*. Data communication: is the exchange of data between 2 or more devices via some form of transmission medium such as wire, or cables etc.

For data communication to occur, the communicating devices must be a part of communication system made up of combination of hardware & software.

⇒ There are four fundamental characteristics of data communication:

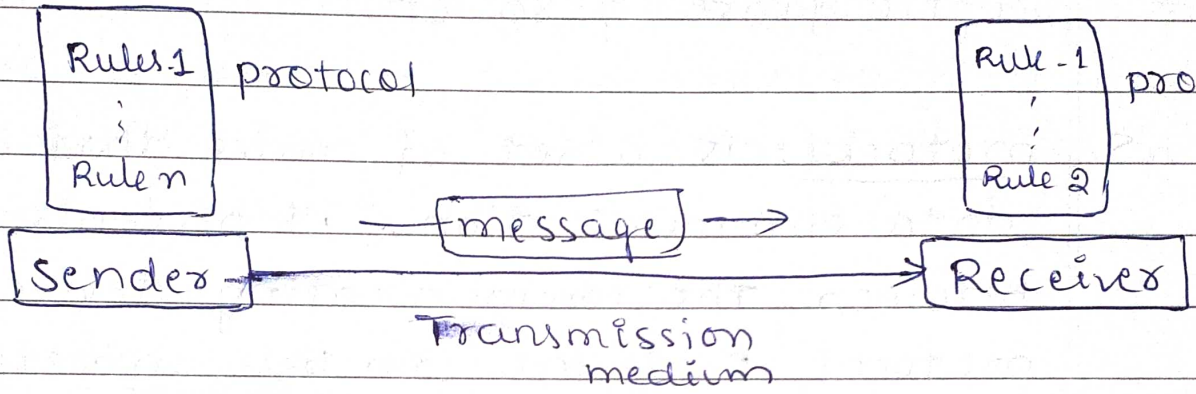
1. Delivery: The system deliver the data to the correct destination.

2. Accuracy: The system must deliver data accurately. Data that have been altered in transmission & left uncorrected are unusable

3. Timeliness: The system must deliver the data in a timely manner. Data delivered late are useless.

4. Jitter: refers to the variation in the packet arrival time.

→ Components of data communication:



There are 5 components of data communication:

1. Message: The message is the information (data) to be communicated, popular form of data include text, numbers, images, audios & videos.

2. Sender: The sender is the device that sends the message. It can be a computer, workstation, or mobile & so on.

3. Receiver: is the device that receives message which was sent by the sender. It can be a computer, workstation or mobile etc.

4. Transmission medium: is a physical path by which a message travels from sender to receiv

ex: co-axial cable, twisted pair cable or optic fibre & so on.

5. protocol: is a set of rules that governs the data communication. It presents agreements between the communicating device, without protocol 2 devices can be connected but not communicate.

-> Network Topology: The arrangement of a network which comprises of nodes & connecting lines via sender & receiver is known as network Topology.

*. Types of network Topologies:

1. Mesh Topology:
2. Star Topology
3. Bus Topology
4. Ring Topology.

1. Mesh Topology: Here, every device is connect-ed to one another via particular channel.

If 'n' number of devices are connected with each other, then total number of ports that are required by each device is N-1. & the total number of dedicated links required to connect them is $^nC_2$ i.e., $N(N-1)/2$.

Advantages:

* It is Robust
* provides security & privacy.
* Data Reliability.

Disadvantages:

* Installation & configuration is difficult.
* cost of maintenance is high.
* cost of cables are high.

2. Star Topology: Here, all the devices are conne-cted to a single hub through a cable.

A star topology is a topology in which all nodes are individually connected to a central point, like a hub or switch. A star takes more cable than a bus.

If N devices are connected to each other in star topology, then the number of cables required is N & only 1 port is required i.e., to connect to the hub.

⇒ problems with star topology:

* If the concentrator (hub) on which the whole topology relies fails, then the whole system will crash down.
* cost of installation is high.
* performance is based on the single concentrator i.e., hub.

3. Bus topology: Here, all the nodes are connected to a single cable. The cable to which the nodes connect is called as the "backbone". If the backbone is broken, then the entire segment fails.

Advantages:

* cost of cables is less as compared to the other topologies, but it is used to built small networks.
* Ease of installation
* If n devices are connected to each other, then the number of cables required is 1 which is known as backbone cable & N drop lines are required.

Disadvantages:

* If the common cable fails, then the whole system will crash down.
* If network traffic is heavy, it increases collisions in the network.

4. Ring topology: Here, each device is connected with its two neighbouring devices.

Here, the transmission is unidirectional, but it can be made bidirectional by having 2 connections between each network node & it is called dual ring topology.

Advantages:

* The possibility of collision is minimum in this type of topology.
* Cheap to install.

Disadvantages:

* If one workstation goes down entire network goes down
* It is slower as compared to bus topology
* Addition or removal of node during a network is difficult.

=> Devices used in each layer of TCP/IP model:

1. physical layer: is responsible for physical connectivity of two devices. The devices used are:

* Hubs: are used to connect segments of a LAN. It contains multiple input/output ports. When a signal is at any input port, this signal will be made at all output ports except the one it is coming form.

* Cables: In wired network architecture (e.g. Ethernet), cables are used to interconnect the devices. Some of the types of cables are coaxial cable, Twisted pair cable and optical fibre etc.

* Repeaters: are used in transmission systems to regenerate analog or digital signals distorted by transmission loss. Analog repeaters can only amplify the signal whereas a digitial repeaters can reproduce a signal to near to its original Quality.

2. Data link layer: is responsible to transfer data hop by hop (i.e., within same LAN, from one device to another device) based on the MAC address. some of the devices used in Data link layer are:

* Bridges: it provides interconnection with other networks that uses the same protocol, connecting two different networks together & providing communication between them.

* Modem: stands for Modulator/Demodulator. A modem converts digital signals generated by the computer into analog signal which, then can be transmitted over cable line & transforms the incoming analog signal into digital equivalent.

* Switches: A switch is a multiport network bridge that uses MAC addresses to forward data. Switches are Intelligent Hubs. Switches can remember which ports are connected to which devices. when a switch receives a packet, it resends the packet directly to the correct port.

3. Network layer: is responsible for creating routing table, and based on routing table, forwarding of the input request. Devices used in network layer are:

* Routers: is a switch like device that routes/forwards data packets based on their IP addresses. Routers are used to connect LANs & WANs.

4. Transport layer: is responsible for end-to-end communication (or process-to-process communication). Some of the devices are:

* Gateways: connects two dissimilar networks which are running different protocols. The gateway is a protocol converter which will translate one protocol into the other.

* Firewall: is a system designed to prevent unauthorised access to or from a private network, some of the functionalities of firewall are, packet filtering & as a proxy server.

5. Application layer : it provides the interface between the applications & network. It is used to exchange messages. some of devices used are. :

i. PC's (personal computer), phones, servers
ii. Gateways & Firewalls

⇒ TCP/IP vs OSI :

TCP/IP	OSI
Refers to transmiss-ion control protocol	Refers to open System interconnection
It has 4 layers	It has 7 layers
It is more reliable	It is less reliable
It uses both session & presentation layer in application layer	It uses different session & presentation layer
TCP/Ip developed protocols then model.	OSI model than protocols

It provides only connectionless services in network layer.	It provides both connectionless & connection

→ Transmission modes :

* Simplex mode : the communication is unidirectional, Only one of the two devices on a link can transmit, the other can only receive.

ex: Keyboard & monitor

* Half duplex mode : each station can both transmit & receive, but not at the same time.

ex: walkie-talkie

* Full duplex mode : both stations can transmit & receive simultaneously.

ex: Telephone service.

=> Stop & wait protocol: Here, a sender after sending a frame waits for an acknowledgement of the frame & sends the next frame only when acknowledgment of the frame has received.

=> What is DHCP, how does it works?

* The idea of DHCP (Dynamic host configuration protocol) is to enable devices to get IP address without any manual configuration.

* The device sends a broadcast message saying something like "I am new here"

* The DHCP server sees the message & responds back to the device & typically allocates an IP address. All other devices on network ignore the message of the new device as they are not DHCP server.

Physical / MAC address.

-> Address Resolution protocol: is a communication protocol used for discovering the MAC address associated with a given IP address

-> Reverse Address Resolution protocol: It is used by a client computer to request its internet protocol (IP) address from a computer network when all it has available is its link layer or hardware address, such as MAC address.

-> MAC (Media Access control) address / physical Address: It is a unique 48 bit hardware number of a computer which is embedded into network card known as Network Interface card (NIC) during the time of manufacturing. MAC address is also known as physical address. It is a physical address which works at data-link layer.

-> Ip Address classes:

Class - A	1 - 127	N.H.H.H
Class - B	128 - 191	N.N.H.H
Class - C	192 - 223	N.N.N.H
Class - D	224 - 239	
Class - E	240 - 255	

→ Data Representation: Information today comes in different forms such as text, numbers, images, audio and video.

1. Text: It is represented as a bit patterns, a sequence of bits (0s or 1s). Different set of have been designed to represent text symbols. Each set is called a code.

Unicode: It uses 32 bits to represent a symbol or character used in any language in world.
ASCII represents the first 127 characters in Unicode

2. Numbers: are also represented by bit patterns. However, a code such as ASCII is not used to represent numbers, Numbers are directly converted to a binary number to simplify math operations.

3. Images: are also represented as bit pattern, images composed of matrix of pixels (picture element) where each pixel is a small dot. The size of dot i.e., pixel depends on resolution.

4. Audio: refers to the recording or broadcasting of sound or music. Audio by nature is different from text, numbers or images. It is continous, not discrete.

5. Video: can either be produced as continuous entity or it can be a combination of images

1.1.3 Data Flow: communication between two devices can be simplex, Half duplex or Full duplex.

1. Simplex:

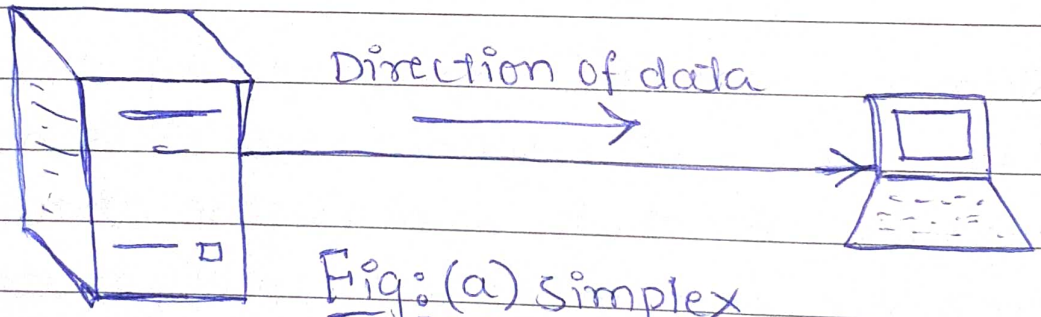


Fig: (a) Simplex

Here, communication is unidirectional as one way street, only one of the 2 devices on a link can transmit the other can only receive.

Keyboards & monitors are examples of simplex devices. Keyboard can only introduce input; & monitor can only accept output.

2. Half Duplex: Here, both stations can transmit and receive, but not at same time, when one device is sending, the other can only receive or vice-versa.

It is used in cases where there is no need for communication in both directions at same time, the entire capacity of the channel can be utilized for each direction.

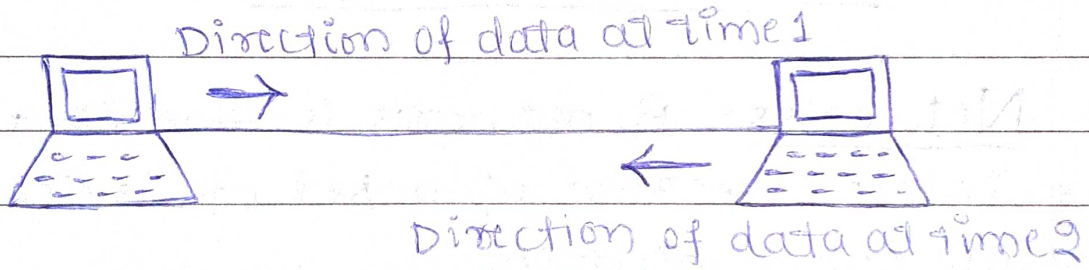


Fig: (b) Half Duplex

3. Full Duplex: Here, both stations can transmit & receive simultaneously.

ex: Telephone network, when 2 peoples are communicating by telephone line, both can talk & listen at same time.

It is used when communication in both direction is required all the time, The capacity of channel, however must be divided between the two directions.

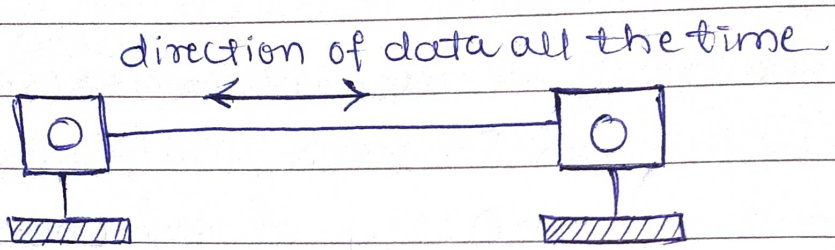


Fig:(c) Full duplex

1.2 Networks: A network is ~~capable a~~ the interconnection of a set of devices capable of communication.

1.2.1 Network criteria: A network must be able to meet a certain number of criteria. The most important are performance, reliability, and security.

1. Performance: can be measured in many ways including transmit time & response time. It also depends on a number of factors such as No. of users, type of transmission medium

used and the capacity of connected hardware & efficiency of h/w.

Performance is often evaluated by networking metrics : Throughput & delay, we need more throughput & less delay.

2. Reliability: In addition to accuracy of delivery, network reliability is measured by frequency of failure, the time it takes a link to recover from failure and the network's robustness.

3. Security: N/w security issues include protecting data from unauthorized access, protecting data from damage and implementing policies & procedures for recovery from breaches & data losses.

1.2.2 Physical Structure:

1. Type of connection:

x. Point-to-Point: provides a dedicated link between 2 devices. The entire capacity of the link is reserved for transmission between those 2 devices.

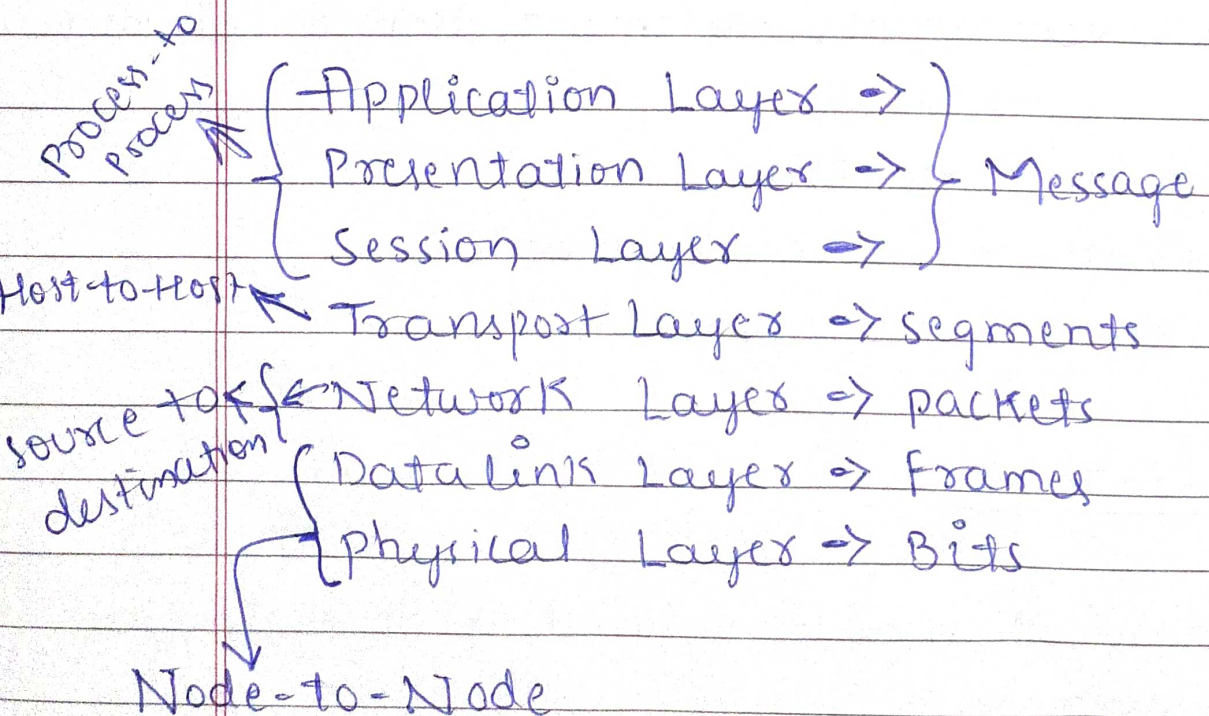
Most of the point-to-point connections use an actual length of wire or cable to connect two ends.

Example: When we change television channels by Infrared remote control, we are establishing a point-to-point connection between remote & tv control system.

TCP/IP protocols Suite:

Physical Layer → Bits
Datalink Layer → Frames
Network Layer → Datagram / packets
Transport Layer → segment / Datagram
Application Layer → Messages

OSI [open System Interconnection] Model:



→ Differences between IPV4 & IPV6

	IPV4	IPV6
1.	It is a 32 bit address length	1. It has 128 bit address length.
2.	It does not provide any Encryption & Authentication	2. It provides encryption & authentication.
3.	In IPV4 checksum-field is available	3. In IPV6 checksum -field is unavailable
4.	It has header of 20-60 bytes.	4. It has a header of 40 bytes fixed.
5.	Address representation is in IPV4 decimal	5. Address representation is Hexadecimal form.
6.	Security feature is dependent on application	7. IPSEC is inbuilt features of IPV6 protocol.

Transport Layer:

1. It is located between the application layer & network layer.
2. It provides a process-to-process communication between two application layers, one at the local host and the other at the remote host.
3. communication is provided using a logical connection.
4. It is the heart of TCP/IP.

Transport Layer Services:

1. process-to-process communication.
2. Addressing: Port Numbers.
3. Encapsulation & Decapsulation.
4. Multiplexing & Demultiplexing.
5. Flow control.
6. Error control
7. congestion control.
8. pushing & pulling

① process-to-process communication:

* The first duty of transport layer protocol is to provide process-to-process communication
* A process is an application layer entity that uses services of transport layer.
* It is responsible for delivery of msgs to appropriate process.

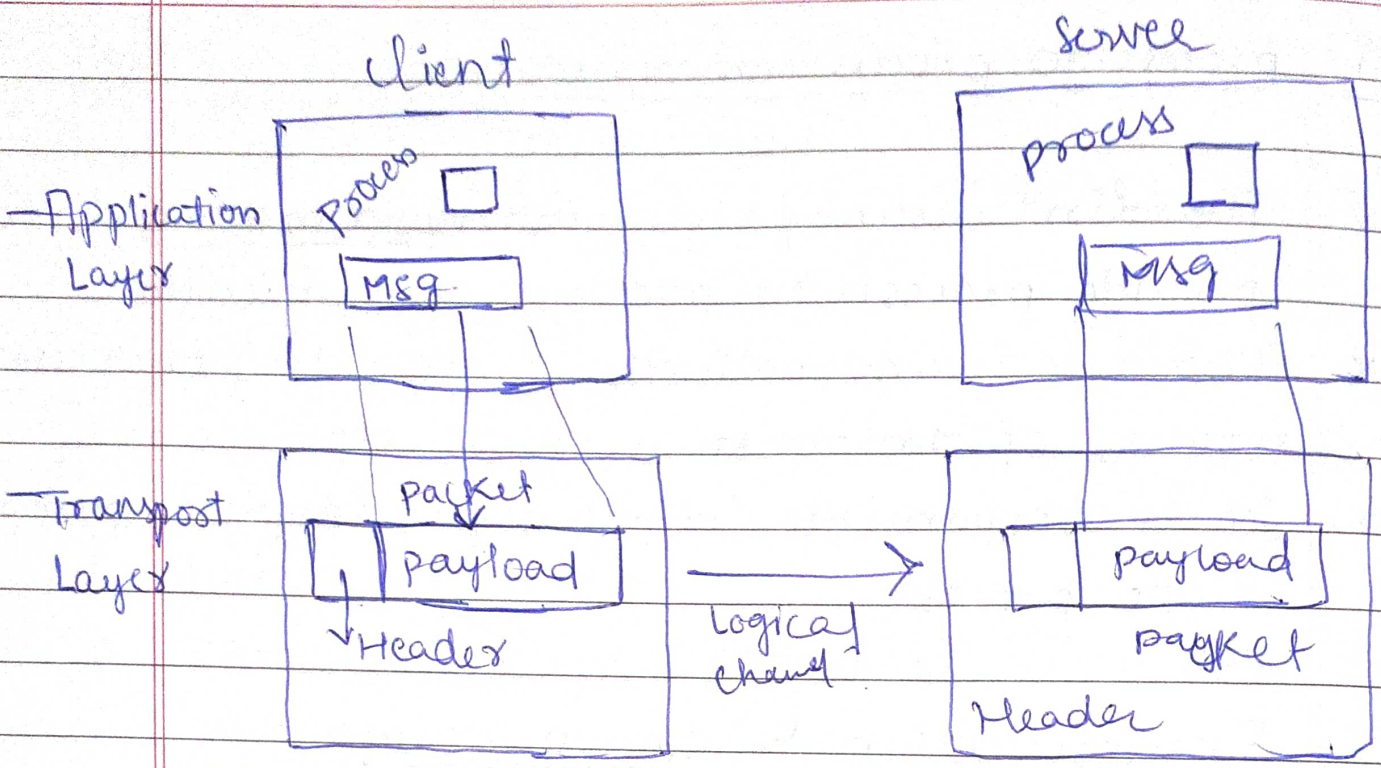
② Encapsulation & Decapsulation:

* To send a msg from one process to another the transport layer protocol encapsulates & decapsulates msgs.
* Encapsulation happens at sender side, when process has msg to send, it passes the msg to transport layer along with socket address & some other peice of info.
* Decapsulation happens at receiver side, header is dropped & msg is delivered to Application layer

⇒ Socked Address : IP Address + port Number.

* 0-1023 : well-known ports
* 1024-49,151 : Registered ports

* 49152-65535 Dynamic or private



(5) Flow control: Whenever an entity produces an item & another entity consumes, there should be a balance b/w producing & consuming rates

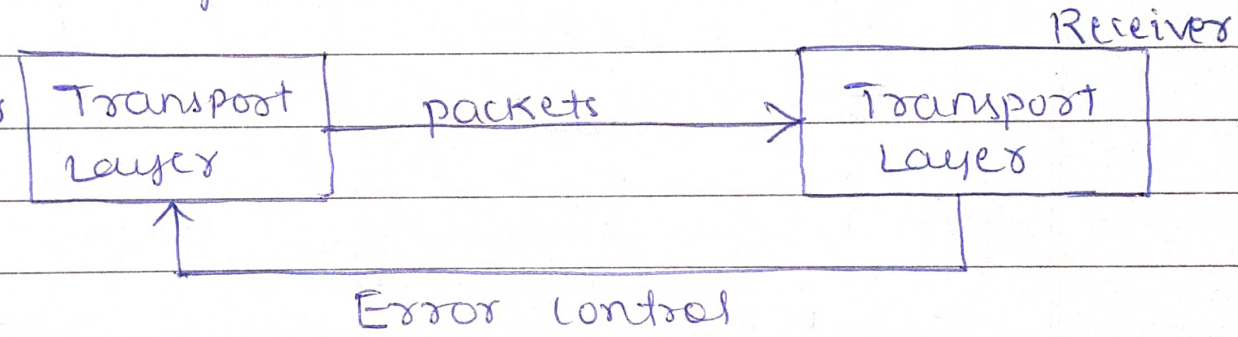
If items are produced faster than consume can be overwhelmed by item & have to discard some times

Transport Layer offers flow control to overcome this issue.

④ pushing & pulling: If sender delivers items to receiver without informing then it is called pushing else pulling.

③ Error control:

* Detecting & discarding corrupted packets
* Recognizing duplicate packets.
* Resending corrupted packets & track.



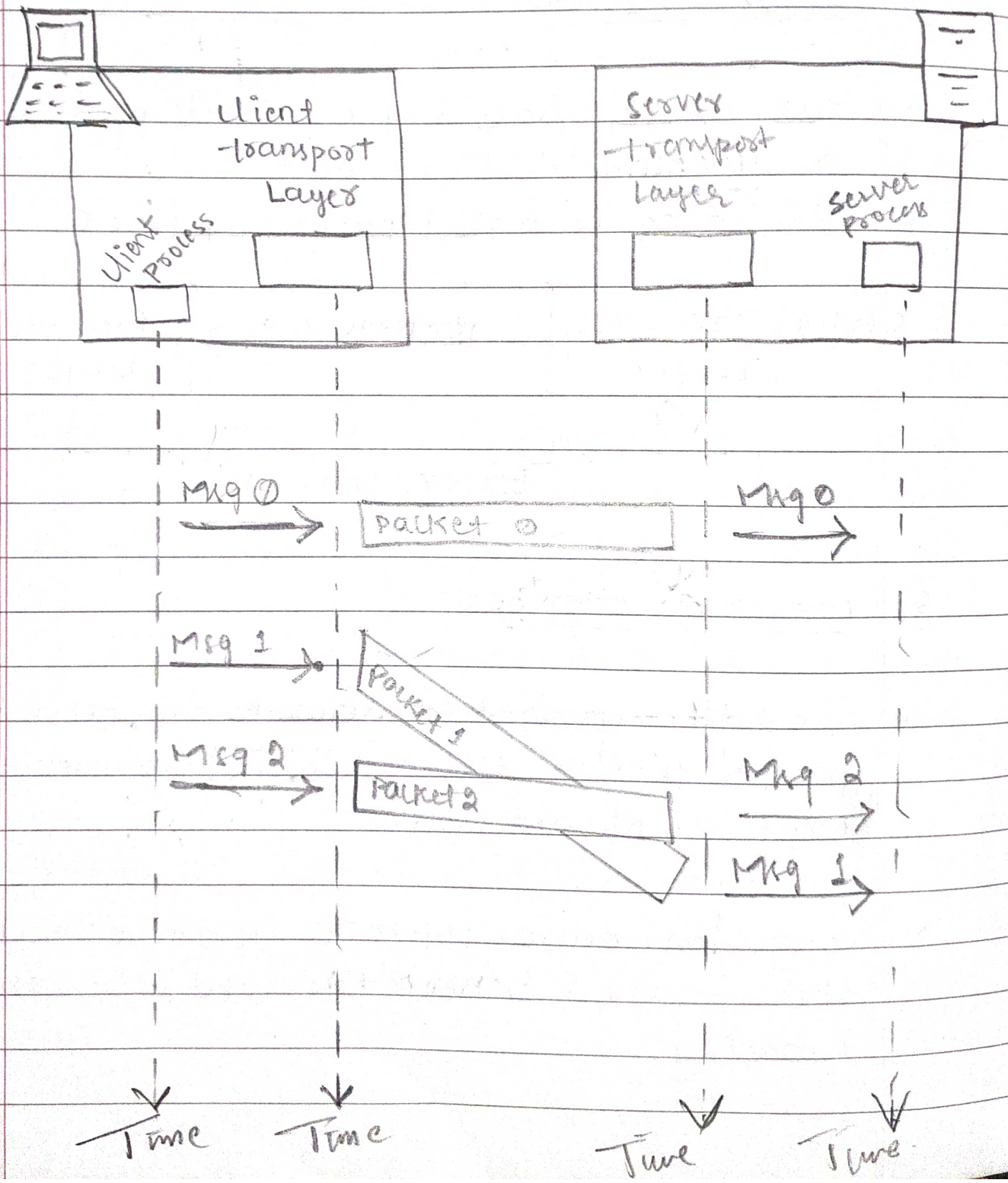
⑥ congestion control:

* congestion ~~control~~ in network may occur if no. of packets sent to the network is greater than the capacity of network.

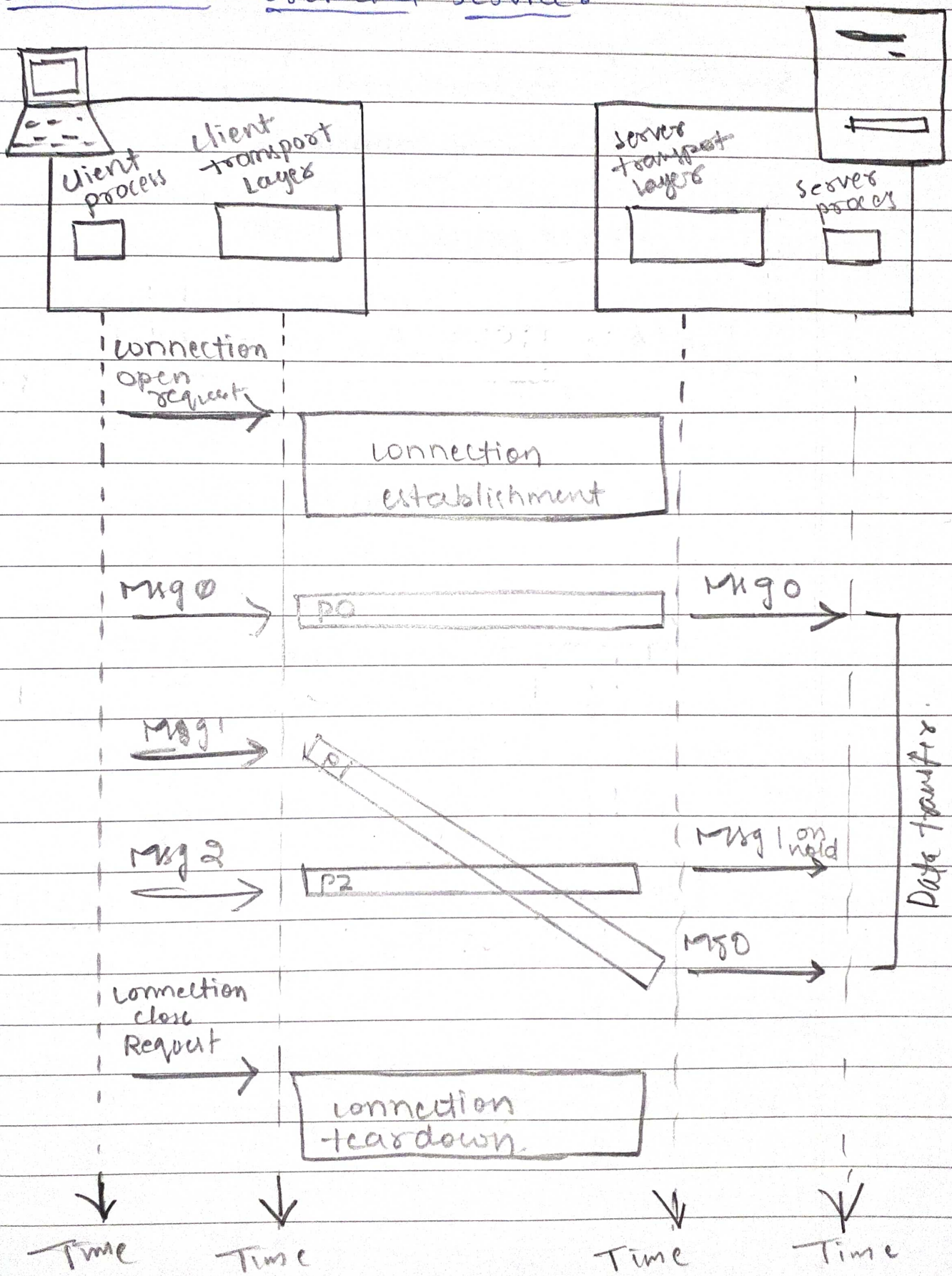
* congestion control refers to technique that control the congestion & keep the load below the capacity.

23.1.2 Connectionless & connection-oriented services:

(1) connectionless service



(2) connection-oriented service:



classmate
Date
Page

Transport Layer Protocols :

1. Simple protocol
2. Stop-and-wait protocol
3. Go Back-N protocol (GBN)
4. Selective-Repeat protocol
5. Bidirectional protocol.

1. Simple Protocol :

* It is a connectionless protocol.
* It has no flow control
* It has no error control
* It assumes that the receiver can immediately handle any packet that it receives.
* In other words, receiver can never be overwhelmed with incoming packets.

(2) Stop-&-wait Protocol:

* It is a connection-oreinted protocol
* It uses both flow & error control
* Both sender & Receiver use a sliding window of size 23.
* The sender sends one packet at a time & waits for an acknowledgment before sending the next one.
* To detect corrupted packets, we need to add a 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 & silently discarded.

(3) Go-Back-N protocol:

* To improve the efficiency of transmission, it sends multiple packets when the sender is waiting for acknowledgements.
* In otherwords, it lets more than one packet be outstanding to keep the channel busy while the sender is waiting for acknowledgement.
* If the ACK of a frame is not received in an agreed upon time period, all frames in the current window are retransmitted.
* N - is the sender's window size

(4) Selective Repeat:

* Here, only the erroneous or lost frames are retransmitted, while the correct frames are received & buffered.
* In GBN, either the frames is lost or the ACK, all the frames in the current window is retransmitted
* The receiver while keeping track of sequence no. buffers the frames in memory & sends NegativeAck for only frames which is missing or damaged.
* The sender will send/retransmit packets for which NACK is received

IPV4 Datagram:

Version	Hlen	DS	Datagram
4 bit	4bit	8 bits	16 bits
Identifier 16		flags 3bit	fragmentation offset 13
Time-to-live	Protocol	Header checksum	
Source IP Address 32 bits			
Destination IP Address 32 bits			
Option			
Payload			

IPV6 datagram:

Version	Traffic	flow label
4 bits	class 8 bits	20-bits
payload length	Next header	Hop limit
Source Address 128 bits = 16 bytes		
Destination Address 128 bits = 16 bytes		

Fig: IPV6 datagram

-> UDP: User datagram Protocol:

* It is a connectionless protocol, unreliable transport protocol.
* UDP is a very simple protocol, using a minimum of overheads
* UDP header is of 8 bytes made of 4 field each of 2 bytes.
* The first two fields define the source & destination port numbers
* The 3rd field defines the total length of the user datagram header plus data
* The 4th field can carry checksum which is optional

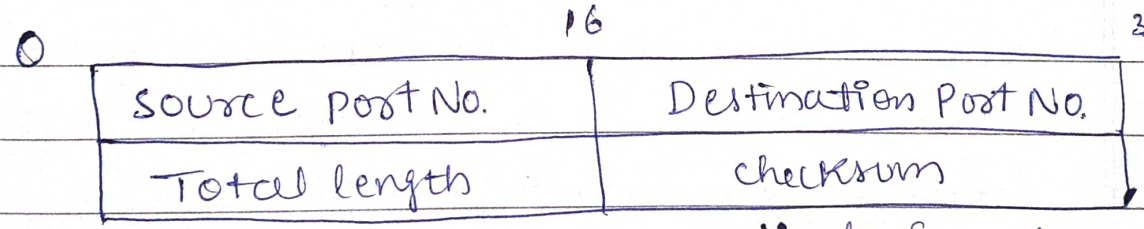
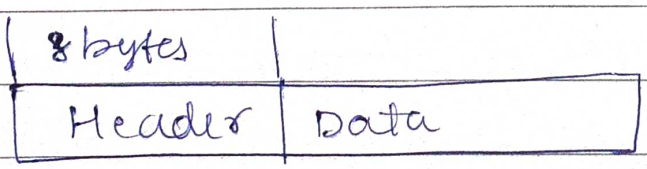


Fig: Header Format



UDP User Datagram

⇒ UDP Services:

1. process-to-process communication
2. Flow control
3. Error control
4. connectionless services
5. checksum

⇒ UDP Applications:

1. In simple request-response communication
2. with internal flow & error control like TFTP
3. management process like SNMP
4. Routing protocol like RIP
5. Interactive realtime apps

→ TCP : [Transmission control protocol].

* TCP is a connection oriented, reliable protocol.
* TCP explicitly defines connection establishment, data transfer & connection teardown phases to provide a connection oriented service
* TCP uses combo of GBN & SR protocol to provide reliability.

→ TCP services:

1. process-to-process communication
2. Stream delivery service
3. Multiplexing & Demultiplexing
4. Full Duplex communication
5. connection oriented service
6. Relaible Service
7. sending Buffer & Receiving Buffer.
8. segments.

→ TCP Segment & Header format :

| 20-60 Bytes |

Header	Data

(a) segment