Page
Date

Date : 06 / 06 / 2023
Day : Tuesday

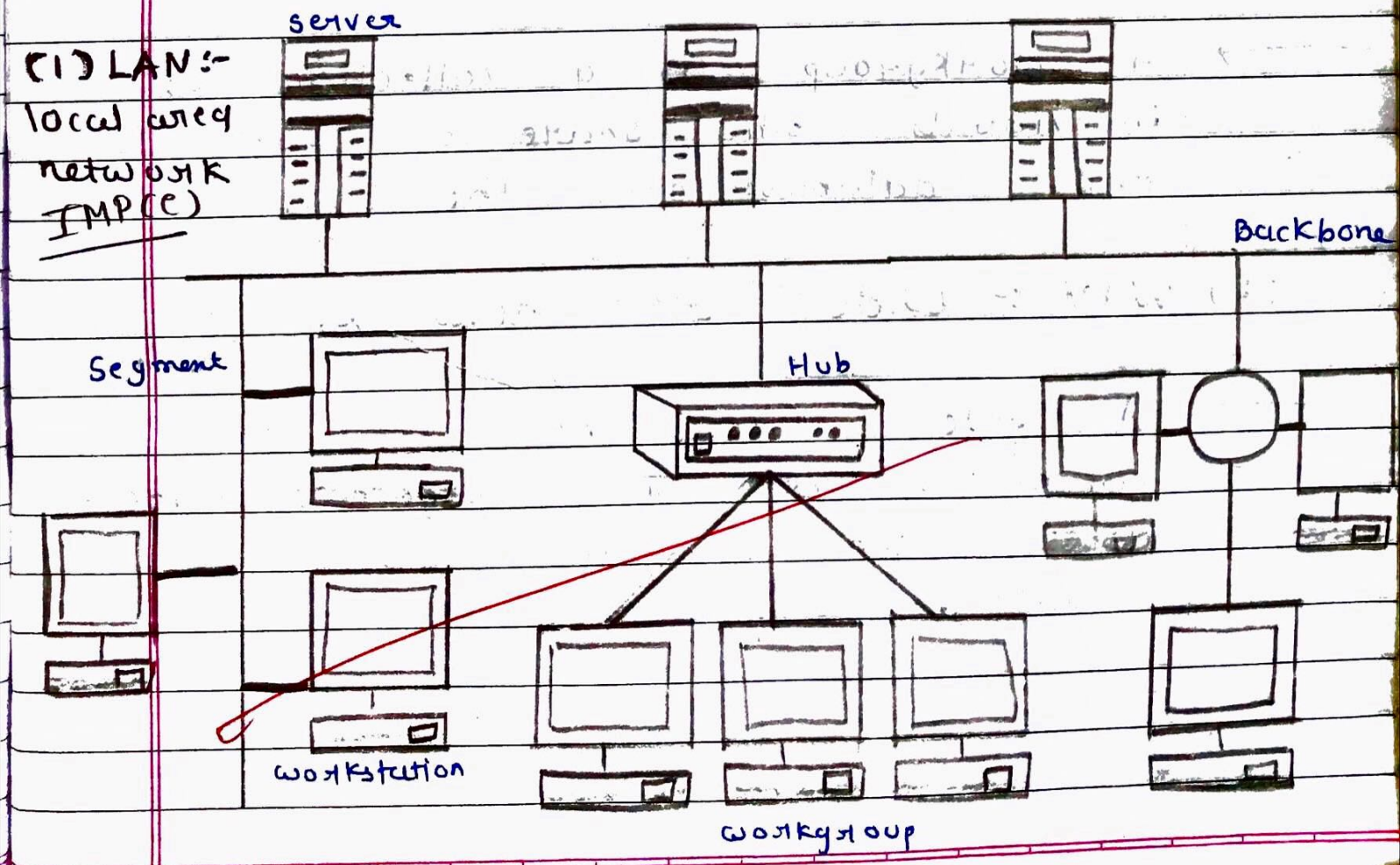
Book : TCP/IP protocol suits

Unit :- 1

Overview and TCP/IP protocol - I

- ARPA Net : Advanced Research projects Agency network
- DOD : Department of Defence

(1) LAN :-
local area network
IMP(E)



→ A network within a building is called LAN.

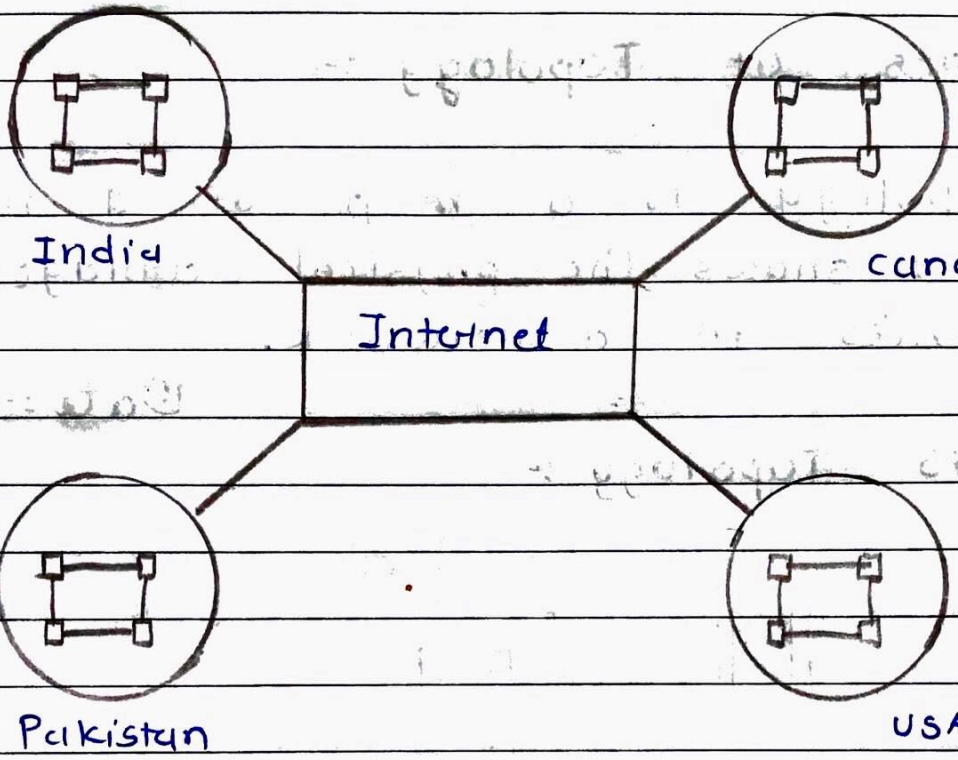
→ A LANs are useful for sharing resources like printer files games or other applications.

→ To establish a LAN network we need ethernet cable, Network adaptors, hubs and switch.

→ A workgroup is a collection of individuals who share a same file and database over the LAN.

(2) WAN :- Wide area network.

→ A wide area networks connects computers ever a large geographic area, such as a state or country.



→ WAN is also known as collections of smaller network such as LANs and MANs.

(3) MAN :- Metropolitan area network

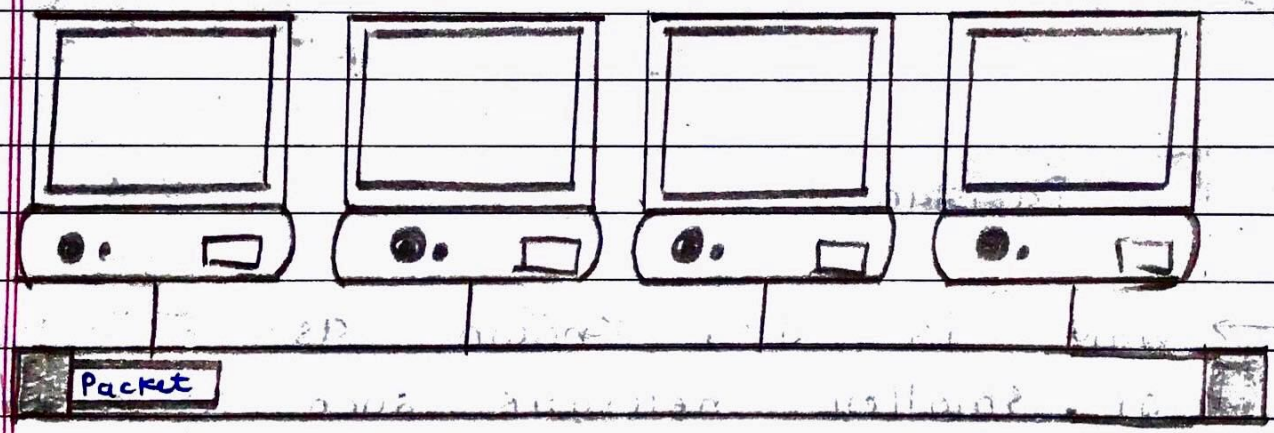
→ A MAN is a network that connects two or more LAN or CAN together within the boundary of a city.

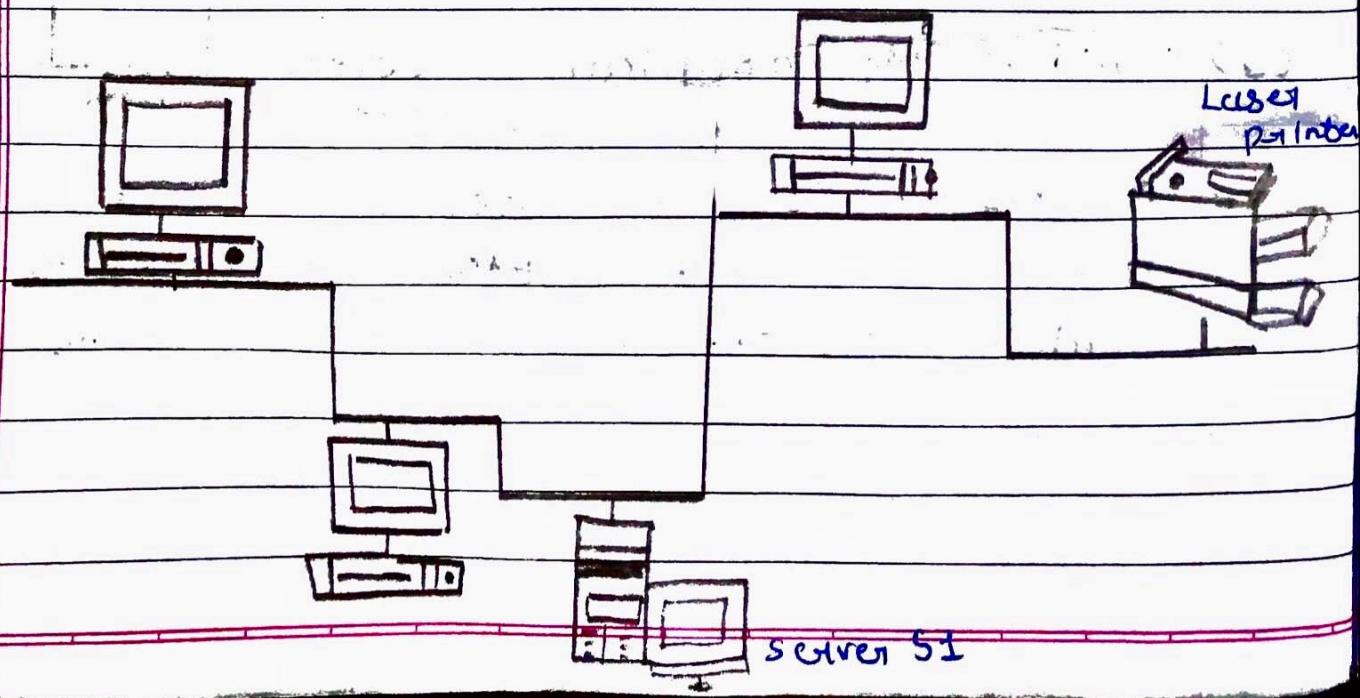
Imp(c) * Types of Topology :-

⟶ Topology is a map of a network. It shows the physical arrangement of devices in a network.

Date :- 12/06/23

(1) BUS Topology :-





→ All computers are ~~connected~~ attached to a single continous cable that is terminated at both ends, which is the simplest way to create a physical network.

→ A single cable the backbone functions as a shared communication medium that attach devices with a connector.

→ A device wanting to communicate with another device on the network sends a broadcast message onto the wire that all other devices see, but only the inteded recipient actually accepts and processes the messages.

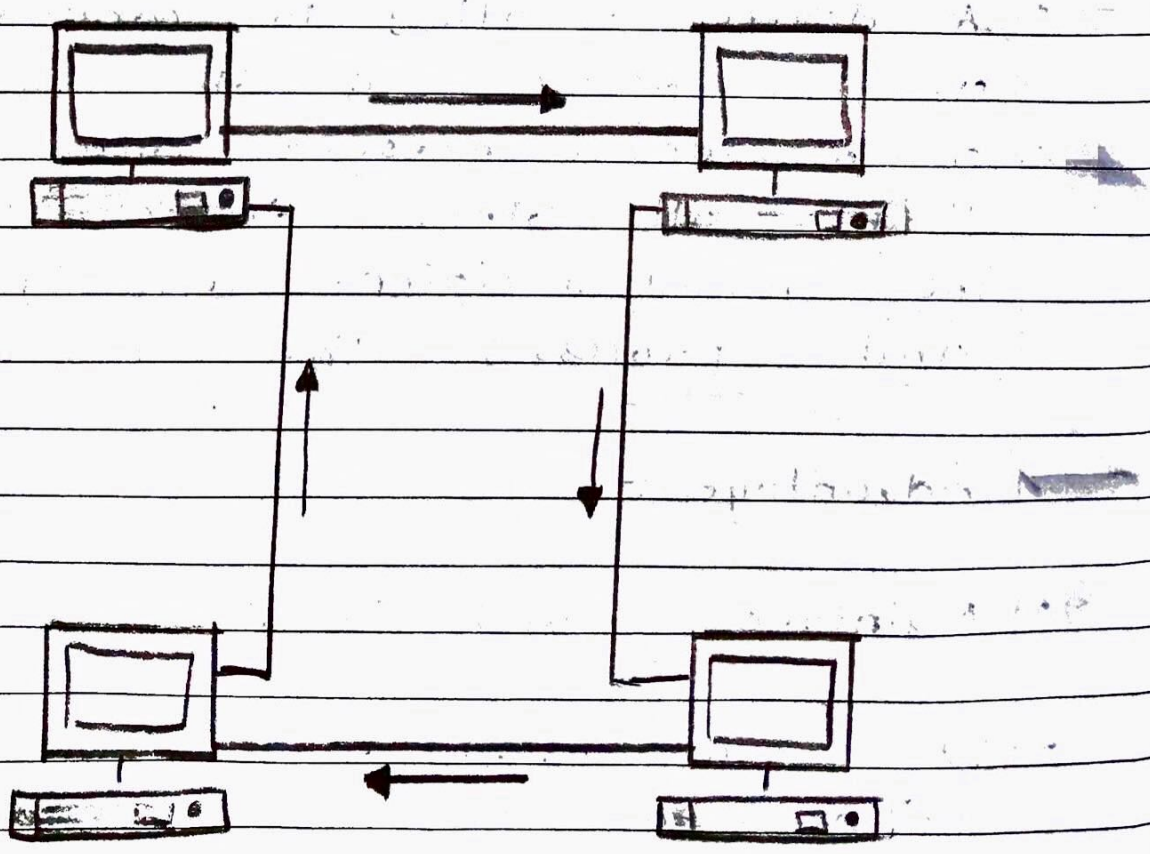
→ Advantages :-

- Maintanens and installation is easy
- We can install more devices as per the need at any time.

→ Disadvantages :-

- A fault in backbone cable can break the whole network.
- If no. of devices are more the speed can be affected.

(2) Ring Topology :-



→ In a ring network, every device has exactly two neighbours for communication purposes.

→ Ring topologies typically utilize a token passing scheme, used to control access to the network.

→ By utilizing this scheme, only one machine which is having the token can transmit on the network at a time

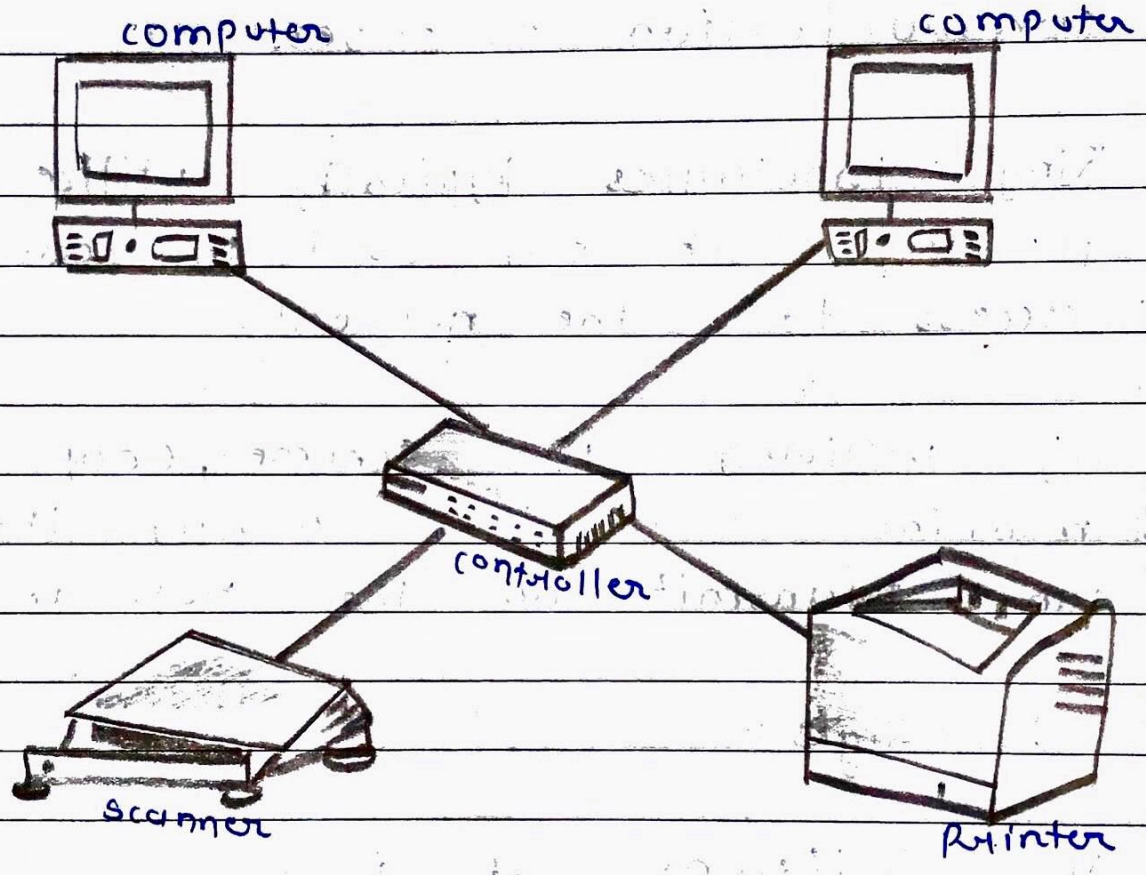
→ Advantages :-

- No collisions of frames
- Does not require server or a HUB

→ Disadvantages :-

- Failure to one device may fail whole network.

(3) Star topology :-



→ All devices are connected to a control device usually like a HUB.

→ A HUB receives and forwards data packets.

→ Generally the home network use the star topologies.

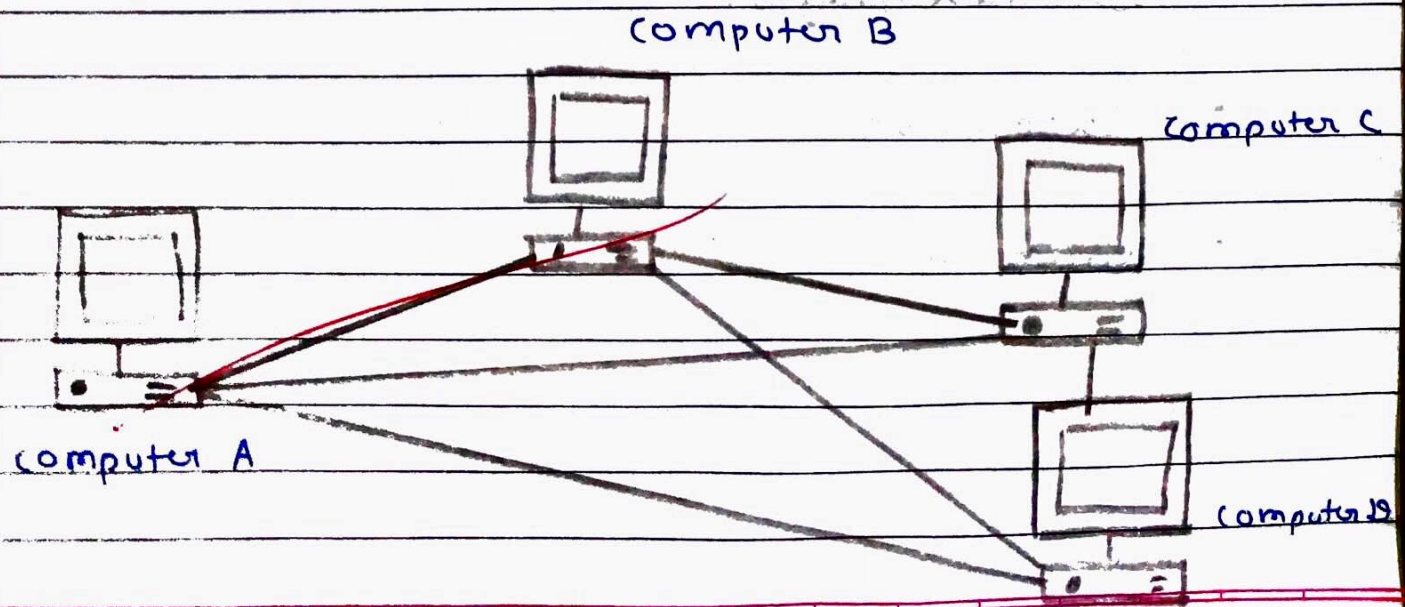
→ Advantages :-

- It gives more perfomance
- A failure in any cable we affect it only that device.

→ Disadvantages :-

- Require more cables
- Network size is limited, depending on the connects in HUB.

(4) Mesh topology :-



→ A Mesh network in which every device connects to every other device with a deticated cable is called full mesh.

→ In partial mesh network, some devices are connected indirectly to other devices.

→ Advantages :-

- No traffic
- Robust as failure of one link does not affect the entire system.

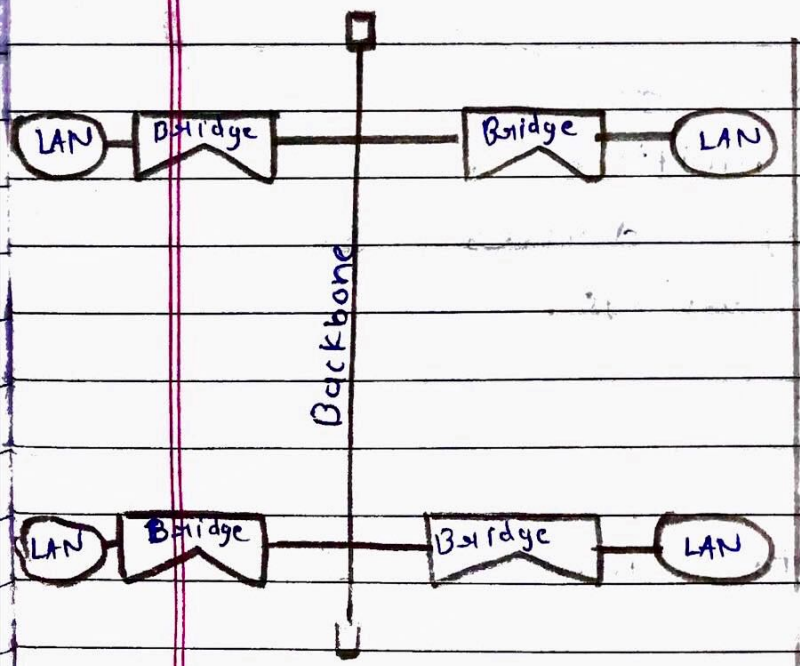
→ Disadvantages :-

- Expensive
- complex

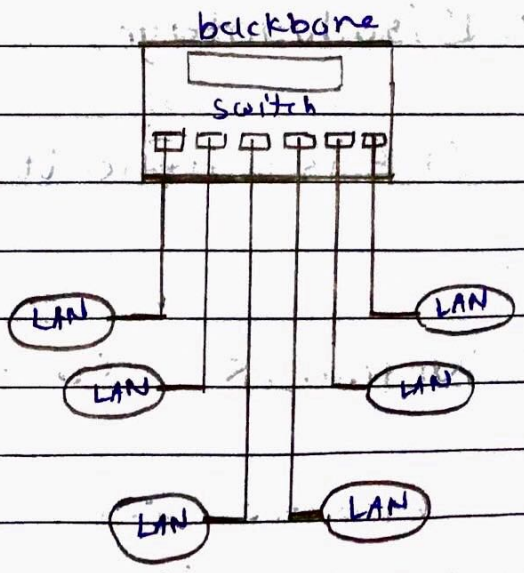
(4) Backbone Topology :-

→ In a bus backbone, the topology of the backbone in a bus.

In a bus backbone, the topology of the backbone is a bus.



In a star backbone, the topology of the backbone is a star; the backbone is just a on switch.



→ A Backbone network allows several LANs to be connected together.

→ A Backbone to can be tie together diverse network in the same building, in different buildings in a campus environment, or over wide areas.

→ Advantages :-

- We can connect multiple network using network connecting devices such as hub, switch or bridge.

→ Disadvantage :-

- It is difficult to maintain privacy.

mple * Network connecting Devices :-

→ Network connecting devices used to connect to or more network:

(1) NIC (Network interface card)
(2) HUB
(3) Switch
(4) Router

(1) NIC (Network interface card)

→ The network interface card allows computers to communicate with each through the network

→ NIC have LED ~~inter~~ indicators showing the network connectivity

→ Each NIC has a 48-bit unique hexadecimal address called the MAC address.

→ An example of a MAC address:
A1B2C3D4E5F6.

• convert into binary:

0-9
10-A
11-B
12-C
13-D
14-E
15-F

A	1	B	2	C
8421	:	:	:	:
1010	0001	1011	0010	1100

3	D	4	E	5
:	:	:	:	:
0011	1101	0100	1110	0101

F	6
:	
1111	0110

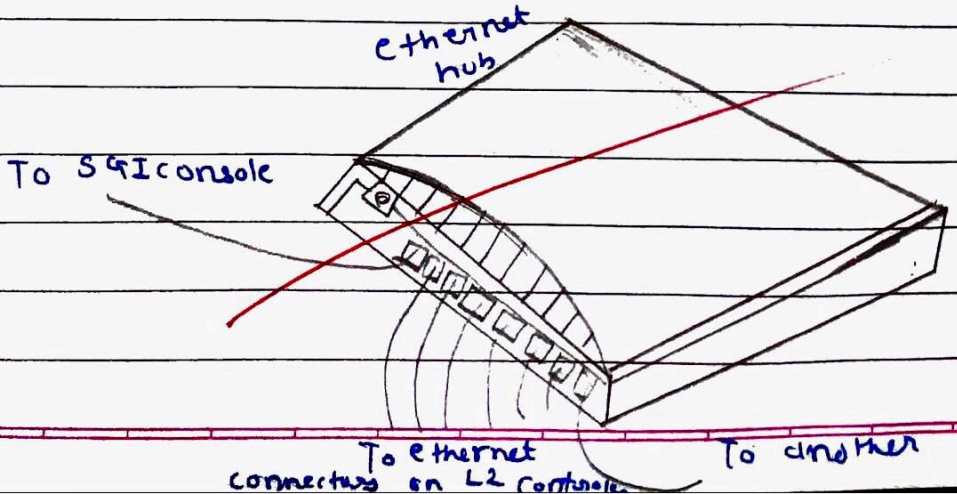
→ If there are two separate LEDs one of them may be Link LED, which illuminates when proper connectivity to an active network is detected.

(2) HUB :-

→ In a Hub, the signals received on one port are transmitted to all other ports, and vice versa.

→ All nodes connected using a Hub can listen to one another all the time but based on addressing in the frame, only the inteded recipient receives it.

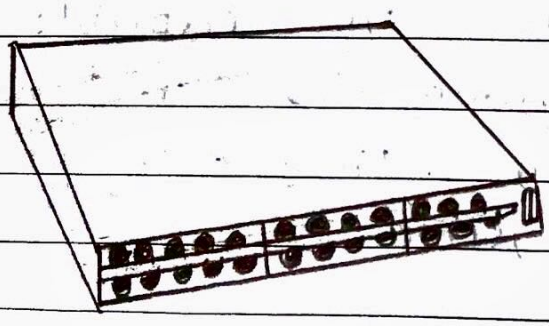
→ It is important to note that hubs are nothing more than repeaters, which are in capable of recognizing frame boundries and data structures, that's why they act with such a lack of intelligence



(3) Switch :-

→ Like a hub, a switch connects multiple segements of a network together, with one important difference.

→ Whereas a hub sends out anything it receives on one port to all the others, a switch recognized frame boundries and pays attention to the destination MAC address of the incoming frame.



(4) Router :-

→ A Router connects multiple, often disimilar networks.

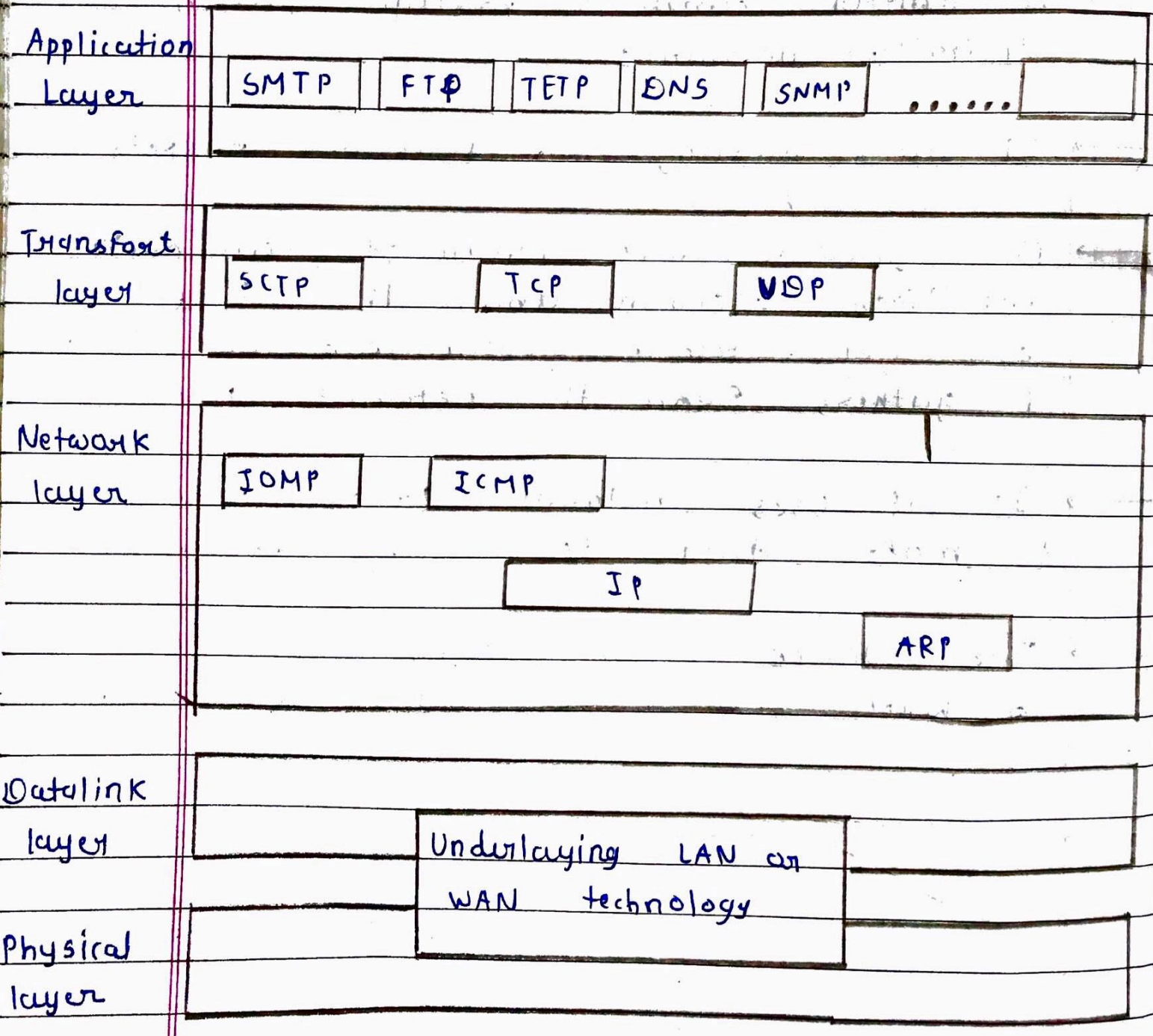
→ It uses routing to forward packets

→ The router, once connected, can make intelligent decisions about how best to get network performance data that it gathers from the network itself.

→ It is uses network layer address to make data forwarding decisions.

→ The device can connect a LAN to a WAN or a WAN to a WAN.

* Position of Protocol in TCP/IP protocol switch :



* Address Maping :-

→ A logical address is an internetwork address, and it is unique universally

→ It is called logical Address because it is implemented in a software.

→ It is also known as IP address or software address.

→ IPv4 is 32 bit long.

→ IPv6 is 128 bit long.

→ A physical address is a local address is a local address and it should be unique locally but not necessarily universally.

→ It is called a physical address because it is usually implemented in a hardware.

Ex:- NIC

→ For ethernet protocol the physical address is 48 bit long.

→ It is also known as hardware address on MAC address.

→ The delievery of a packet to a host or a router requires two levels of addressing : A logical And physical.

→ We need to be able to map a logical address to is corresponding physical address and vice-versa.

→ This can be done using static on dynamic Mapping.

* Static Mapping :-

→ Static mapping means creating a table that mates a logical address with physical Address.

→ This table is stored in each machine on the network.

→ Any machine wants to map the address can look out in this table.

IP Add.	Physical Add.
127.5.5.0	A2F3045680F2
-	-
-	-
-	-
-	-

* Limitation of Static Memory :-

(1) Change in NIC, while change physical address.

(2) Many networks changes physical address every time the computer in turned on.

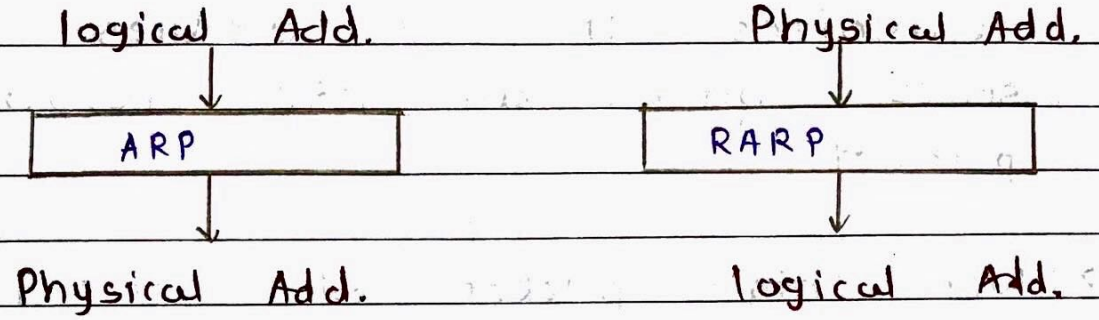
(3) When a computer moves from one physical network from another it changes its physical address.

→ to implement that changes in physical address the static mapping table must be updated periodically.

→ This overhead could affect network perfomance.

* Dynamic Mapping :-

→ In dynamic mapping we use ARP (Address Resolution Protocol) and RARP (Reverse address Resolution Protocol) to map logical Address to vice-versa.



* ARP Operation :-

→ Any time a host or a Router needs to find the physical address of another host or router on its network it sends an ARP query / Request packet. The packet includes sender and IP address of a receiver.

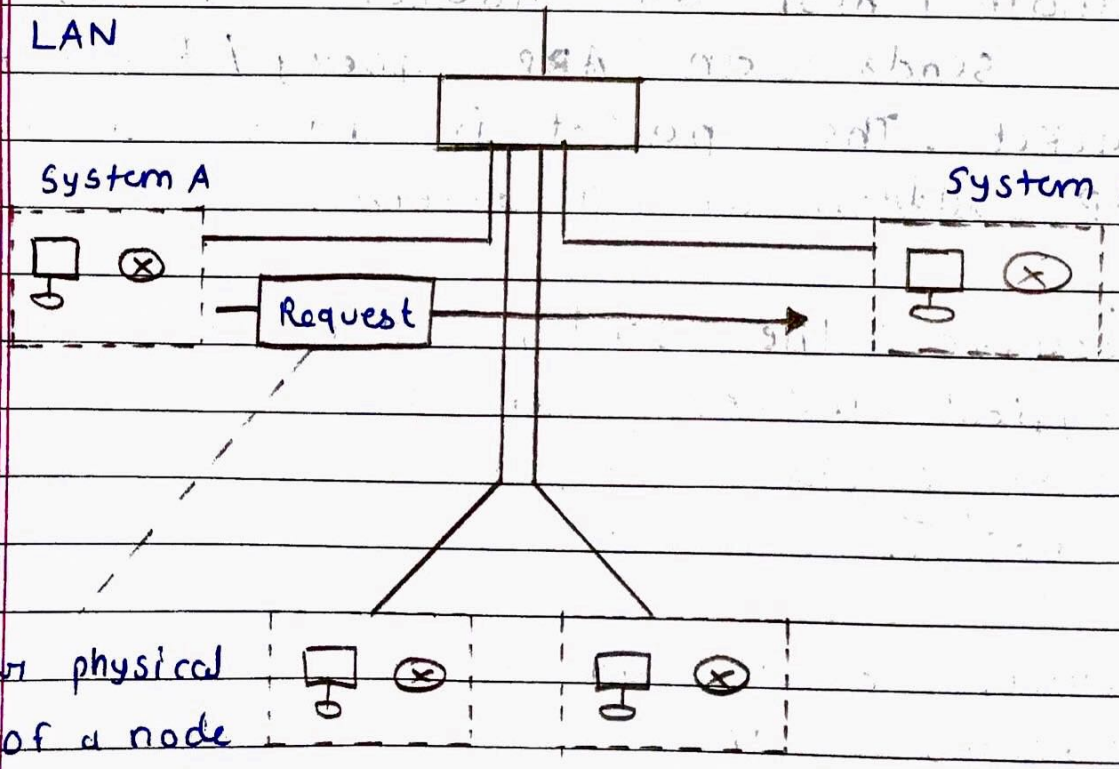
→ Because the sender does not know the physical address of the receiver this query packet is broadcast over the network.

→ Every host or router on network receives and processes the ARP request packet, but the intented receipient

recognizes its IP address and sends back an ARP response packet.

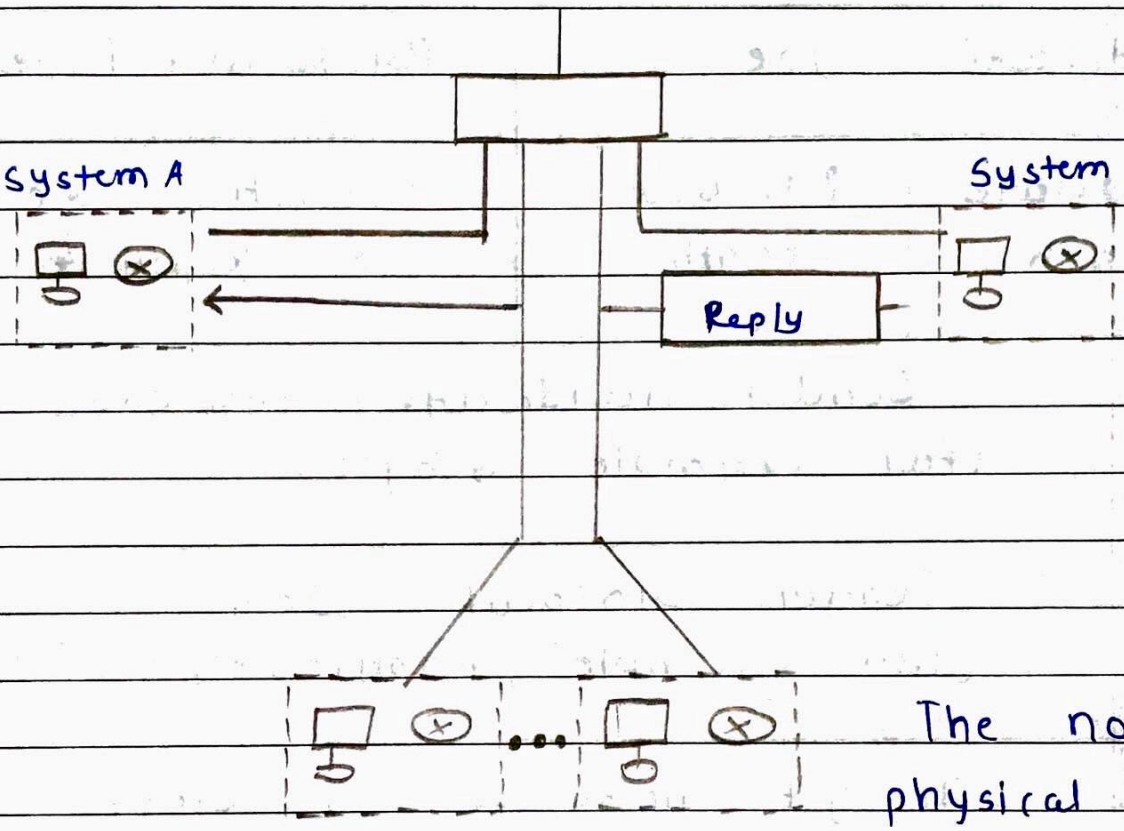
→ Now this packet also contains receivers physical address the packet is unicast to the packet.

→ The packet is unicast directly to the inquirer using the physical address received in the query packet



looking for physical address of a node with IP address 141.23.56.23

a. ARP Request is multicast



b. ARP reply is unicast

The node physical address is A4:6E:F4:59:83:AB

* ARP packet format:-

Imp

Hardware type		Protocol Type
Hardware length	Protocol length	Operation request 1, Reply 2
Sender hardware address (For example, 6 bytes For ethernet)		
Sender protocol address (For example, 4 bytes For IP)		
Target hardware address (For example, 6 bytes for ethernet (It is not filled in a request		
Target protocol address (For example, 4 byte for IP		

→ **Hardware type**: This is a 16 bit HTYPE Field defines the type of the physical network. Its value is 0013_{16} for an ATM network.

→ For example, For ethernet hardware the type is one.

→ **Protocol Type :-** This is a 16 bit field defining the protocol type.

→ For example, For IPv4 the value is 0800_{16}.

→ **Hardware length :-** This is an 8 bit field defining the length of physical address in bytes.

→ For example, ethernet has value 6 bytes. (48 bit divided by 8 = 6 byte).

→ **Protocol length :-** This is an 8 bit field defining the length of logical address in bytes.

→ For example, For IPV4 the length is 4 bytes (32 bit / 8 = 4 b byte)

→ **Operation :-** This is a 16 bit field defining the type of the packet. For request packet the value is one and for reply packet the value is 2.

→ **Sender hardware address :-** This is a variable length field defining the physical address of the sender.

→ **Sender protocol address :-** This is a variable length field defining the logical address of the sender.

→ **Target hardware address :-** This is a variable length field defining the physical address of the target or receiver.

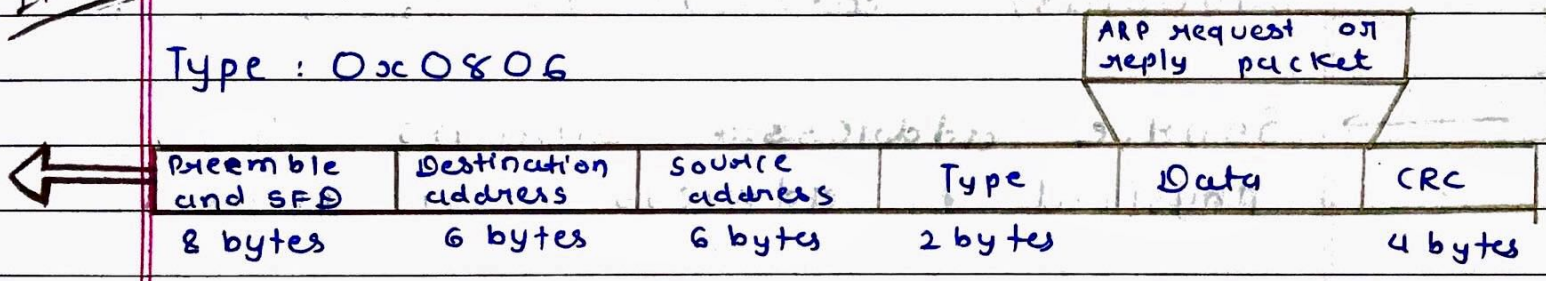
→ For an ARP request message, this field is all zeros because we don't know the physical address of receiver yet

→ Target protocol address :- This is variable length field defining the logical address of the target.

* ARP Encapsulation :-

IMP

Type : 0x0806



→ Preemble and SFD :- The field is of 7 bytes, which alerts the receiver of the coming frame and enable it to synchonize its input timing.

→ SFD :- Start Frame Delimiter

→ The SFD warns the station that this is the last chance for synchonization.

→ **Destination address** :- Contains the physical address of destination. Field with broadcast address for the request.

- broadcast address is FF, FF, FF, FF, FF, FF

→ **Source address** :- Contains the physical address of sender.

→ **Type**: This field contains the protocol used in upper layer for example, ARP, TCP, UDP

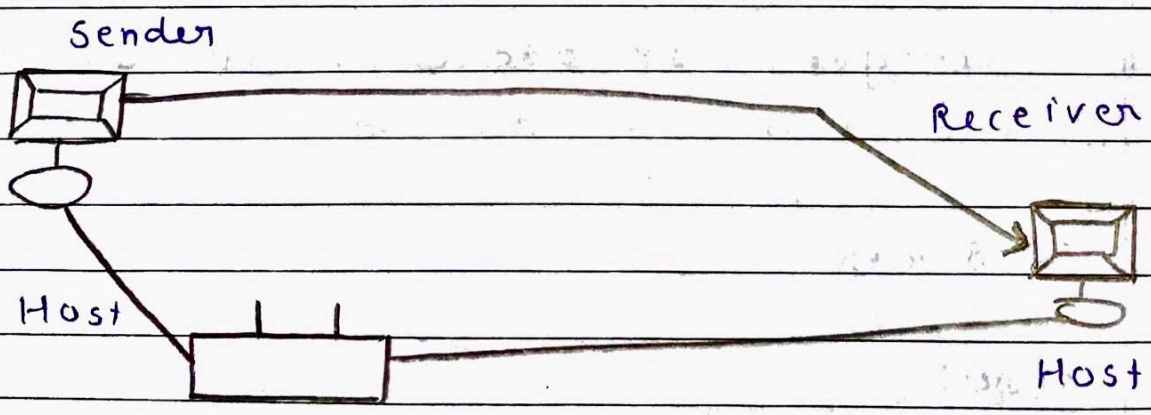
→ **Data**: This field carries packets from upper layer protocol (network layer)

→ **CRC (Cyclic Redundancy check)** :- This is a error detection technique used to find out errors in the receive frame.

* Four cases in which ARP service can be used :

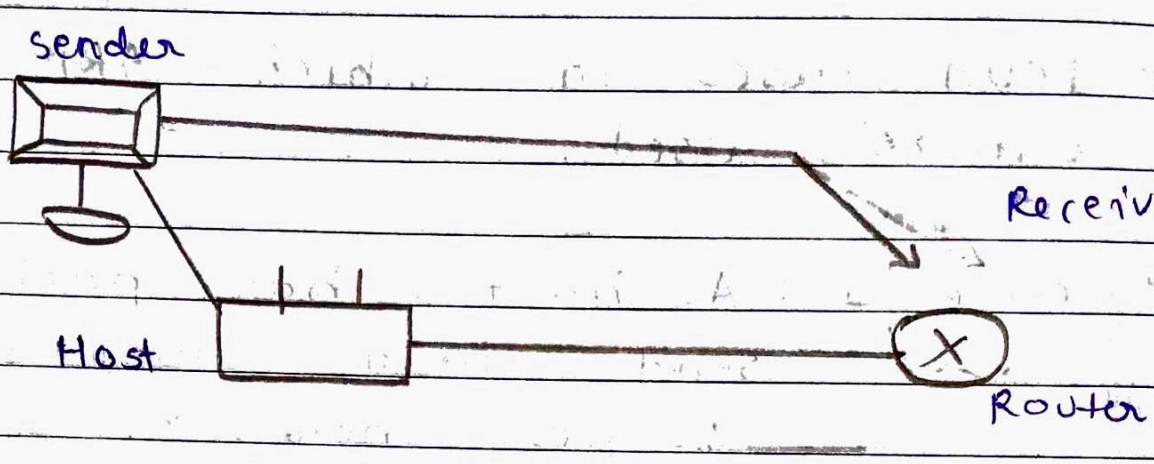
- case 1 : A host has packet to send to a host on the same network.

  Target IP address : Destination address in the IP datagram



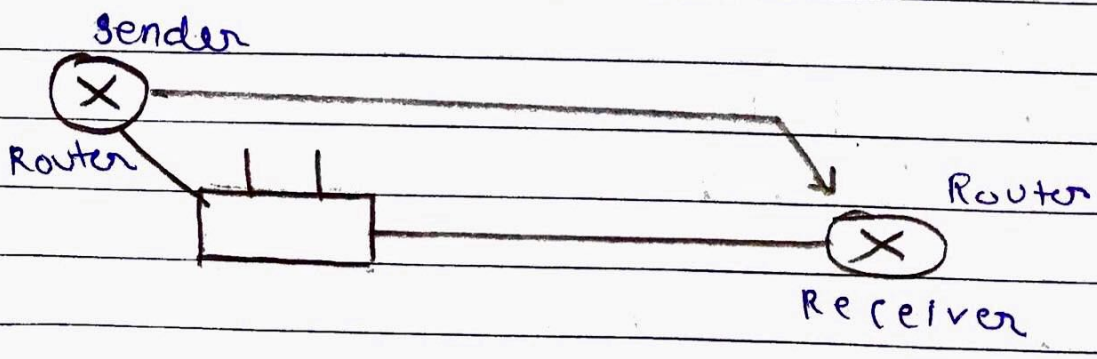
- case 2 : A host a packet to send to a host on another level.

  Target IP address : IP address of a router.



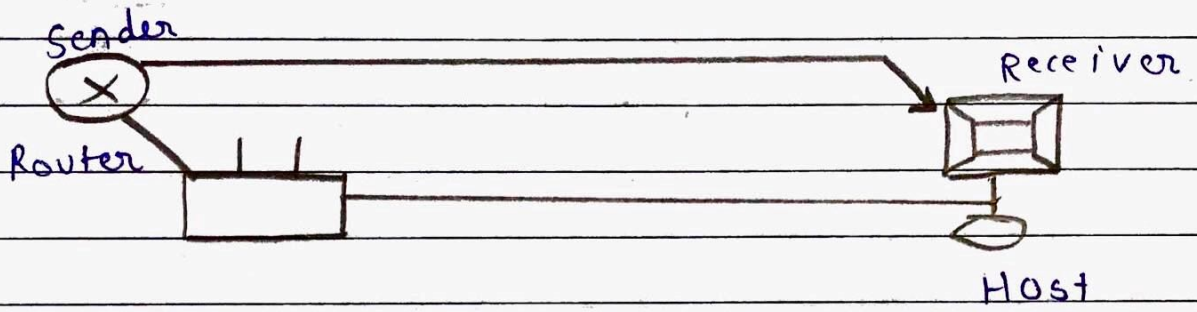
- Case 3 : A router has packet to send to a host on another network

Target IP address : IP address of a router.



- case 4 : A router has a packet to send to a host on the same network

Target IP address: Destination address in the IP diagram.



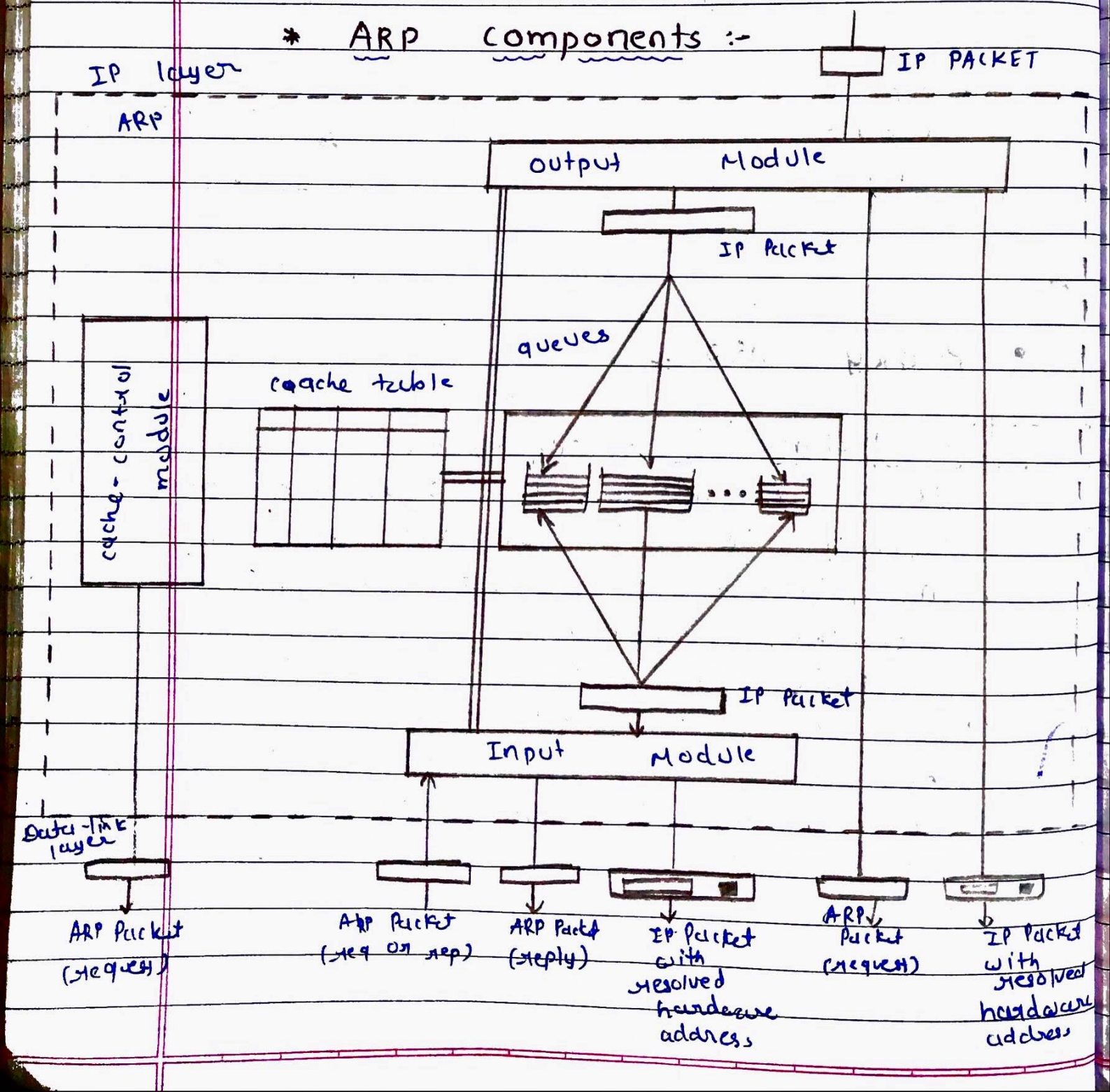
- **Proxy ARP :-**

A technique called proxy ARP is used to create a subnetting effect. A proxy ARP is an ARP that acts on behalf of a set of hosts. Whenever a router running a proxy ARP receives an ARP request looking for the IP address of one of these hosts, the router sends an ARP reply announcing its own hardware (physical) address. After the router receives the actual IP packet, It sends the packet to the appropriate host or router.

Page
Date

* ARP PACKAGE :-

* ARP components :-



→ An ARP package involves following components :-

(1) Cache Table
(2) Queus
(3) Output modules
(4) Input modules
(5) Cache control module

Imp(e)

(1) Cache Table :-

Imp(e) Imp(e)

State	Queue	Attempt	Time-out	Protocol add.	Hardware add.
R	5		900	180.3.6.1	ACAE32457342
P	2	2		129.34.4.8	
P	14	5		201.11.56.7	
R	8		450	114.5.7.89	457342ACAE32
P	12	1		220.55.5.7	
F					
R	9		60	19.1.7.82	4573E242ACA
P	18	3		188.11.8.71	

- **State** :- This column shows the state of the entry.

→ It can have one of three values: FREE, PENDING, or RESOLVED.

→ The Free state means that the time-to live for this entry has expired.

→ The PENDING state means a request for this entry has been sent, but the reply has not yet been received.

→ The RESOLVED state means that the entry is complete.

- **Queue Number**: ARP uses numbered queues to enqueue the packet waiting for address resolution. Packets for the same destination are usually enqueued in the same queue.

- **Attempts :-** This column shows the number of times an ARP request is sent out for this entry.

- **Time-out :-** This column shows the lifetime of an entry in second.

- **Protocol Address :-** This column shows the destination IP address.

- **Hardware Address :-** This column shows the destination hardware address. It remains empty until resolved by on ARP reply.

(2) **Queues :-**

→ Our ARP package maintains a set of queues, one for each destination, to hold the IP packets while ARP tries to resolve the hardware address. The output module sends unresolved packets into the corresponding queue the input module removes a packet from a queue and sends it, with the resolved physical address, to the data link layer for transmission.

(3) Output Module :-

```
ARP_output_Module()
{
    Sleep Until an IP Packet is
received from IP software. check cache
table for an entry corresponding
to the destination of IP address.
Packet.

  If (entry is found)
{
    Extract the value of the hardware
address from the entry send the
packet and the hardware address to
date link layer.
  Return
}   // end if

    IF (the State is PENDING)
{
```

Enqueue the packet to the corresponding queue.

Return

} // end if

} // end if

If (entry is not found)

{

Create a cache entry with state set to PENDING and ATTEMPTS set to 1.

Create a queue.

Enqueue the packet.

Send an ARP request

Return

} // end if

} // end module

(4) Input Module :-

ARP_Input_Module()

{

Sleep until an ARP packet (request or reply) arrives. check the cache table to find the corresponding entry.

```
IF (Found)
{
    Update the entry
    IF (the state is PENDING)
    {
        while (the queue is not empty)
        {
            Dequeue one packet
            Send the packet and the hardware
            address.
        } // end if
    } // end if
}// end if
 IF (not found)
{
    Create an entry.
    Add the entry to the table.
} // end if
 IF (the packet is a request)
{
    send an ARP reply
} // end if
   Return
} // end module
```

(5) Cache - control Module :-

```
ARP_ Cache_ control_ Module ()
{
    Sleep until the periodic timer matures.
    Repeat for every in the cache
    {
        IF (the state is PENDING)
        {
            Increment the value of attempts by 1.
            IF (attempts greater than maximum)
            {
                Change the state to FREE.
                Destroy the corresponding queue.
            } // end if
            else
            {
                send an ARP request
            } // end else
            continue.
        } // end if
        IF (the state is RESOLVED),
```

{

Decrement the value of time-out,

IF (time - out less than or equal 0)

{

change the state to FREE

Destory the corresponding queue.

} // end if

} // end if

} // end report

Return

} // end module

* RARP MAP :-

→ RARP maps physical address to an ip address. However, RARP only provides IP address, which is not sufficient for a communicator.

→ Most need following information for the communication :-

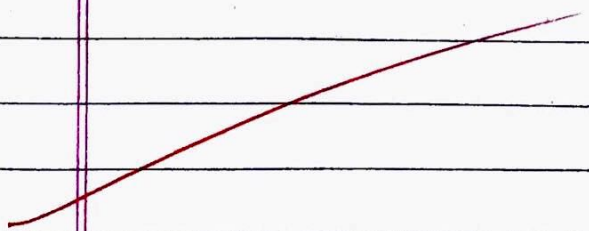
(1) The IP address of the computer
(2) The subnet mask of the computer
(3) The IP address of the router
(4) The IP address of a name server.

→ The alternate solution in case of RARP is provided by following few protocols :-

Imp (2)

(1) Boot P (Boot strap protocol)
(2) Dhcp :- (Dynamic host configuration protocol)

* RARP Packet format :-



Hardware type		Protocol Type
Hardware length	Protocol length	Operation Request 3, Reply 4
Sender hardware address (For example, 6 byte For ethernet)		
Sender protocol address (For example, 4 bytes For IP)		
Target hardware address (For example, 6 bytes For ethernet) (It is not filled in a request)		
Target protocol address (For example, 4 bytes Par IP)		

- **Operation** :- This is a 16- bit field defining the type of packet. Two packet types are defined RARP request 3, RARP Reply 4.

- **Sender hardware Address :-** This is a variable - length field defining the physical address of the sender for example, for ethernet this field is 6 bytes long.

- **Sender Protocol Address :-** This is a variable e- length field defining the logical address of the sender, for the Ip protocol, this field is 4 bytes long.

- **Target hardware address :-** This is a variable - length field defining the physical address of the target.

- **Target protocol address :-** This is a variable length field defining the logical address of the target for IPv4 Protocol, this field is 4 bytes long.