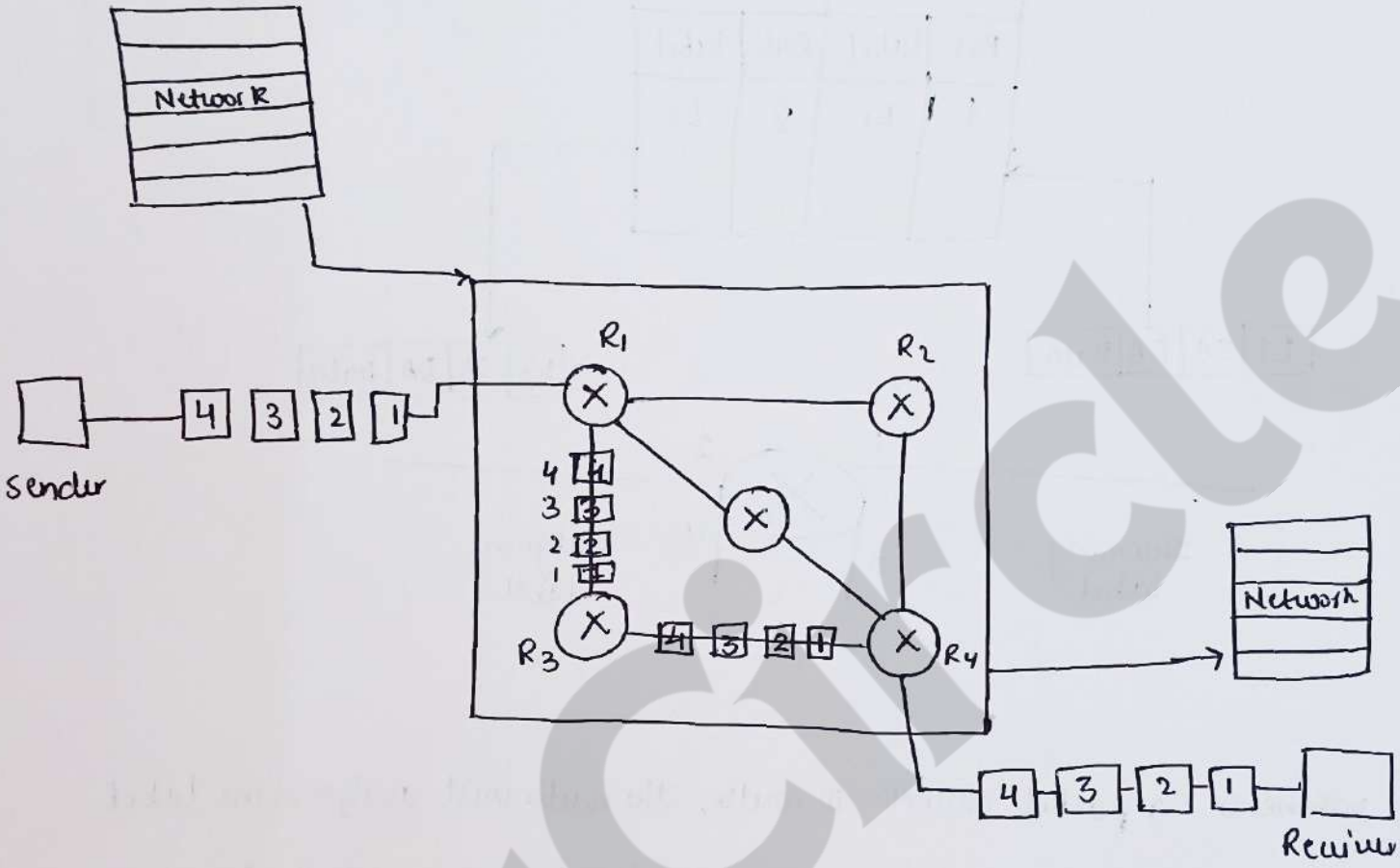
4) The packet sent will not be the actuall manner, how the sender sent it.

5) Datagram approach forwarding table



6) The router routes the packet based only on the destination address

* Virtual circuit approach.



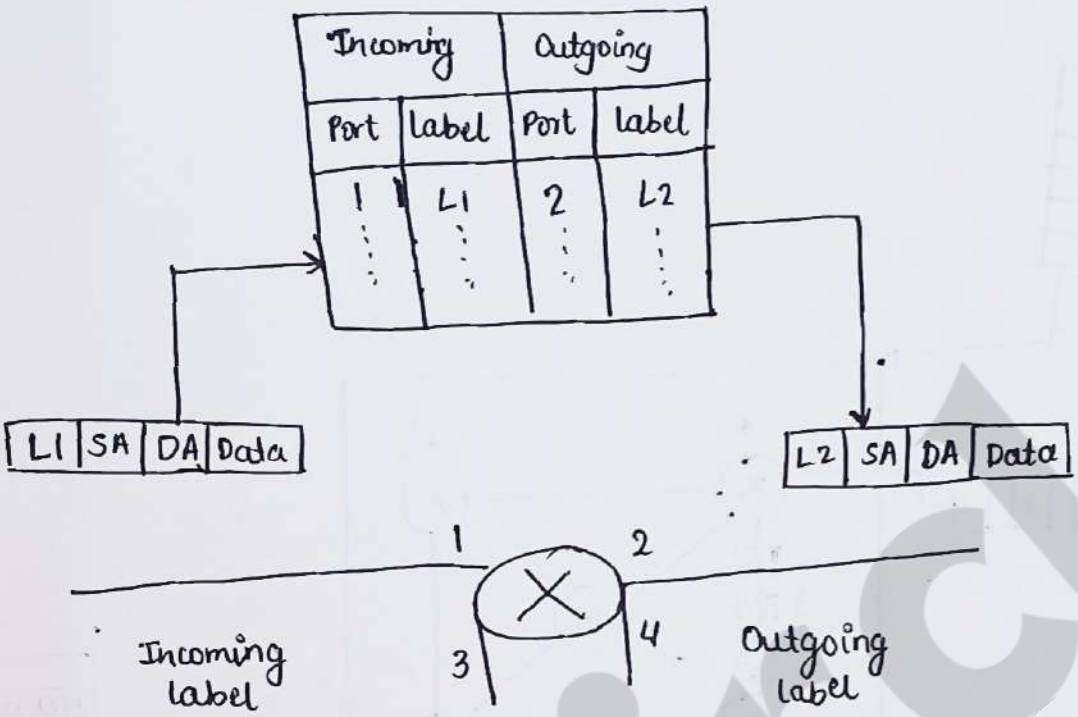
1) Virtual circuit approach is a connection oriented service

2) Before all the packets that have been sent from the sender to Receiver a path will be established between sender and receiver, after that all the packet follow the particular path.

3) Along with the packet, there is another variable called virtual circuit identifier.

4) The packet sent will be in the same manner how sender ~~sent~~ sent it

5) Virtual circuit forwarding table



6) Whenever a packet arrives to router, the router will assign some label, its sequence number. Router assigns the label and send to next port with other labelling.

7) There are 3 phases in virtual circuit.

i) Setup Phase: In setup phase, a router creates an entry for a virtual circuit.

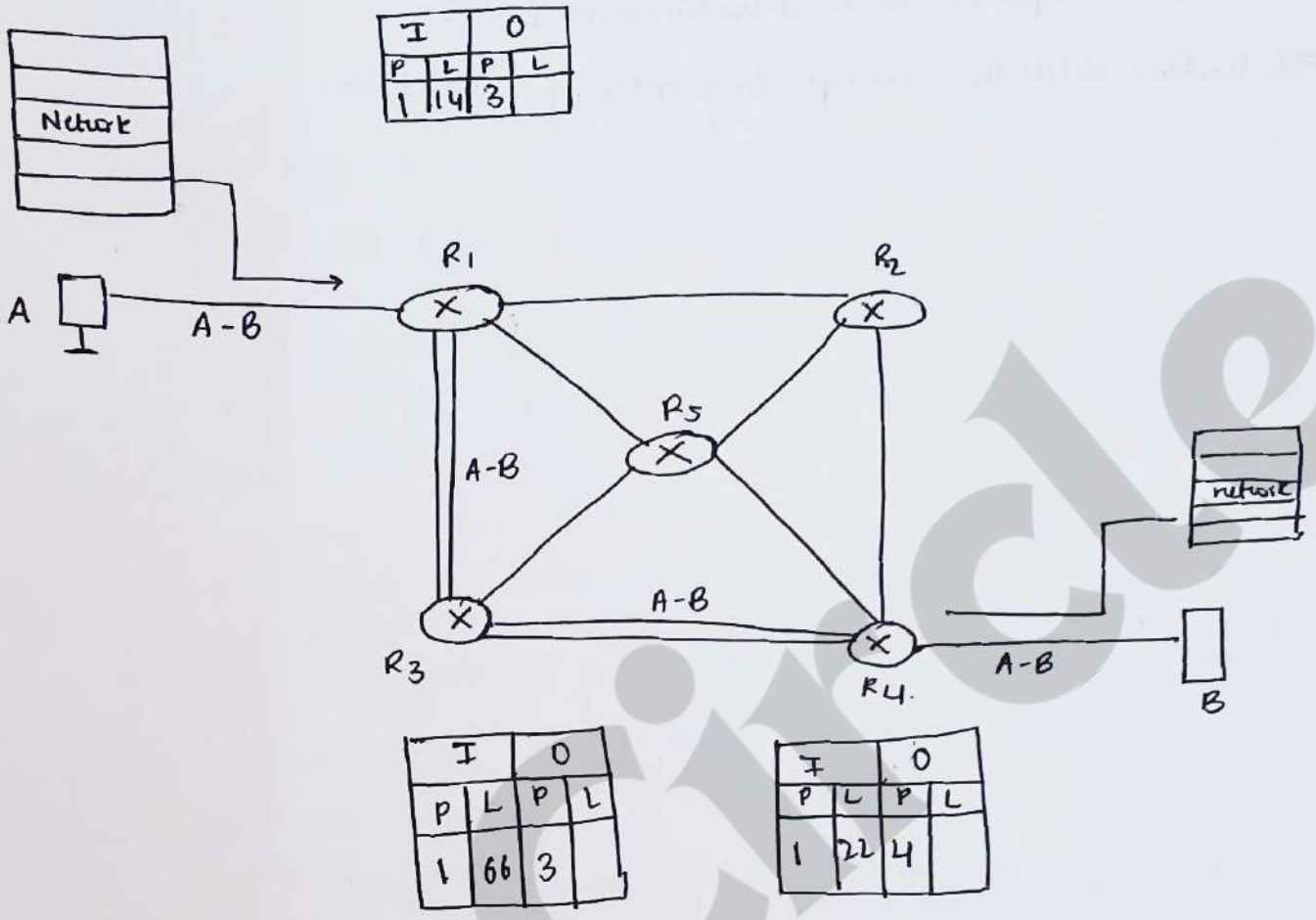
a) Source A sends a request packet to router R1

b) Router R1 receives the request packet

c) Router R3 recieves the setup request packet

d) Router R4 receives the setup request packet

e) Destination B receives the setup packet, and if it is ready to receive packet from A, it assigns a label to incoming packets that come from A

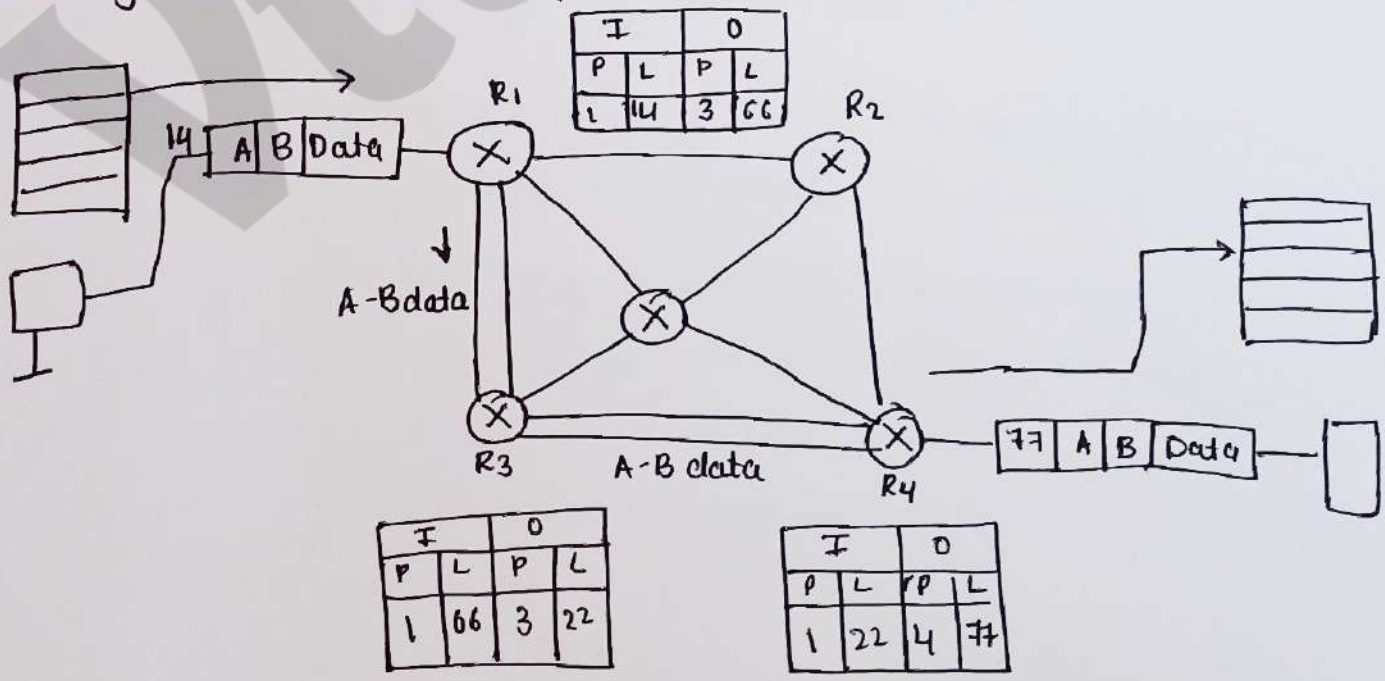


I		O	
P	L	P	L
1	14	3	

I		O	
P	L	P	L
1	66	3	

I		O	
P	L	P	L
1	22	4	

2) Datatransfer phase: After all the routers have created their forwarding table for a specific virtual circuit, then the network layer packet belonging to one message can be sent one after another.



I		O	
P	L	P	L
1	14	3	66

I		O	
P	L	P	L
1	66	3	22

I		O	
P	L	P	L
1	22	4	77

3) Teardown phase: In teardown phase, source A, after sending all packets to B send a special packet called teardown packet.

Destination B responds with a confirmation packet

All routers delete the corresponding entries from their tables.

Write a program for Bellman ford algorithm.

```
import java.io.*;
import java.util.Scanner;
class dist_vec{
public static void main(String args[]){
int dmat[][];
int dist[][];
int via[][];
int n=0,i=0,j=0,k=0,count=0;
Scanner in = new Scanner(System.in);
System.out.println("enter the number of nodes\n");
n = in.nextInt();
dmat = new int[n][n];
dist = new int[n][n];
via = new int[n][n];
System.out.println("enter the cost matrix\n");
for(i=0;i<n;i++)
for(j=0;j<n;j++){
dmat[i][j] = in.nextInt();
dmat[i][i]=0;
dist[i][j]=dmat[i][j];
via[i][j]=j;
}
do{
count=0;
for(i=0;i<n;i++)
for(j=0;j<n;j++)
for(k=0;k<n;k++)
if(dist[i][j]>dmat[i][k]+dist[k][j]) {
dist[i][j]=dist[i][k]+dist[k][j];
via[i][j]=k;
count++;
}
}while(count!=0);
for(i=0;i<n;i++)
{
System.out.println("state value for router"+i+" is");
for(j=0;j<n;j++){
System.out.println("To "+j+" -Via "+via[i][j]+" distance is "+dist[i][j]);
}}}}
```

Module 4

(1) Explain Transport layer services Process to Process Communication in detail.

→

1) The Transport layer is responsible for providing services to application layer, it receives services from the network layer.

2) The first duty of the transport layer protocol is to provide process to process communication. A process is an application entity that uses the services of the transport layer.

3) The network layer is responsible for for communication at computer level.

4) A network layer protocol can deliver the message only to the destination computer, however this is an incomplete delivery, the message still need to be handed to the correct process. This is where a transport-layer protocol takes over. A transport layer protocol is responsible for delivery of the message to the appropriate process.

Addressing port numbers

Although there are two ways to achieve process to process communication, the most common is through client-server paradigm.

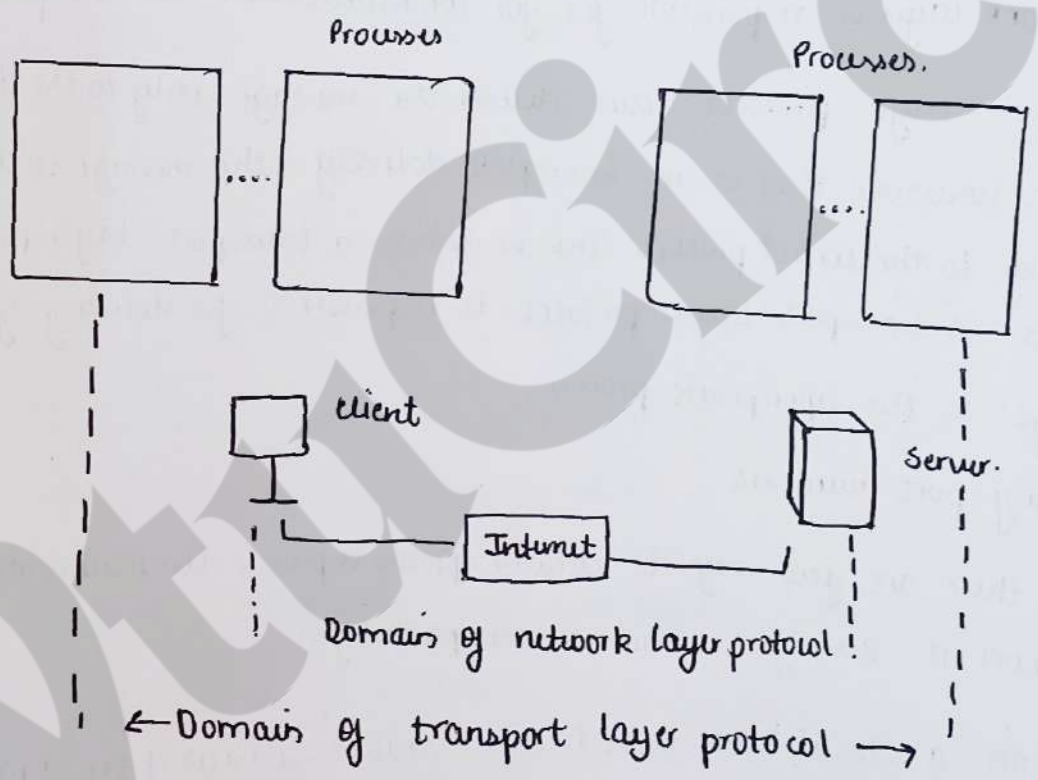
5) A process on a local host called client, needs services from a process usually on the remote host called server.

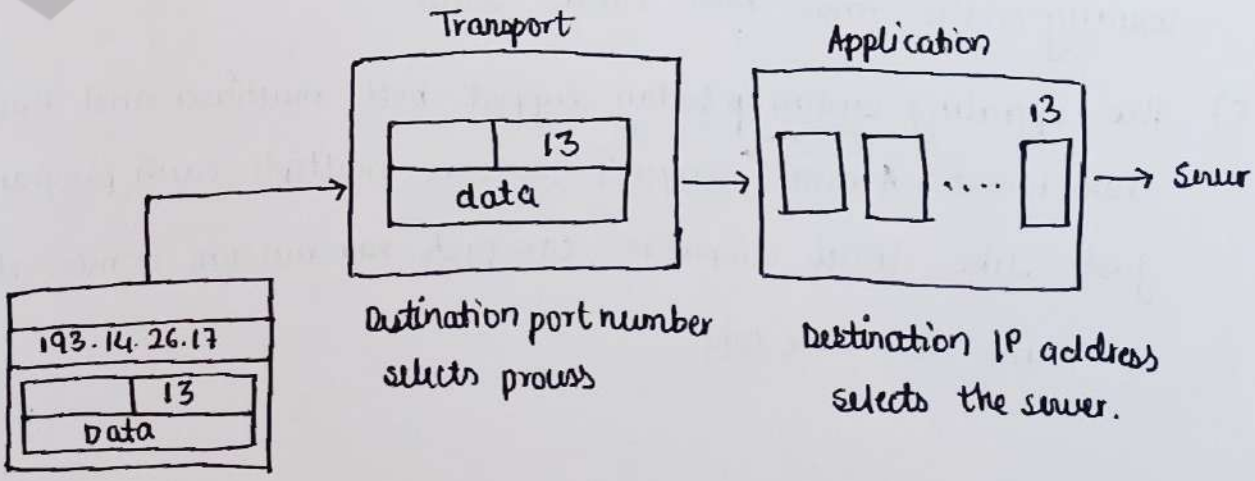
6) The operating system today support both multiuser and multiprogramming environment. A remote computer can run multiple server program at once just like local computers can each run one or more client programs at same time.

1) For communication, we must define the local host, local process, remote host, remote process. The local host and remote host are defined using IP addresses. To define the processes, we need port numbers (0 - 65,535)

2) The client program defines itself with a port number called the ephemeral port number. The word ephemeral means "short lived" and it is used because the life of a client is normally short.

3) The server program must also define itself with a port number. TCP/IP has decided to use universal port numbers for servers. these are called well known port numbers.





(2) List the services and application of TCP.

→ The services of the TCP are

1) Process to process communication: TCP provide process to process communication using port numbers.

2) Stream delivery Services: TCP allows the sending process to deliver data as a stream of bytes and allows the receiving process to obtain data as a stream of bytes.

3) Sending and Receiving Buffers: Because the sending and receiving processes may not necessarily write or read data at the same rate, TCP needs buffer for storage. There are two buffers, the sending buffer and receiving buffer, one for each direction.

4) Segments: The network layer transmit data in packets, not as byte stream, TCP group bytes into stream, adds control header, and passes them to network layer for transmission, where they are encapsulated in IP datagram.

5) Full duplex Communication: TCP offer full duplex service, where data can flow in both directions at same time.

6) Multiplexing and demultiplexing: TCP performs multiplexing at sender and demultiplexing at receiver.

7) Connection oriented service: When a process at site A wants to send and receive data from another process at site B, three phase occurs.
   a) The two TCP establish a logical connection between them
   b) Data are exchanged in both directions.
   c) The connection is terminated.

8) Reliable service: It is uses an acknowledgement to check the safe and sound arrival of data.

Applications of TCP.

1) Web Browsing
2) Email
3) File transfer
4) Streaming Servies
5) Multiplayer games
6) Database communication
7) VPN

(3) List the servies and application of UDP.

→ The servicse provided by the UDP are

1) Procss to procss communication: UDP provides procss to procss ~~compu~~ communication using socket addresses.

2) Connitionless Servies: UDP provides connectionless servie, this mans that each user datagram sent by UDP is an independent datagram.

3) Flow control: UDP is very simple protocol. There is no flow control, and hence no window mechanism. The receiver may overflow with incoming messages.

4) Error control: There is no error control mechanism in UDP exp except for checksum

5) checksum: UDP checksum calculation includes 3 section, a pseudoheader, the UDP header, and data coming from application layer.

6) Congestion Control: Sinc UDP is a connectionless protocol, it does not provide congestion control.

7) Encapsulation and decapsulation: To send messages from one procss to another, the UDP protocol encapsulates and decapsulates messages.

8) Queuing: In UDP queues are associated with ports.

9) Multiplexing and Demultiplexing: UDP multiplexes and demultiplexes processes that may want to use the servi of UDP.

Applications of UDP are

1) UDP is suitable for a process that request simple request respone communication with little concern for flow and error control.

2) UDP is suitable for a process with internal flow and error control mechanism.

3) UDP is suitable for transport protocol for multitasking.

4) UDP is used for management process such as SNMP

5) UDP is used for route updating protocol.

6) UDP is normally used for interactive real time application

(4) Explain stop and wait protocol

→ 1) Stop and Wait is a connection-oriented protocol which uses both error and flow control

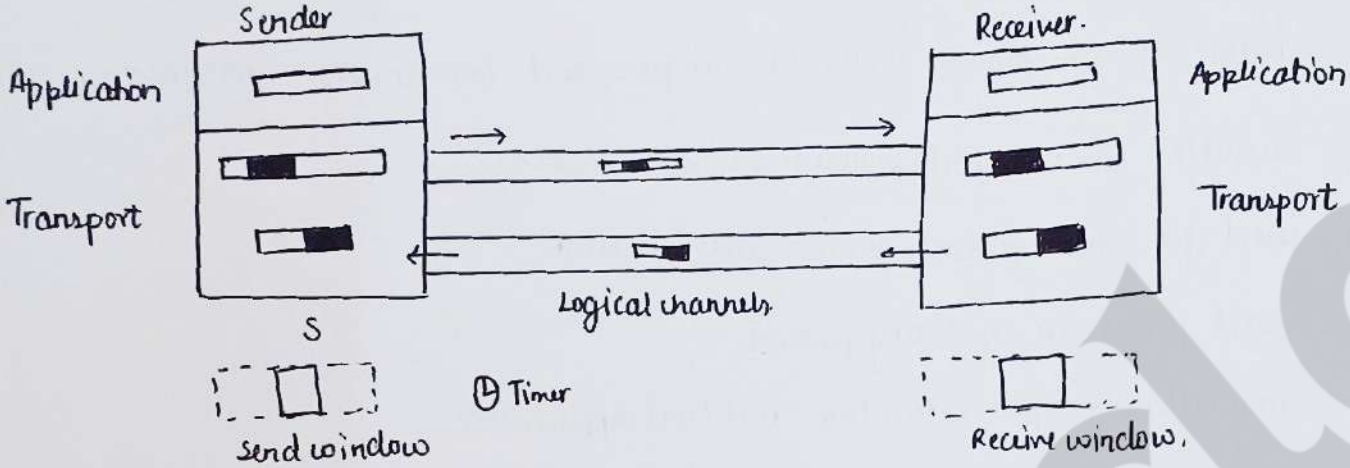
2) Both the sender and receiver use a sliding window of size 1. The sender sends one packet at a time and waits for an acknowledgement before sending the next one.

3) To detect corrupted packets, we need to add checksum to each data packet. When a packet arrives at the receiver site, it is checked. If its checksum is incorrect, the packet is corrupted and silently discarded.

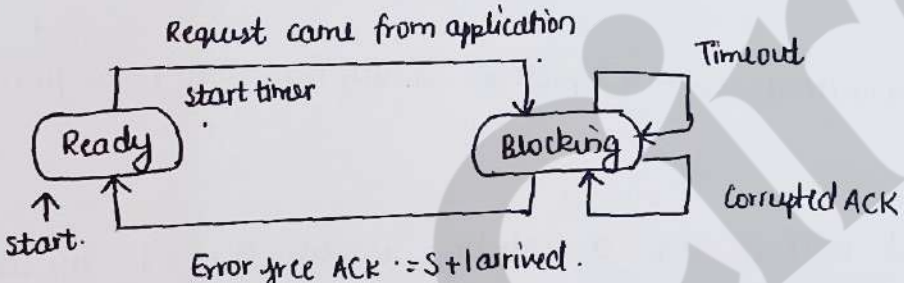
4) The silence of the receiver is a signal for the sender that a packet was either corrupted or lost. Every time the sender sends a packet it start timer.

5) If an acknowledgement arrives before the time expires, the timer is stopped and the sender sends the next packet.

6) If the timer expires, the sender resends the previous packet, assuming that the packet was corrupted or lost. This means that the sender need to keep a copy of packet until its acknowledgment arrives



Sender FSM



1) Sender is initially in ready state.

2) Ready state: when the sender is in this state, it is only waiting for one event to occur. If a request comes from application layer, the sender creates a packet with sequence number S, a copy of packet is stored. and packet is sent. The sender then start timer.

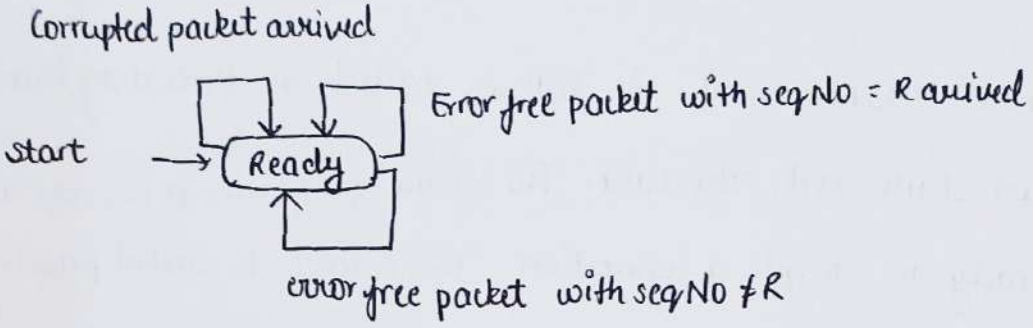
3) Blocking state: when sender is in this state, three event occur.

   1) In an error free ACK arrives with ackNo related to next packet to be sent, which means ackNo = (S+1) modulo 2, then the time is stopped. The window slides S=(S+1) modulo 2, finally moves to ready state.

   2) If a corrupted ACK arrives, the ACK is discarded

   3) If a time out occurs, the sender resends the packet and restart the timer.

FSM: Receiver.

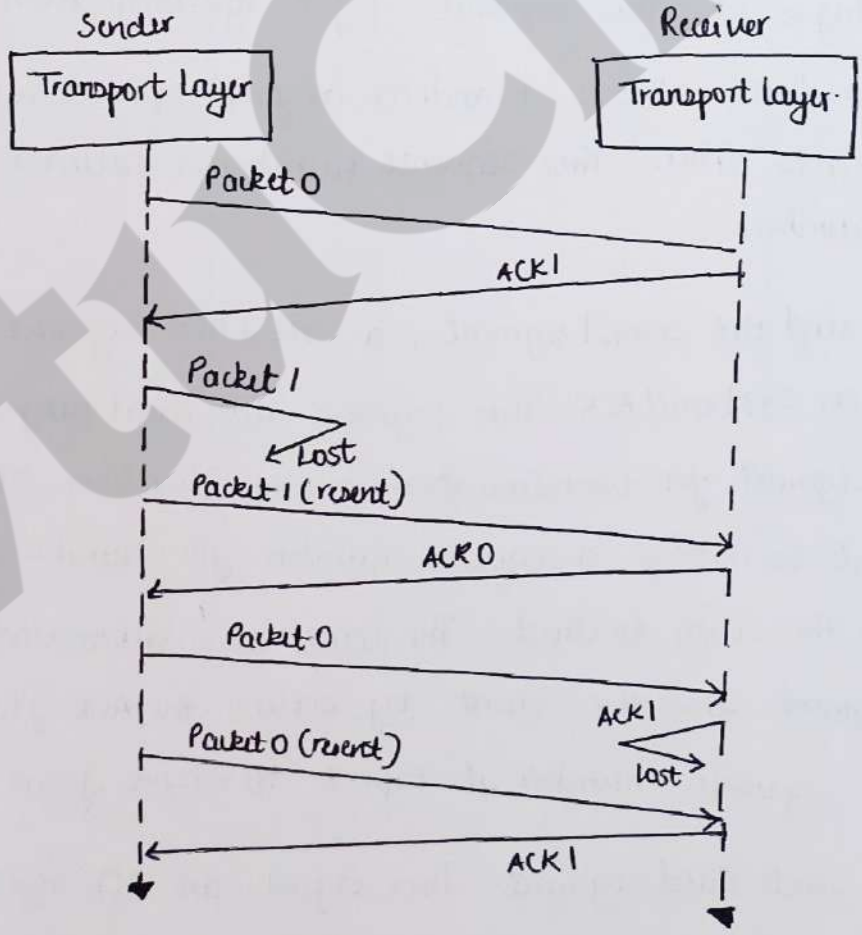


1) The receiver is always in ready state, Three event may occur

a) If an error free packet with seqno = R arrives, the message in the packet is delivered to application layer. The window slides R = (R+1) modulo 2.

b) If error free packet with seqNo ≠ R arrives, the packets are discarded but a ACK with ack No is sent.

c) If corrupted packet arrives, the packet is discarded.



(5) Explain connection establishment of TCP using 3 way handshaking.

→

1) The connection establishment in TCP is called as three way handshaking.

2) The process starts with the server. The server program TELLS its TCP that it is ready to accept a connection. This request is called passive open.

Although the server TCP is ready to accept a connection from any machine in the world., it cannot make the connection itself.

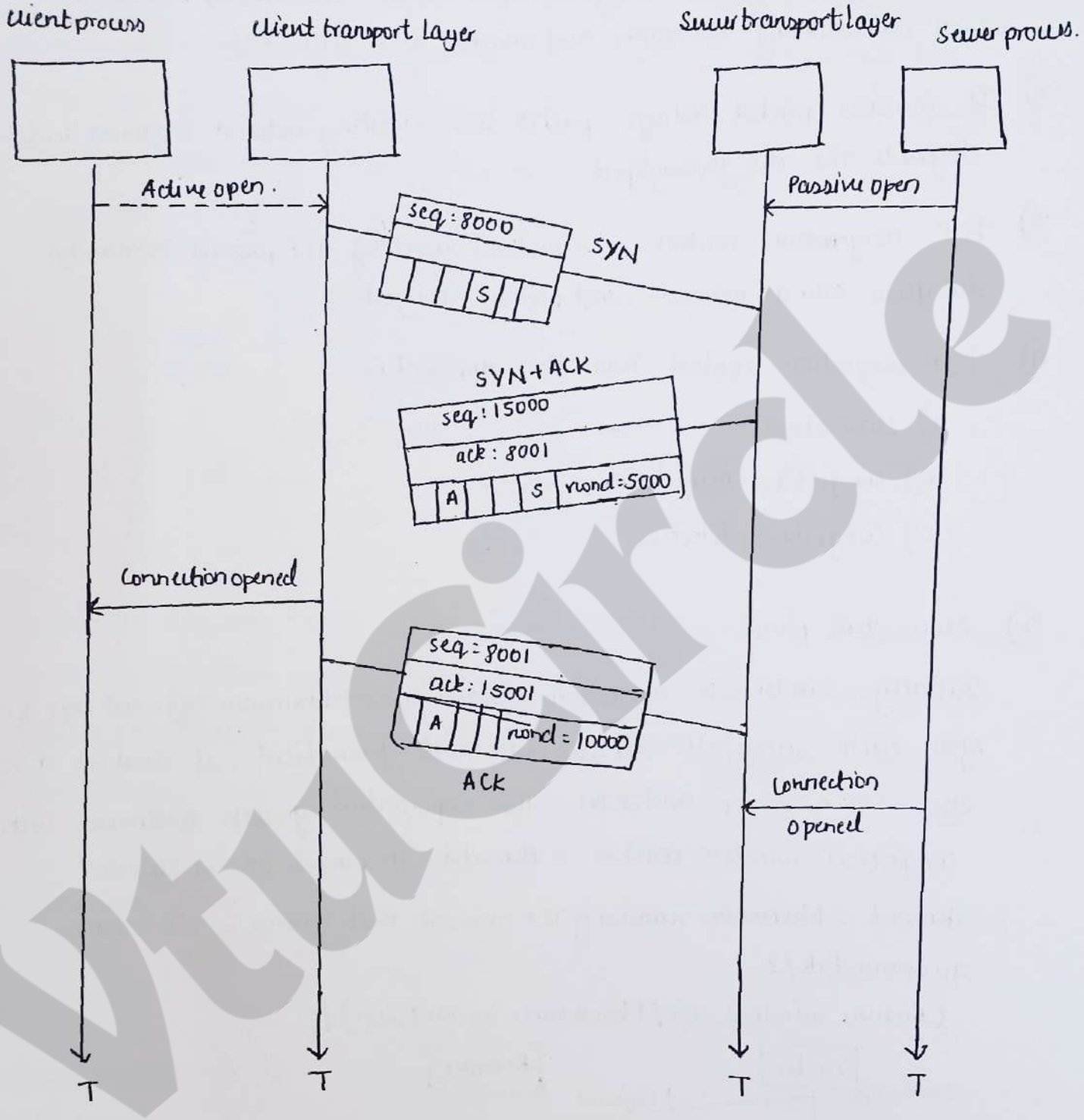
3) The client program issue a request for an active open. A client that wishes to connect to an open server tell it TCP to connect to a particular server. TCP can now start the three way handshaking process.

Three steps in this phase as follows.

i) The client sends the first segment, a SYN segment, in which only the SYN flag is set. This segment is for synchronization of sequence number. The client chooses a random as first sequence number and sends number to server. This sequence number is called as the initial sequence number.

2) The server send the second segment, a SYN + ACK segment with two flag bit set as SYN and ACK. This segment has dual purpose. First it is a SYN segment for communication in other direction. The server uses this segment to initilize a sequence number for numbering the bytes. sent from the server to client. The server also acknowledges the receipt of SYN segment from the client by setting the ACK flag and displaying the next sequence number it expects to receive from client.

3) The client sends third segment: This is just an ACK segment. It acknowledges the receipt of the second segment. with the ACK flag and acknowledges number field.


Client process
Client transport layer
Server transport layer
Server process.
Active open.
Passive open
seq: 8000
S
SYN
SYN+ACK
seq: 15000
ack: 8001
A
S
rwnd=5000
Connection opened
seq: 8001
ack: 15001
A
rwnd = 10000
ACK
Connection
opened
T
T
T
T

⑥ Explain TCP congestion control

→

1) Congestion happens when too many data packets are sent through a network which overwhelming the routers and switches that direct traffic.

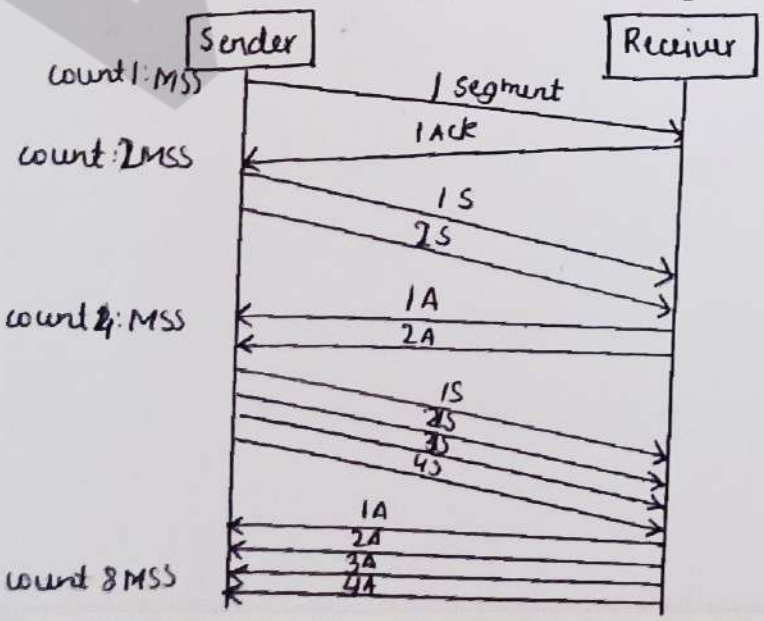
2) It increases packet delays, packet loss, wasting network resources and degrade the ~~the~~ throughput.

3) TCP congestion control is a method used by TCP protocol to manage dataflow over a network and prevent congestion.

4) TCP congestion control has three approaches
   a) Slow start
   b) Congestion Avoidance
   c) Congestion detection.

5) Slow start phase:

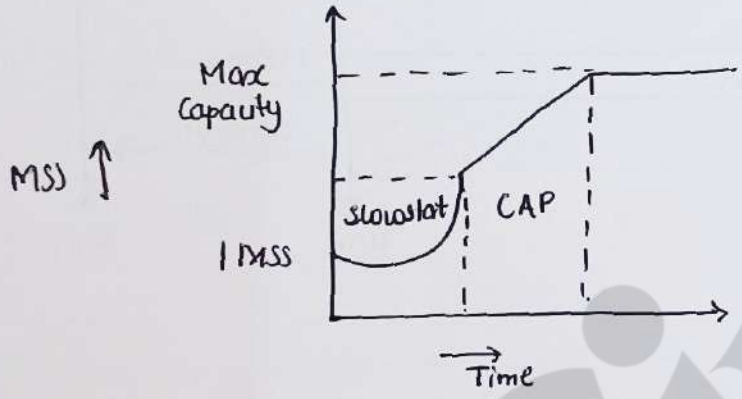
Initially, sender sets Congestion window size = Maximum Segment Size (1MSS)
After each sucessfull acknowledgment from client, it doubles window size : 1 to 2, 2 to 4, and so on. This exponential growth continues until congestion window reaches a threshold. or packet loss is detected.
Threshold : Maximum number of TCP segment that receiver window can accommodate/2
(Receiver window size / Maximum segment size) /2



6) Congestion avoidance phase:

Suppose the threshold is 16 segments. Once the congestion window reaches 16 the server stops doubling and increases window linearly by adding one segment for each successful round trip. This steady growth prevents the server from overwhelming the network. This phase continues until size of window becomes equal to that of the receiver window size.

Congestion window size = congestion window size + 1

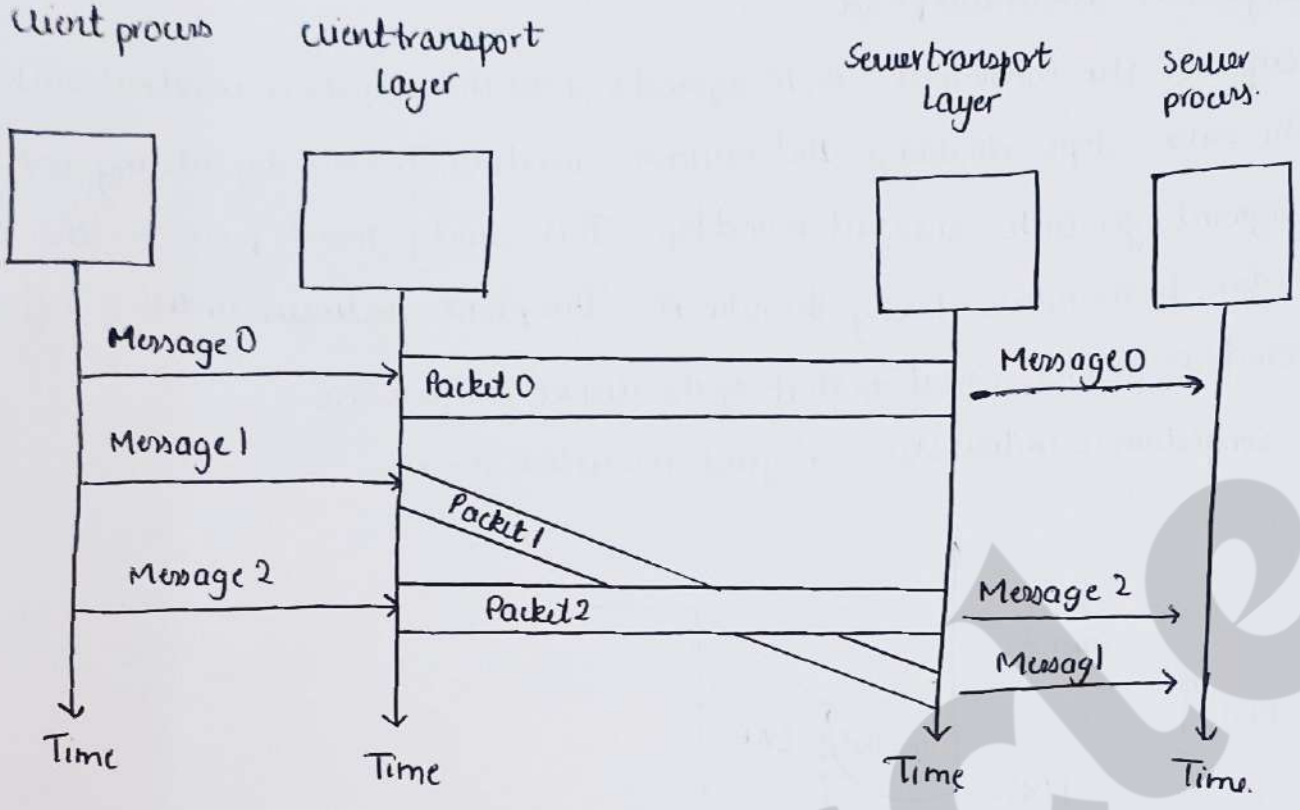


7) Congestion Detection Phase: If the network is congested or congestion window grow too large then packets might get dropped or loss. The server detects packets loss through Three duplicate ACK's or timeout then it immediately reduces the congestion window as half the current size.

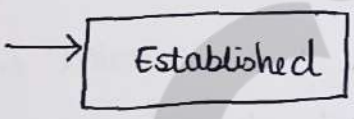
(7) Draw the FSM diagrams for connectionless and connection oriented services offered by transport layer.

→ Connectionless Service

In a connectionless service, the source application divides its messages into chunks of data and sends them to transport layer, which treats each chunk independently. There is no relationship between the chunks, so they arrive out of order at destination.



FSM.

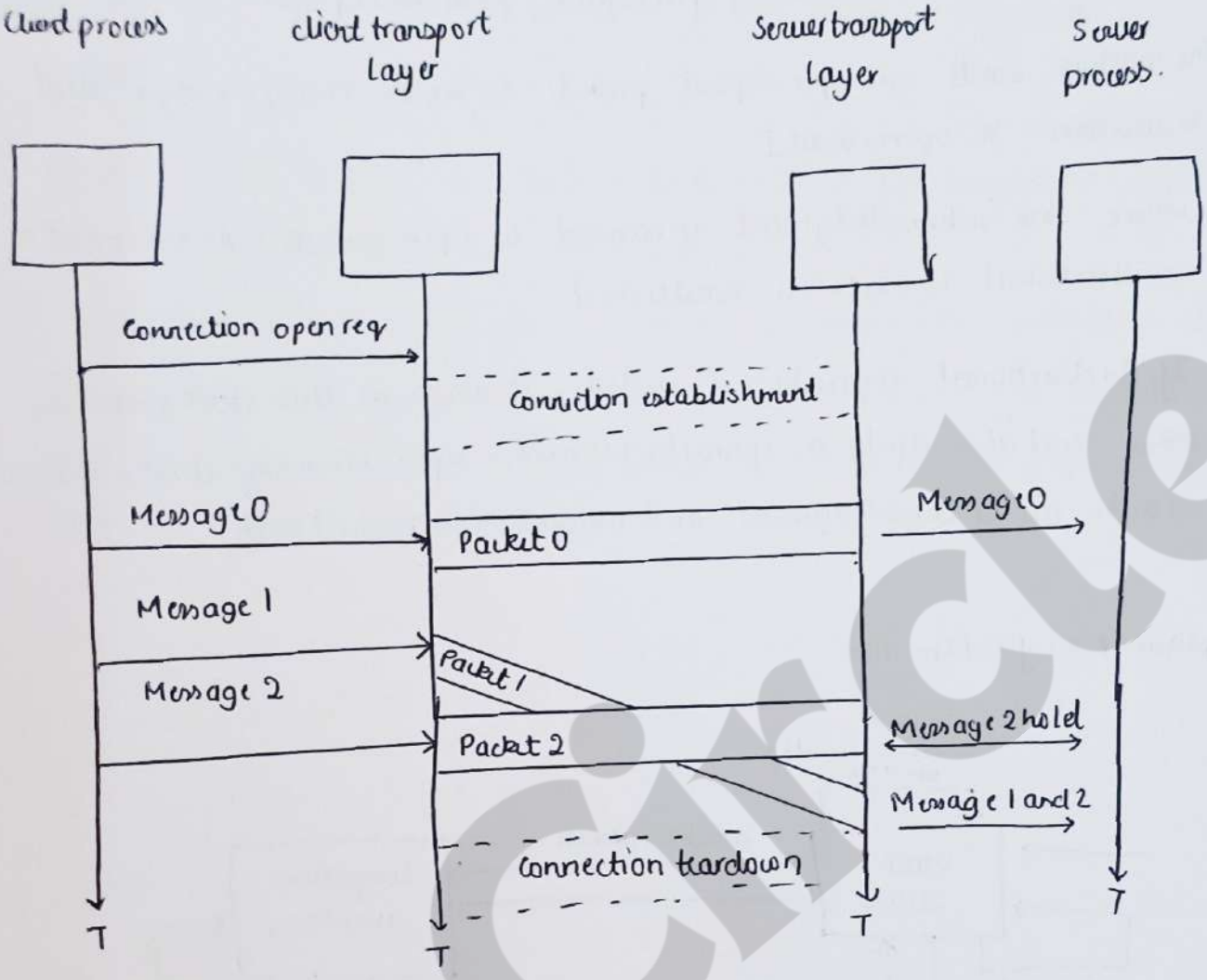


Both ends are always in established state

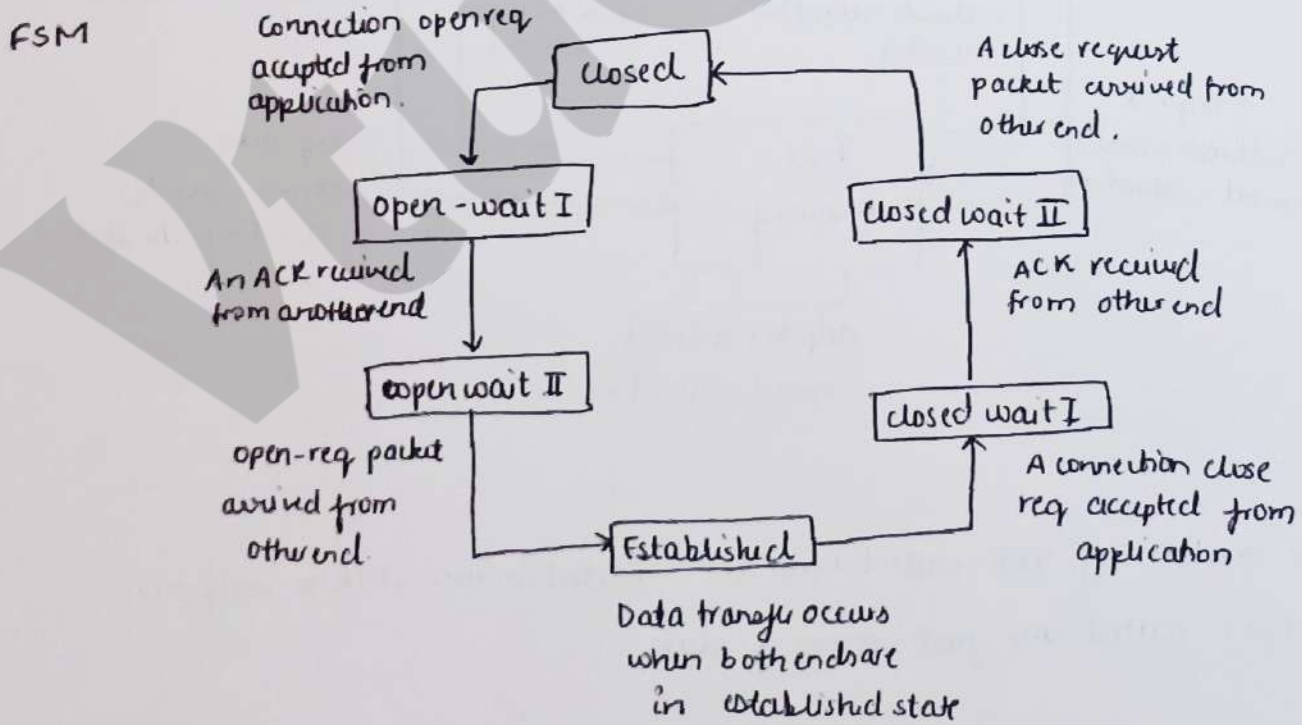
In a connectionless transport layer, the FSM has only one state, the established state. The machines on both client and server side remains in the established state, always ready to send and receive transport layer packets.

Connection oriented:

In connection oriented service, the client and server first need to establish a logical connection between themselves. The data exchange can only happen after connection establishment. After data exchange connection needs to be torn down.


Client process
client transport layer
Server transport layer
Server process
Connection open req
Connection establishment
Message 0
Packet 0
Message 0
Message 1
Packet 1
Message 2
Packet 2
Message 2 held
Message 1 and 2
Connection teardown
T
T
T
T

FSM


Connection open req accepted from application.
Closed
A close request packet arrived from other end.
Open-wait I
Closed wait II
An ACK received from another end
ACK received from other end
Open wait II
Closed wait I
open-req packet arrived from other end
A connection close req accepted from application
Established
Data transfer occurs when both ends are in established state

1) closed state: The FSM starts here when there is no connection. It stays in this state until it receives an open request from local prouss.

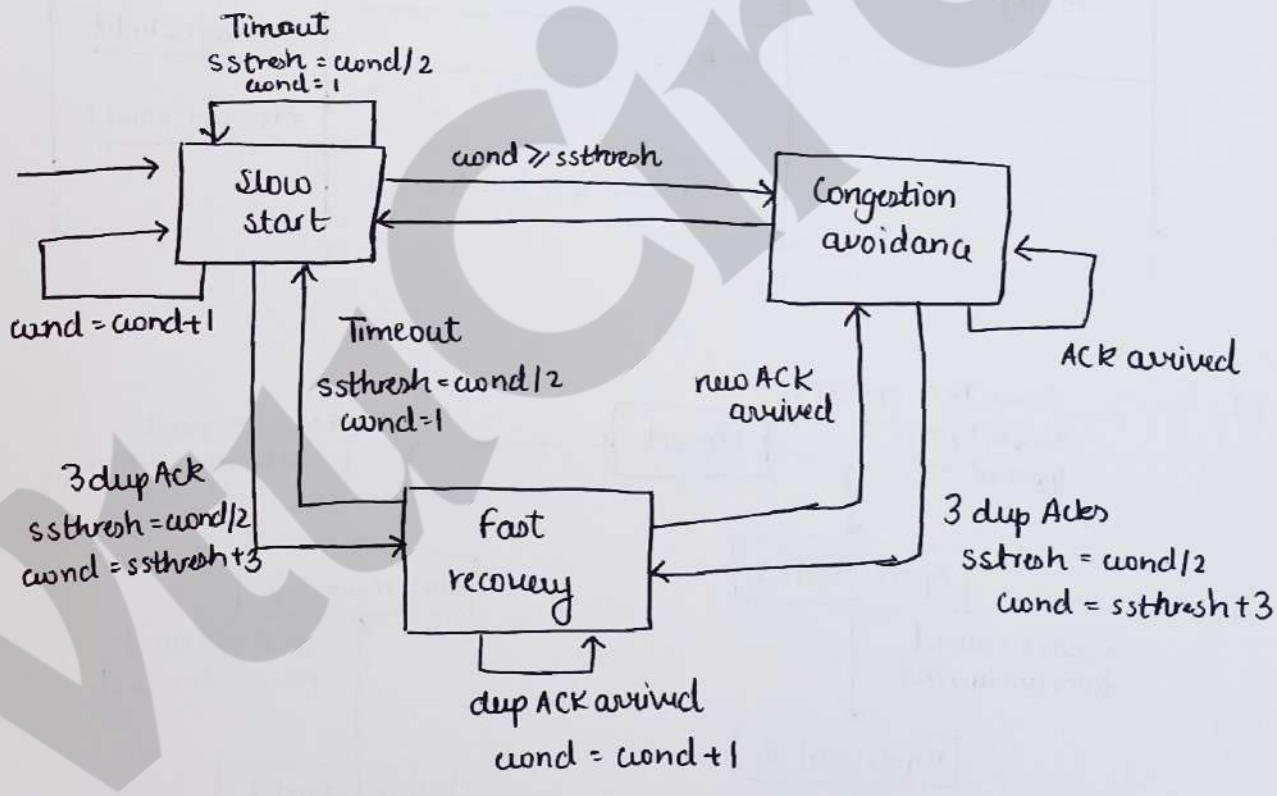
2) The machine sends an oper request packet to remote transport layer and transition to open-wait I

3) when the acknowledgment is received. to open wait II, At this point a unidirectional connection is established.

4) If bidirectional connection is needed, it waits in this state until the other end also sends a connection request. upon receiving it the machine sends an acknowledgment and moves to established state.

(8) Explain FSM for Reno TCP.

→



1) A newer version of TCP called Reno TCP, added a new state to congestion control FSM called the fast-recovery state.

2) This version treated the two signals of congestion, timeout and new arrival of three duplicate ACK differently.

3) When TCP enters fast recovery state, three major event occurs.

a) If duplicate ACKs continue to arrive, TCP stays in this state, but the cwnd grows exponentially.

b) If a time out occurs, TCP assumes that there is real congestion in the network and moves to the slow start state.

c) If a new ACK arrives, TCP moves to the congestion - avoidance state but deflates the size of the cwnd to the ssthresh value, as though the three duplicates ACKs have not occured., a transition is go from slowstart state to congestion avoidance state.

Computer Networks

Module 5

(1) Differentiate client server ~~paad~~ paradigm and peer to peer paradigm.

→

	client server paradigm	Peer to peer paradigm
1)	Centralized architecture	Decentralized architecture
2)	Server controls and manages resources and services	Control is distributed among peers.
3)	Limited scalability	Highly scalability.
4)	Clients depend on the server for resources	Peer share resources directly with each other.
5)	High cost	Low cost.
6)	Security is easy due to the centralized control	Security is harder due to the decentralized control.
7)	Higher latency	Low Latency.
8)	Eg: Web application, email	Eg: File sharing.

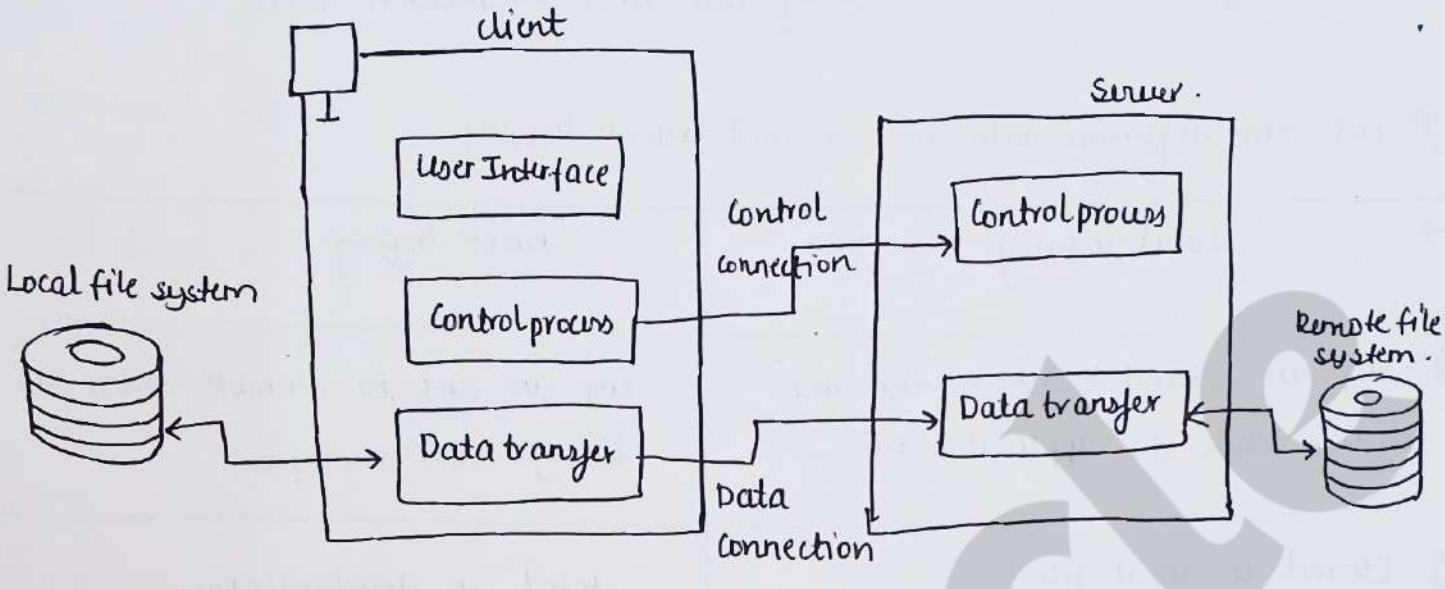
(2) Differentiate between Persistent and Non Persistent connection in http.

→

Persistent connection	Non Persistent connection.
1) The connection between client and server remains open for multiple request and responses.	The connection is closed after each request and response pair.
2) More efficient	Less efficient
3) Establishes a single connection for multiple transaction	Establishes a new connection for each transaction.
4) Lower Latency	High Latency
5) HTTP version : HTTP/1.1	HTTP version : HTTP/1.0
6) Uses fewer resources	Uses more resources.
7) Suitable for application requiring multiple resources	Suitable for simple request that don't require multiple resources.

(5) Explain how data connection happens in File Transfer Protocol.

→



1) FTP is used for transferring file from one host to another host. transferring files between system isn't always simple, as system can have different file name, rules, data formats, or directory structures.

2) The data connection is made between the data transfer processes.

3) The data connection is opened and then closed for each file transfer. FTP uses port 20 for data connection

4) The client issues a passive open using an ephemeral port. This must be done by client because it is the client that issues the commands for transferring files.

5) Using PORT command the client sends this port number to server.

6) The server receives the port number and issues an active open using the well known port 20 and the received ephemeral port number.

3) The purpose and implementation of data connection are to transfer files through the data connection. The client must define the type of file to be transferred, the structure of data and transmission mode.

(4) List the difference between local and remote logging

→	Local logging	Remote logging
1)	Logs are stored locally on the same system where the application runs	Logs are sent to a remote server for storage and analysis
2)	stored in local files	stored in cloud storage.
3)	Accessible only on the local machine	Accessible from multiple locations
4)	Higher risk if local system fails	Lower risk due to backup and redudancy.
5)	Suitable for standalone system	Suitable for distributed system.
6)	Limited to local tools	Limited to advanced tools.

(5) Explain briefly Domain Name System (DNS).

→ 1) DNS stand for Domain Name System. It translate human readable domain names into machine-readable IP addresses.

2) Step1: Users Request

Suppose the users enters www.google.com in browser, user request to DNS server for resolving an corresponding IP address.

3) Step2: Query to Recurive DNS Resolver.

The request is first sent to Recursive Resolver, managed by your Internet Service provider. This resolver find the IP address

Step3: Check local cache:

The ~~Recursi~~ Recursive resolver checks if it already has the IP address for www.google.com cached from previous queries. If found, it skips the next steps and provides IP address immediately

Step4: Query to Root DNS server:

If the resolver doesn't have the IP address in its cache, it queries Root DNS server. The Root server do not store IP addresses but it directs the query to the appropriate Top-level domain Server based on domain extension (.com).

Step 5: Query to TLD DNS server:

Responds with the location of the authoritative DNS server.

Step 6: Query to Authoritative DNS server.

Authoritative DSN server for www.google.com receive the query, which stores the actual IP address associated with domain name.

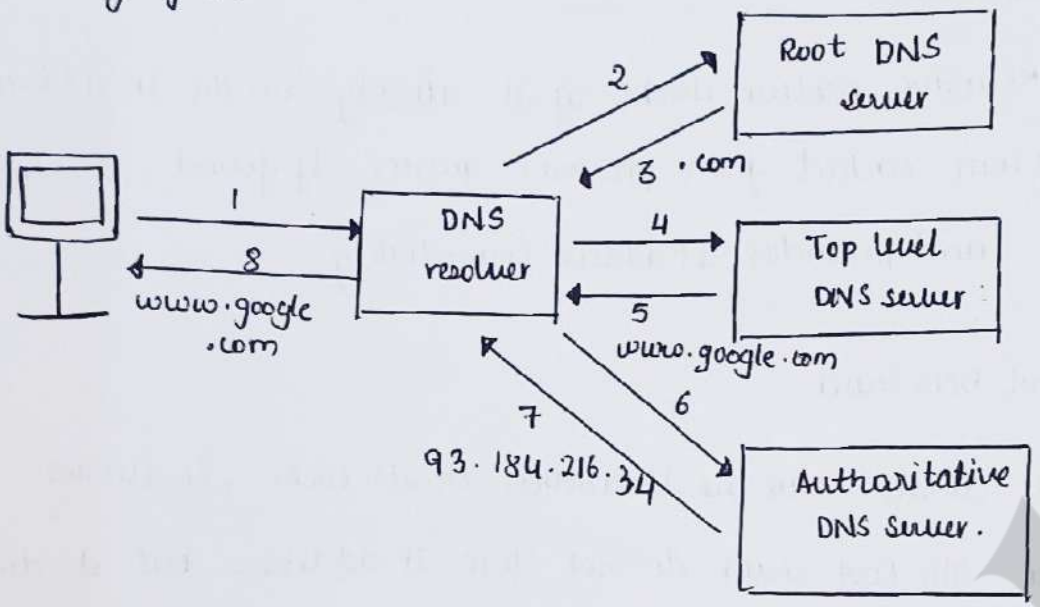
Step 7: Response to Browser:

Authoritative DNS server respond with IP address of www.google.com, the Recursive Resolver caches this response for future request and sends it back to browser.

Step 8: Accessing the website.

The browser uses the obtained IP address to establish connection to the web server hosting www.google.com and load all content of website.

Working of DNS



⑥ Explain about Web document and HTTP.

→

1) The documents ~~xxx be~~ in the WWW can be grouped into three categories static, dynamic and active.

2) Static document: Static document are fixed-content document that are created and stored in a web. When a client accesses the document, a copy of document is sent. The user can then use a browser to see document. Static documents are prepared using one of several languages. HTML, XML, XSL, XHTML

3) Dynamic Document: A dynamic document is created by a web server whenever a browser request the document. When a request arrives, the web server runs an application program or script that creates the dynamic document. The server returns the result of the program or script as a response to the browser that requested the document. Because a fresh document is created for each request the contents of dynamic document may vary from one request to another.

3) Active document: Active document are created using two methods.

1) Java Applets: Written in java and compiled into bytecode. Ready to run on clients device

2) Java Scipt: Scipts that are downloaded from the server and executed directly by the client's browser.

HTTP (Hyper text Transfer protocol)

1) The HTTP is the Web's application layer protocol is at the heart of web.

2) HTTP is implemented in two programs, a client program and a server program. The client program and server program, executing on different end systems talk to each other by exchanging HTTP messages.

3) A web page consists of object. An object is simply a file like HTML-file, a JPEG image, a Java applet, or video clip.

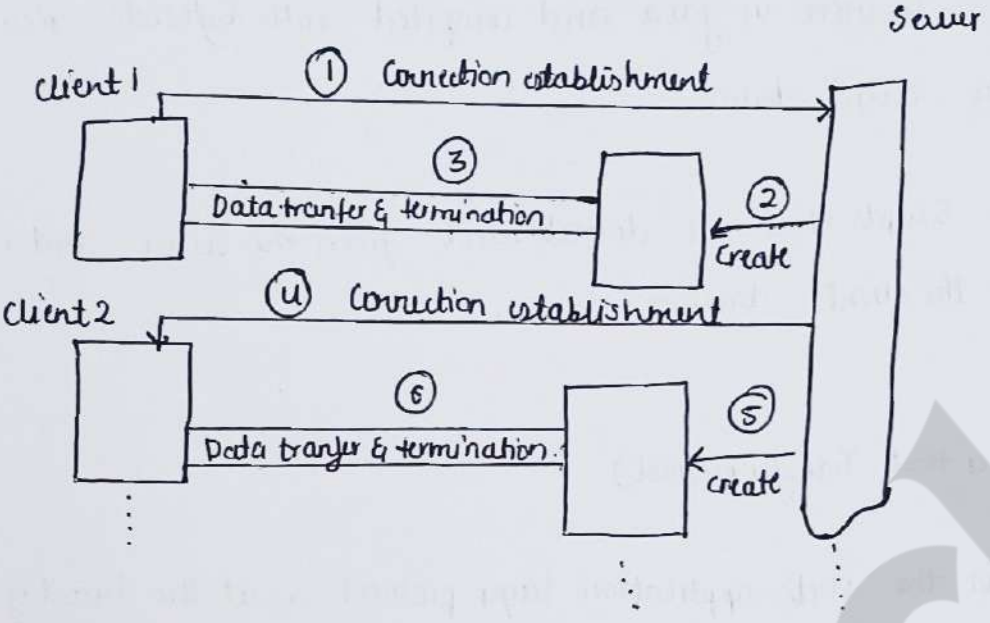
4) Most of web page consist of ~~object~~ base HTML file and several referenced object.

5) The base HTML file references the other object in web pages with object URL's

6) When a user request a Web page, the browser sends HTTP request messages for objects in the page to server. The server receives the request and responds with HTTP response message that contain the object.

(7) Explain in detail Iterative Communication using TCP.

→



1) TCP is a connection oriented protocol. Before sending or receiving data, a connection needs to be established between client server and server.

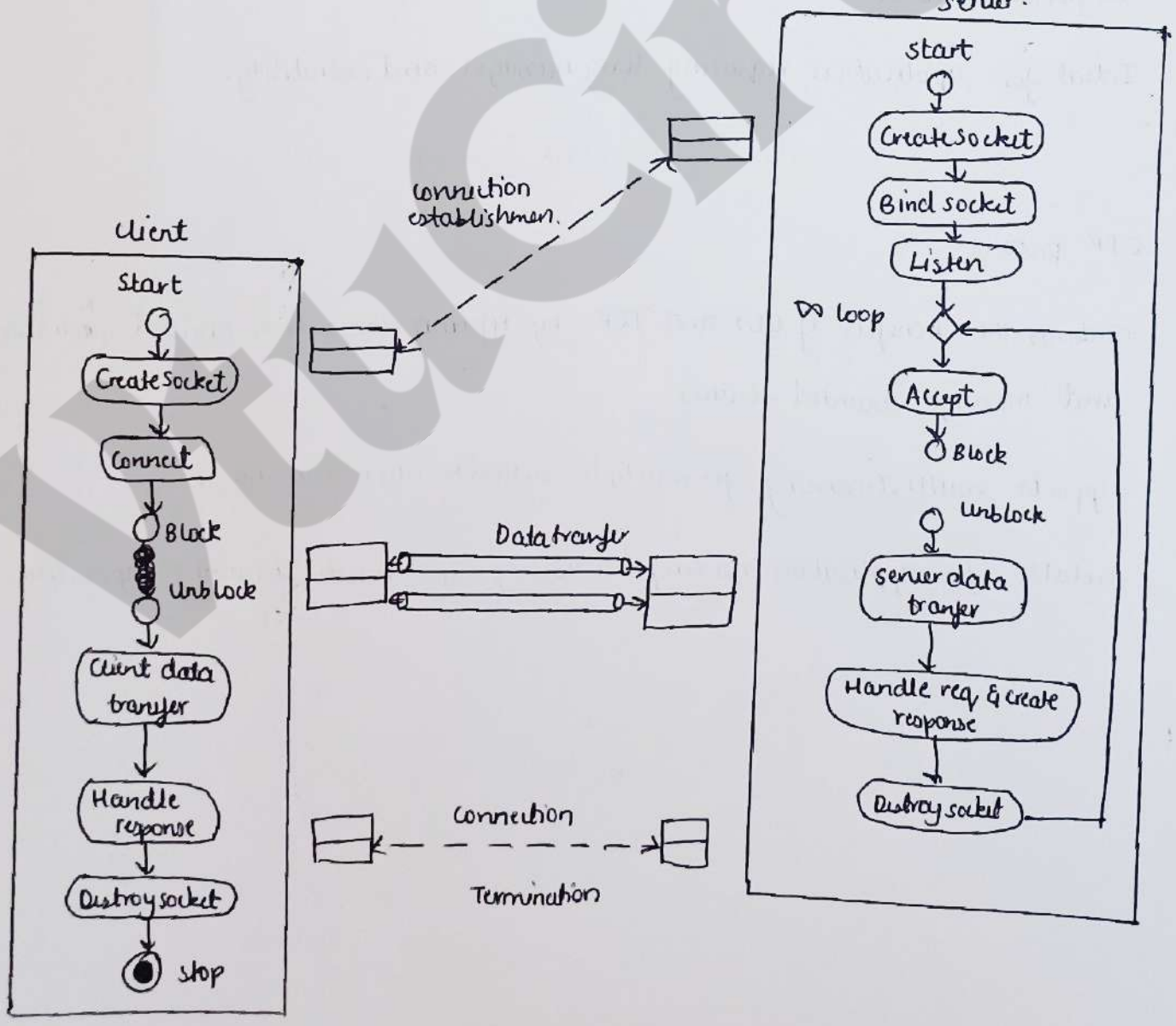
2) TCP ~~server~~ ~~server~~ server uses two different socket, one for connection establishment and other for data transfer, we call the first socket as listen socket and second one as socket.

3) The reason for having two types of sockets is to seprate the connection phase from data exchange phase.

4) A server uses a listen socket to listen for a new client trying to establish connection. After the connection is established, the server creates a socket to exchange data with client and finally to terminate connection.

Server process

1) TCP server creates a listening socket and bind it network address port.
2) The server calls a "listen" function, allowing the operating system to accept connection and add them to waiting list.
3) The server enter a loop, handling each client one at a time.
4) In each loop iteration, the server uses the "accept" function to pick client from the waiting list, if no clients waiting, server blocks. until client arrives.
5) Upon accepting a client, a new socket is created specifically for data exchange with that client.
6) The server sets this new socket with the clients address for direct communication.



(8) Explain the services provided by the Transport layer with different protocols.

→ Common transport layer protocols in the TCP are UDP, TCP, and SCTP.

1) UDP Protocol.

Provides connectionless, unreliable and message-oriented datagram service.

Each message is independent, with no logical connection between packets.

Suitable for application prioritizing simplicity and speed over Reliability.

2) TCP Protocol.

Provides connection oriented, reliable and byte stream service.

Uses a handshake to establish communication parameters, support flow and congestion control.

Ideal for application requiring long messages and reliability.

3) SCTP protocol.

Combines the benefits of UDP and TCP by offering connection oriented, Reliable and message oriented services.

Supports multi streaming for multiple network layer connections.

Suitable for application needing reliability and multi streaming capabilities.