Page No.:
Date: / /

switching -

1) Passage of message ~~involvs~~ from source to destination involves many decisions.
2) When a message reaches a connecting device a decision needs to be made to select one of the output ports through which packet needs to be send out.
3) In other words, connecting device act as a switch that concers one port to another port.

- circuit switching
- Packet switching

① circuit switching →

1) one solution to the switching is referred to as circuit switch. In which a physical circuit established bet^n source and destin^n of the message before the delivery of the message.
2) After the circuit established, the entire message is transferred from source to destination.
3) The source can then inform the network that the transmission is complete which allows the net work to open all switches and use the links and connecting device ~~for~~ another connection.
4) The circuit switching was never implemented at the network layer. It is mostly used in the physical layer.

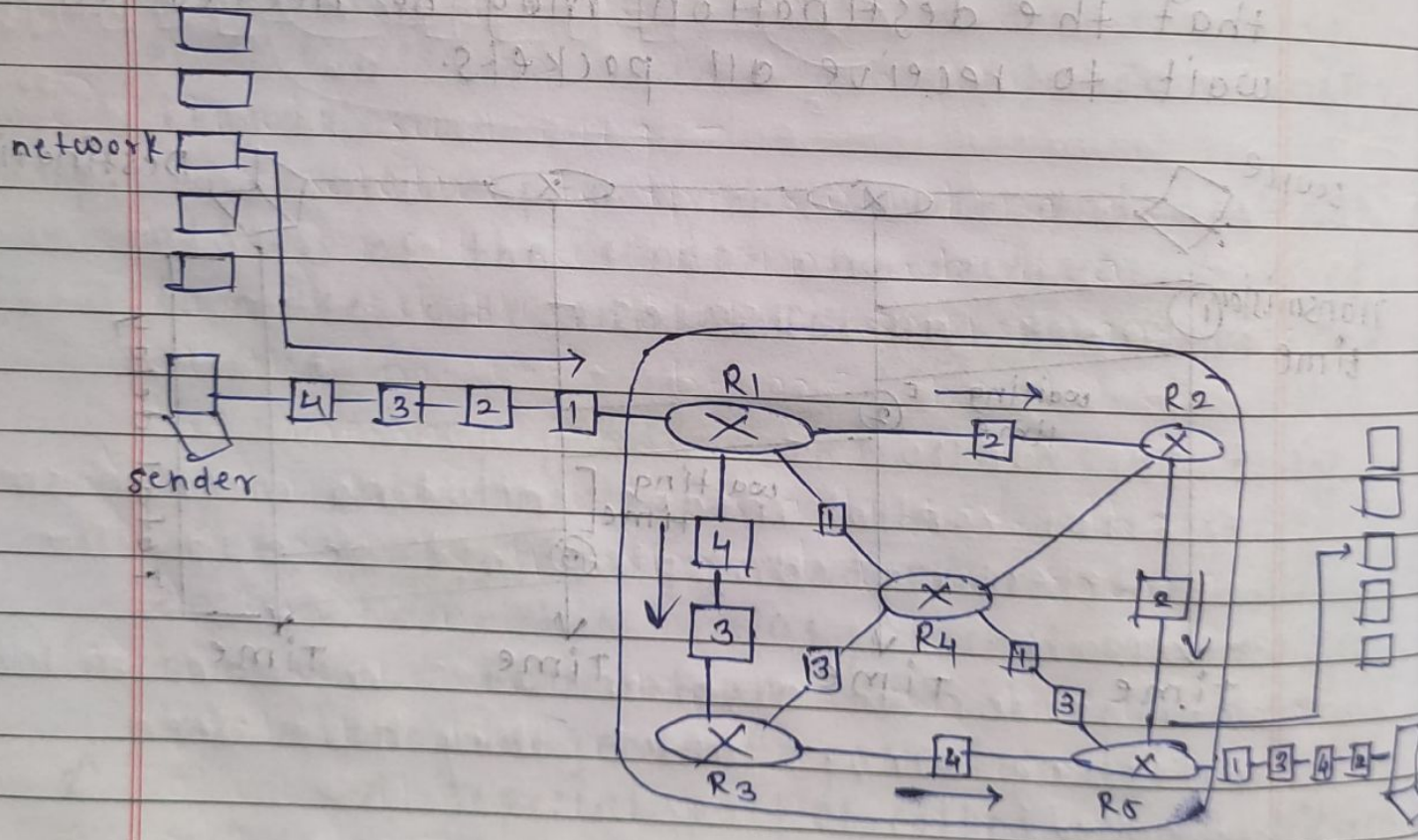
5) Whole message send from source to destinat" without divided into packet
Ex- Telephone system.

(2) packet switching -
1) The network layer in the internet today is the packet switched networks.
2) A message from upper layer is divided into managable packet. and each packet is send through network.
3) The source of the message send packets one by one. the destination of the msg receives the packets one by one.
4) The destination waits for all the packets belonging to the same msg. To arrive before delivering msg to the upper layer.
5) Packet switched network can used to diff. approach to route the packets the datagram approach and virtual circuit approach.

* packet switching At network layer -
1) packet at source is divided into manageable packet normally called datagrams.
2) Individual datagrams are then transferred from source to destination.
3) The packet switched network layer of the internet was originally designed as connectionless service, but recently there is a tendency to change this connection oriented service.

- Connectionless service -

1) ~~When~~ The packets in msg may or may not be travelled in same path to their destination. when
2) when the internet started it was decided to make a ~~connecti~~ network layer a connectionless service to make it simple.
3) when NL provides a connectionless service each packet travelling in a internet is an independent ~~inten~~ entity. There is no relationship ~~bet~~ between packet belonging to the same msg
4)



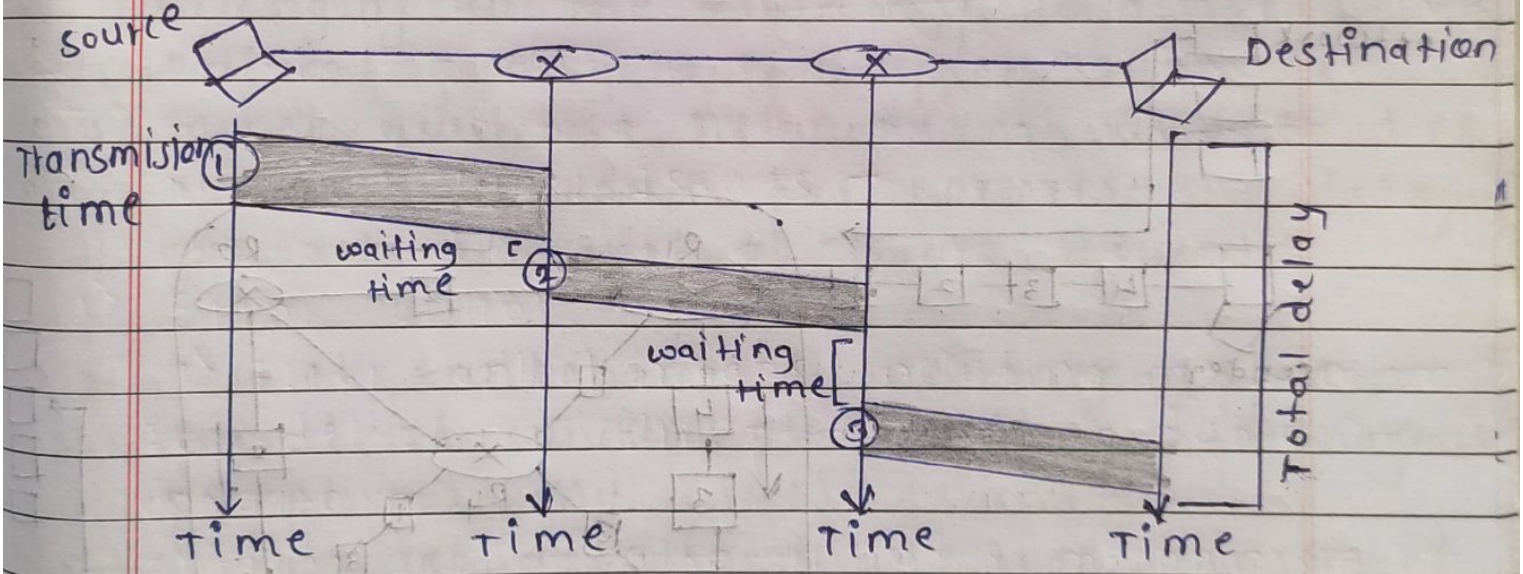
4) The switches in these type of network called routers. Each packet is routed based on the information contained in its header: source and destination add.

5) Destination address where it should go the source address defines where it comes from.

6) The router in these case the packet based only on the destination address. source address may be used to send error message to the source if the packet is discarded.

7) Delay in connectionless network -

① If we ignore the fact that the packet may be lost and resend and also the fact that the destination may be needed to wait to receive all packets.



- Connection oriented service-

1) There is relation bet^n all the packets belonging to a message.
2) Each packet based on the forwarded label in the packet. To follow the idea of connection oriented design to be used in the internet we assume that packet has label when it reaches the router.
3) In these case, forwarding decision is based on the value of label or virtual circuit identifier as it is sometimes called.
4) To create connection oriented service three phase process is used : set up, data transfer, teardown.

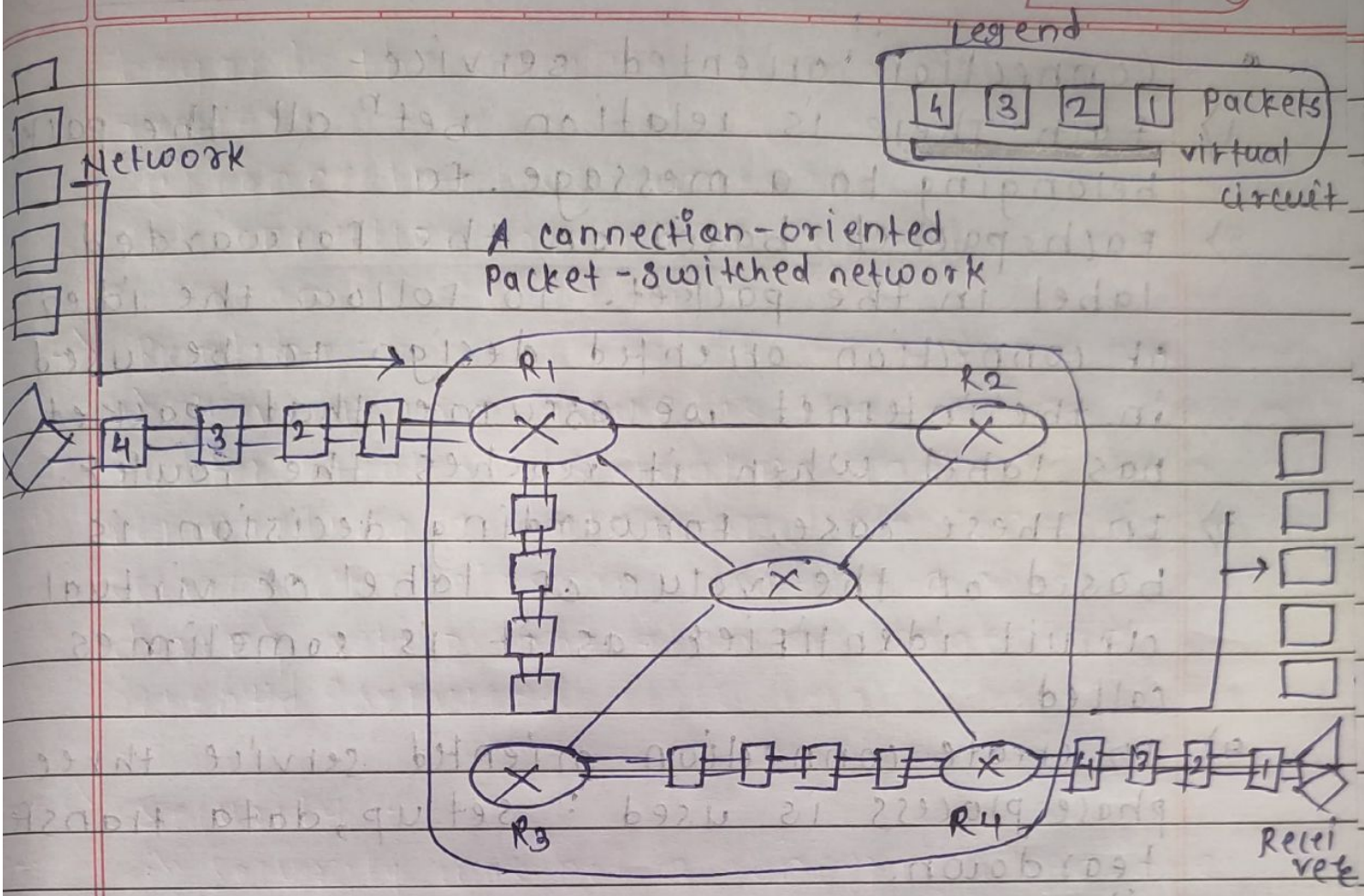
set up: i) In set up phase the source and destinat^n address of the sender and receiver is used to make table entries for connection oriented service.

ii) In set up phase router creates an entry for virtual circuit.

iii) Request packet is send from source to destination. This auxilary packet carries source and destination address.

iv) Acknowledgement packet :

5) A sepecial packet called acknowledgement packet comple the entries in the switching table.



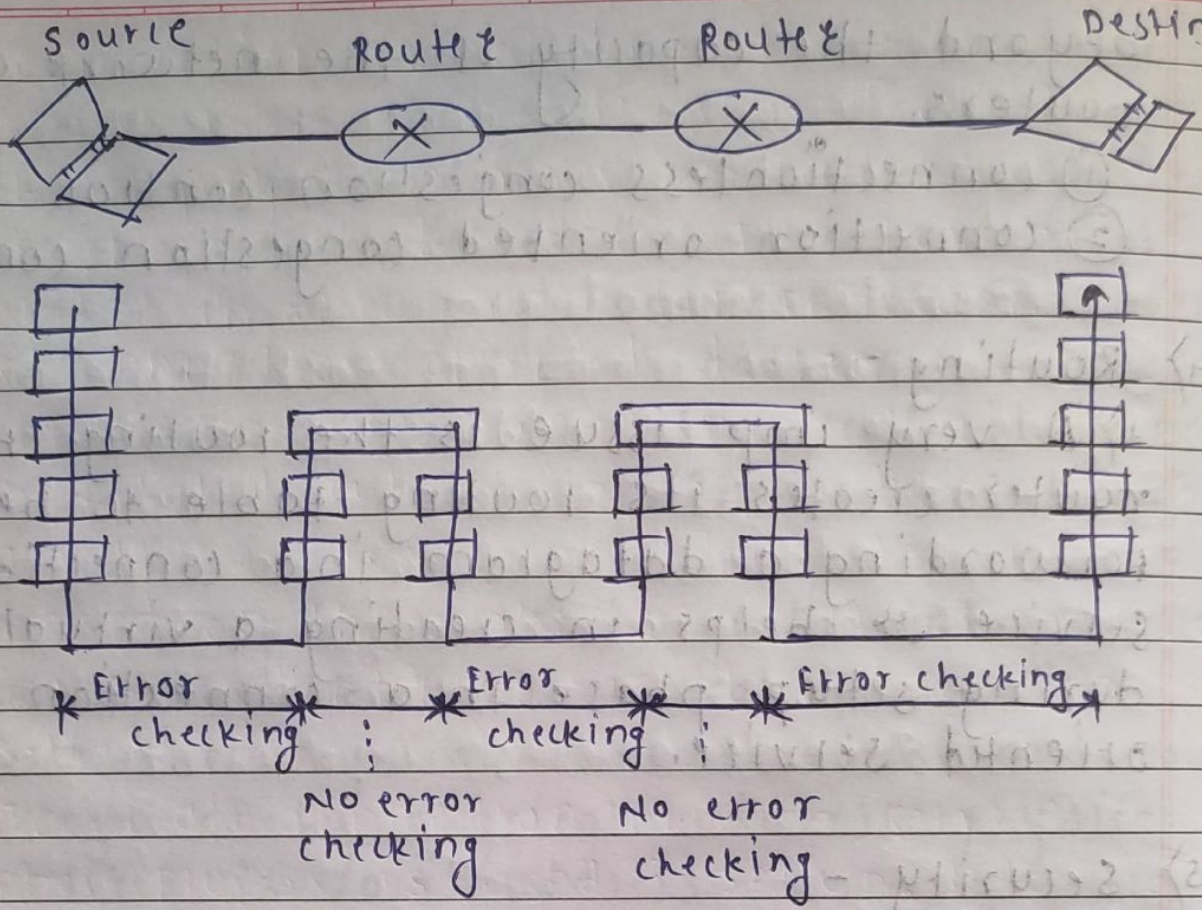
* Network layer Issues -

1) Error control -

1) Error control means including mechanism for detecting corrupted lost or duplicate datagram.

2) Error control also includes mechanism for correcting errors after they have been detected.

3) At the surface level it looks as though there is no need for error control at the network layer because each datagram passes through several networks before reaching its final destination.



2) Flow control -

1) Flow control regulates the amount of data source can send without ~~over the~~ overwhelmin the receiver, to control the flow of data the receiver send some feedback to the sender to inform the later it is overwhelme with data.

2) No flow control provided for the current version of Internet network layer.

3) Congestion control -

1) congestion in the network layer is the situation in which too many datagram are present in an area of the internet

2) congestion may occur if the number of datagrams sent by source computers are

beyond the capacity of the network or routers.

① connectionless congestion control.
② connection oriented congestion control.

4) Routing -

i) A very imp issue is the routing. How a router creates its routing table to help in forwarding a datagram in a connectionless service or helps in creating a virtual circuit during setup phase in a connection oriented service.

5) Security -

i) Security was not a concern when the internet was originally designed because it was used by a small no. of users at the universities to do research activities. Other people had no ~~use~~ access to the internet.

* ARP (Address Resolution protocol)

1) Address Mapping -

1) The hosts and routers are recognized at the network level by their logical addresses. A logical address is an internetwork address. logical address unique universally. It is called logical address because it is usually implemented in software.

2) Every protocol deals with interconnecting networks requires logical addresses.

3) At the physical level the host and routers recognized by physical address. physical address is local address.

4) There are two types of Mapping -

1) static Mapping.

2) Dynamic Mapping.

- static Mapping -

① static mapping means creating a table that associate a logical address, with the physical address.

② This table is stored in each machine on the network.

③ physical address may change ~~with~~ in following ways -

1. Machine could change its NIC, resulting in a New physical address.

2. In some LANS, such as LocalTalk, the physical address changes every time the computer is turned on.

3. A mobile computer can move from one physical network to another resulting in change in its physical address.

- Dynamic Mapping -

① In dynamic mapping, each time machine knows the logical address of another mapping.

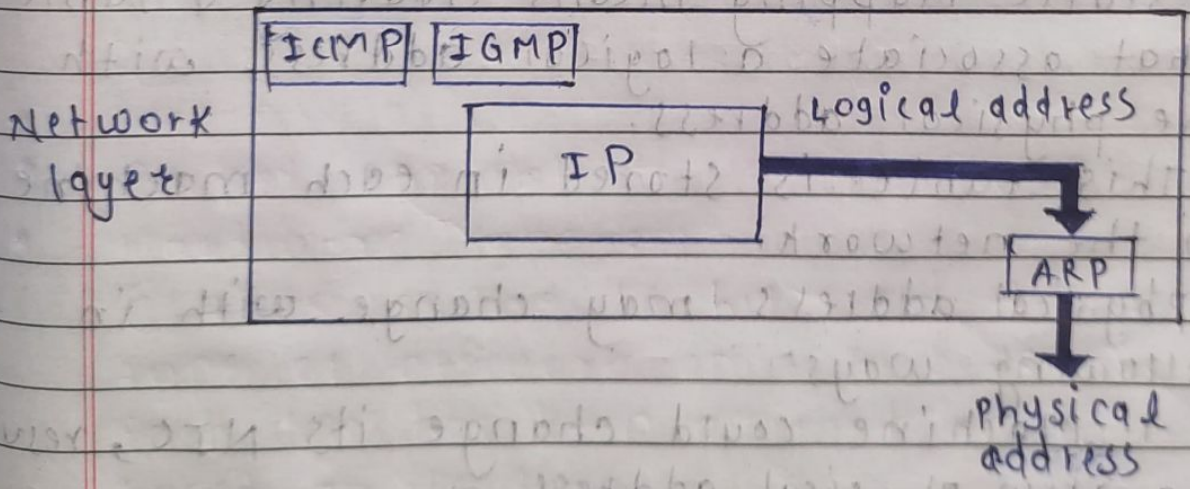
② It can use the protocol to find the physical address. protocol have been designed to perform dynamic mapping:

i) Address resolution protocol

ii) Reverse address resolution protocol.

* ARP Protocol -

1) ARP accept the logical address from the IP protocol, maps the address to the corresponding physical addres and pass it to the data link layer.



- ARP operation -

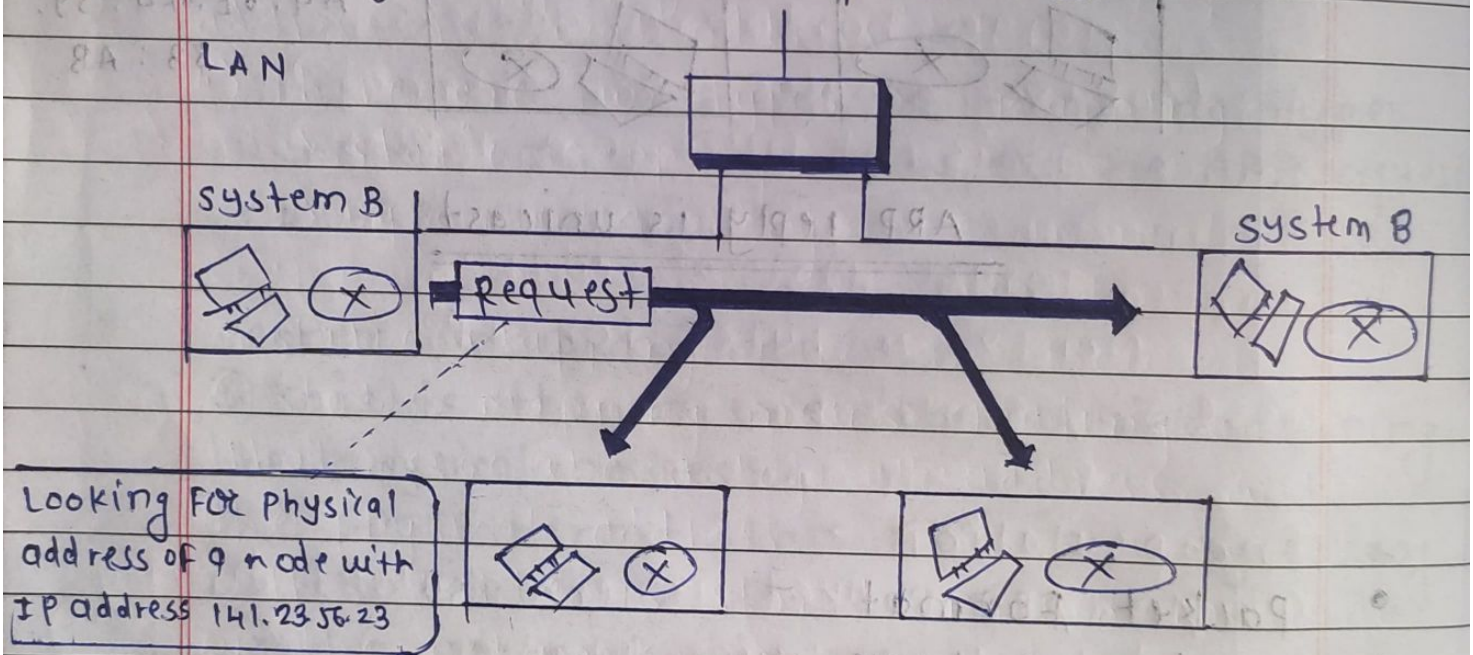
1) ARP broadcasts a request packet to all the machines on the LAN and asks if any of the

machines are using that particular IP.

a) ARP request is multicast -

① The system on the left A thas has packet that needs to be delivered to the system B with IP address, system A needs to pass the packet to its data link layer for actual delivery but it does not know the physical address of recipients.

② It uses the services of ARP by asking the ARP protocol to send a broadcast ARP request packet to ask for physical address of a system with an IP address.



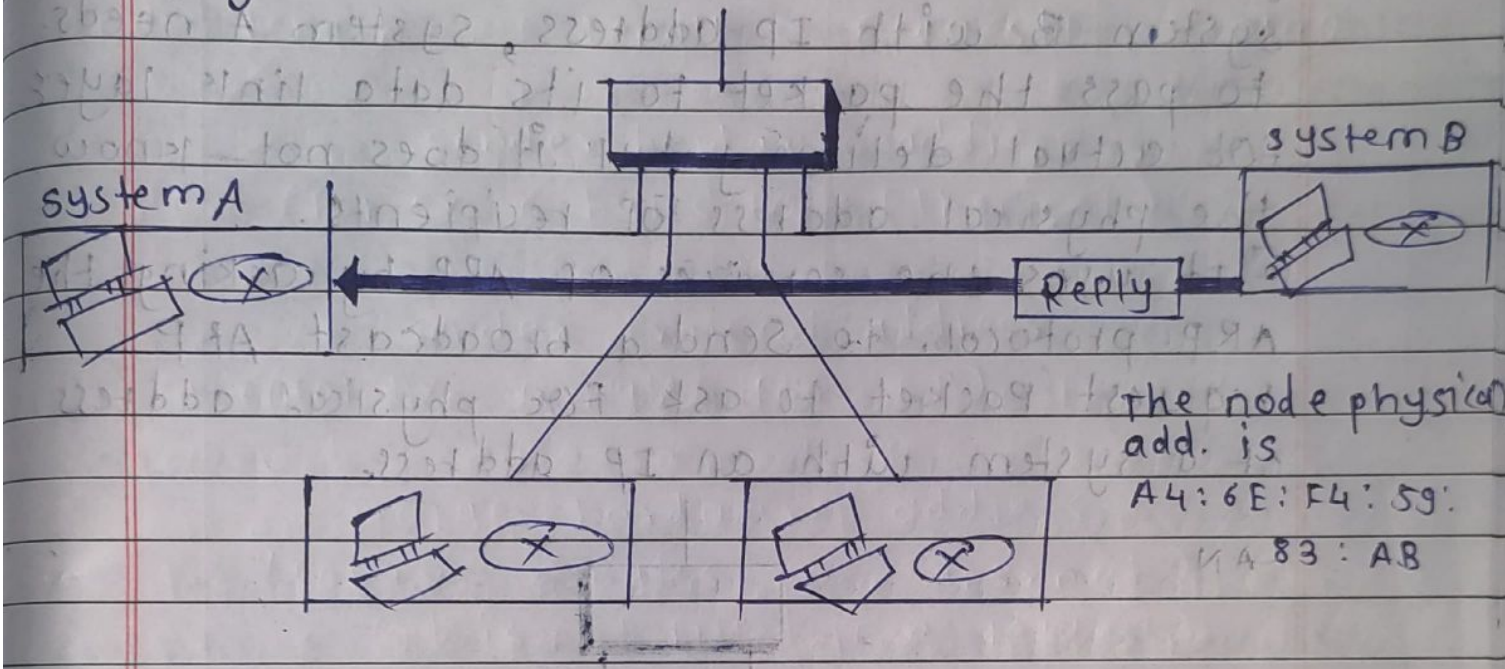
ARP request is multicast.

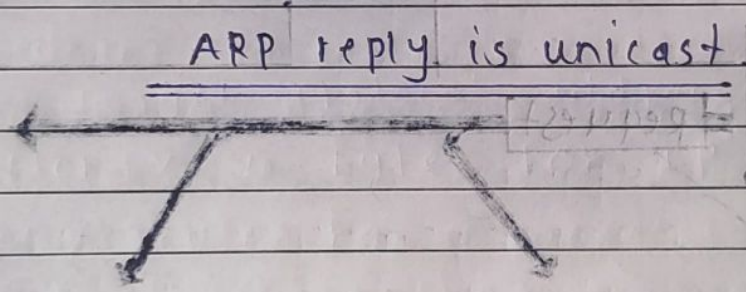
b) ARP reply is unicast -

① The packet is received by ~~any~~ every system on physical network but only system B will answer it. System B sends an ARP

reply packet that includes its physical address.

② Now, system A can send all the packets it has for these destination using the physical address it received.





- Packet Format -
- Hardware type :
  ① This is the 16 bit field defining the type of network on which ARP is running. Each LAN has been assigned an integer based on its type.
- Protocol type -
  ① 16 bit field defining the protocol.

Page No.:
Date: / /

Ex- Value of these field for the IPV4 protocol is 0800_{16} ~~base~~.

- Hardware length -
① This is an 8 bit field defining the length of the physical address in bytes.
Ex- For Ethernet value is 6.

- Protocol length -
① This is 8 bit field defining the length of the logical address.
Ex- IPV4 protocol value.

- Operation -
① This is 16 bit field defining the type of packet. Two packet types are ARP request and ARP reply.

- sender hardware address -
① This is the variable length field defining the physical address.
Ex- For Ethernet this field is 6 byte long.

- Sender protocol address -
This is the variable length field defining the logical address of the sender.
Ex- Ip protocol - For IP protocol this field 4 bytes long.

-

- ARP packet –

Hardware type		protocol type
Hardware length	protocol length	operation Request1, Reply2
sender hardware address (For Ex. 6 bytes for Ethernet)		
sender Protocol address (For Ex- 4 bytes for IP)		
target hardware address (For Ex- 6 bytes for Ethernet) (It is not filled in a request.)		
target protocol address (For Ex- 4 bytes for IP		

* Encapsulation –

① An ARP packet is encapsulated directly into data link ~~layer~~ frame.

Ex – ~~Encapsula~~ ARP packet is encapsulated in an ethernet frame. Note that the type field indicate ~~that~~ the data carried by the frame is an ARP packet.

ARP request or reply packet

Type: 0x0806

Preamble and SFD	Destination address	source address	Type	Data	CRC
8 bytes	6 bytes	6 bytes	2 bytes		4 bytes

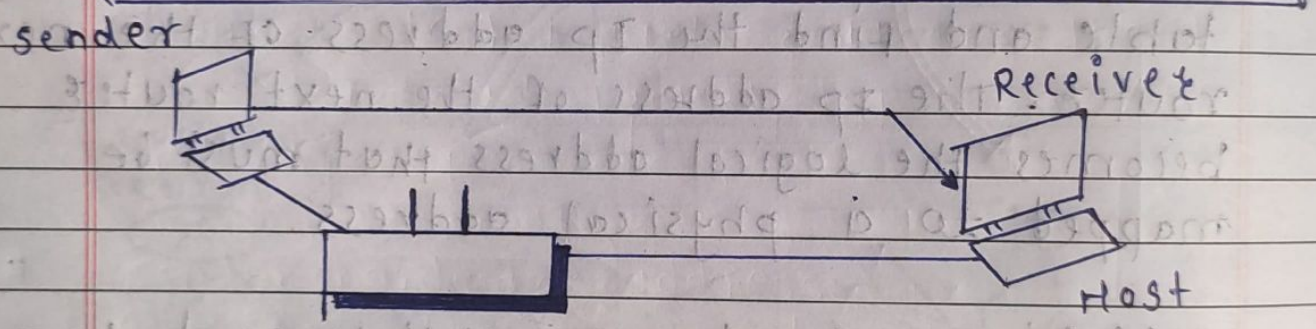
~~oper~~

* operations in ARP -

1) case 1 - The sender is a host and wants to send a packet to another host on the same network. In these case, the logical address that must be mapped to a physical address is the destination IP address in datagram header.

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

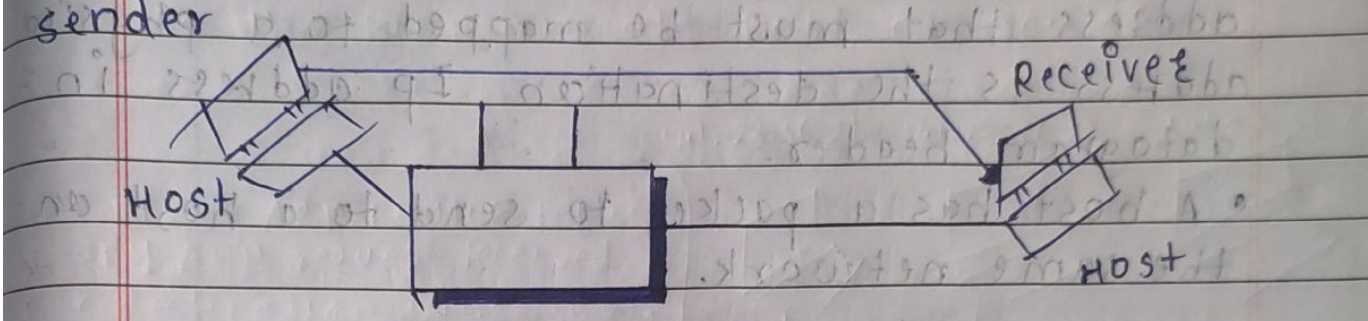
Target IP address:
Destination address in the IP datagram.



2) case 2 - The sender is the host and wants to send packet to another host on the network. In this case the host looks at its routing table and find the IP address of next Hop for the destination. If it does not have routing table it looks the IP address of the default router. The IP address of the router becomes the logical address that must be mapped to a physical address.

case 2: A host has a packet to send to a host on another network.

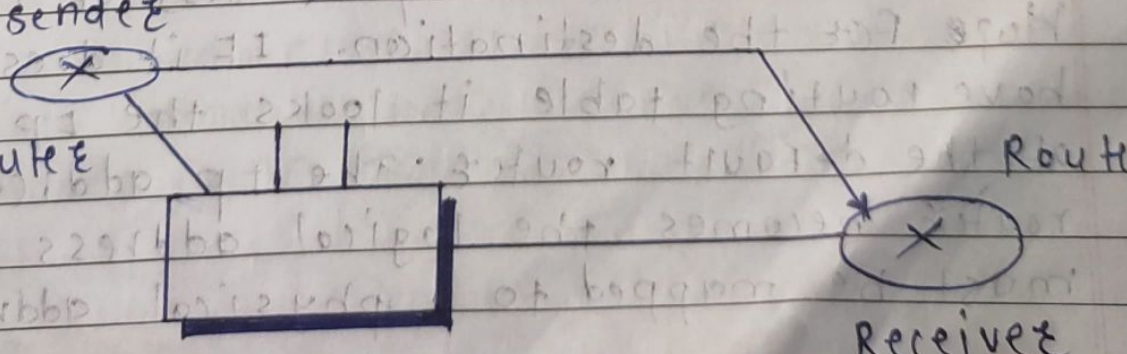
target IP address: IP add. of a router



3) Case 3 - The sender is a router that has received a datagram destined for a host on another network. It checks its routing table and find the IP address of the next router. The IP address of the next router becomes the logical address that must be mapped to a physical address.

case 3: A router has a packet to send to a host on another network.

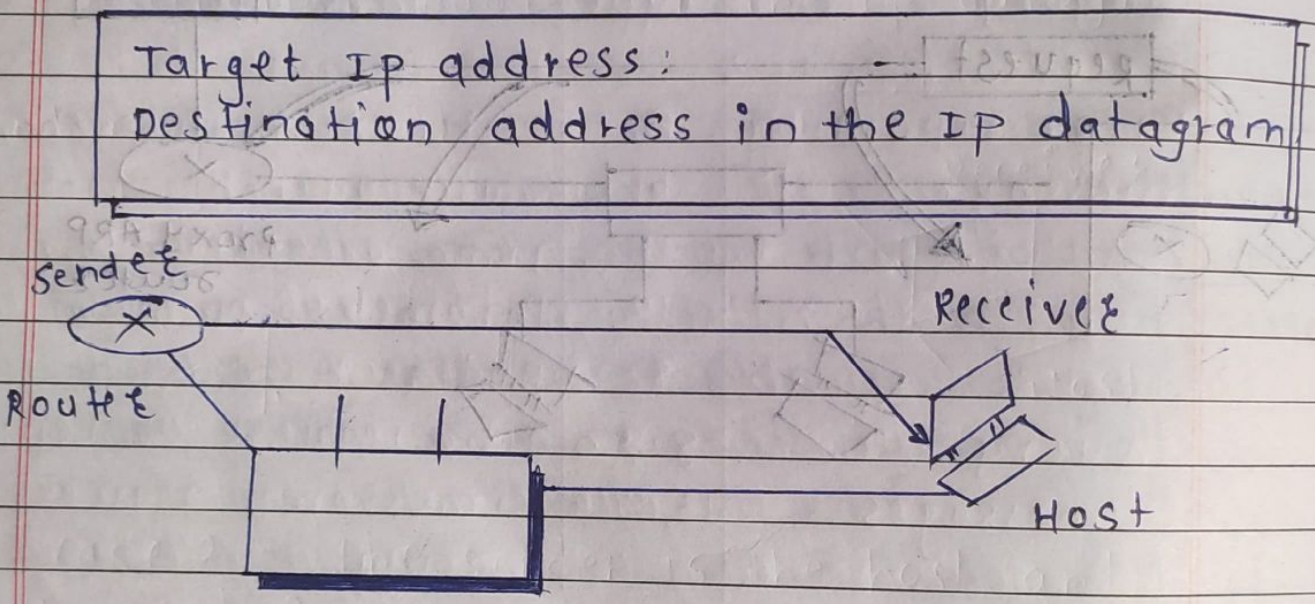
target IP address: IP add of router



4) case 4- The sender is a router that has received a datagram destined for a host in the same network. the destination IP address of the datagram, becomes the logical address that must be mapped to a physical address.

~~Target IP address:~~
~~Destination address in the IP datagram~~

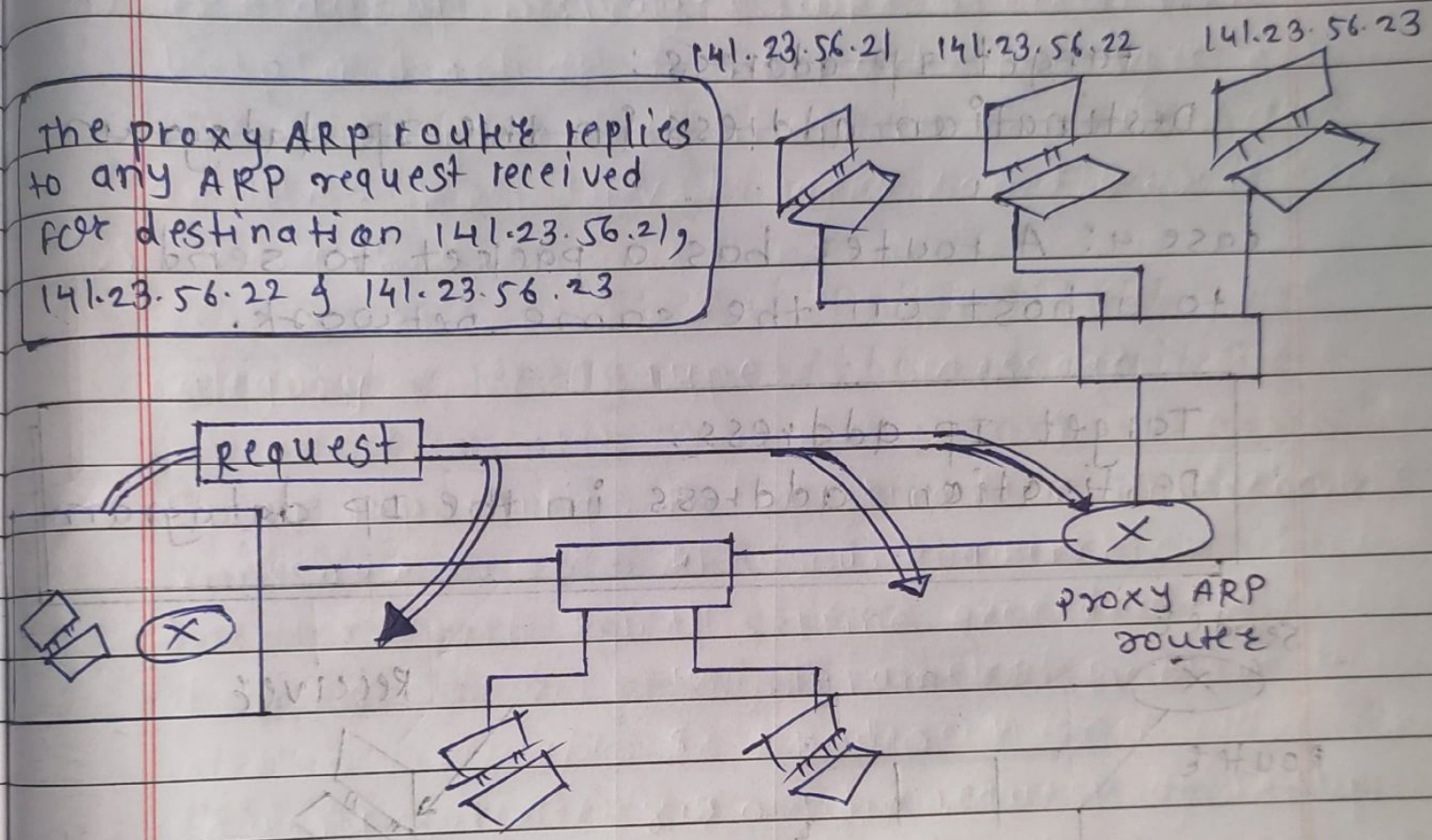
case 4: A router has a packet to send to a host on the same network.



* Proxy ARP -

1) A technique called proxy ARP is used to create subnetting effect.
2) A proxy ARP is an ARP that acts on behalf of set of host. whenever a router running, A proxy ARP receives an ARP request looking for IP address one of

these host, the router sends an ARP reply announcing its own hardware or physical address. After the router receives the actual IP packet it sends the packet to the appropriate host or router.



Page No.:
Date: / /

* ICMP -

1) The IP protocol has no error reporting or error correcting mechanism.

2) The IP protocol lacks a mechanism for host & management queries. A host sometime ~~a network~~ needs to determine if a router or another host is alive and sometimes a network manager needs information from another host and router the

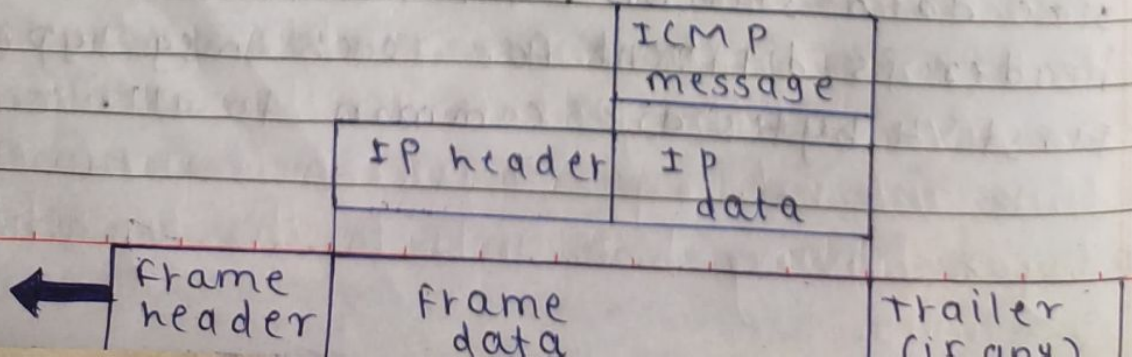
3) The Internet control message protocol (ICMP) has been designed to compensate for the above two deficiencies. It is companion to IP protocol.

* Position of ICMP in the network layer -

1) ICMP itself a network layer protocol. However its message are not passed directly to data link layer as would be expected. Instead the message are first encapsulated inside IP datagrams before going to the lower layer.

* ICMP Encapsulation -

1) The value of the protocol field in the IP datagram is 1 to indicate that the IP data is an ICMP message.



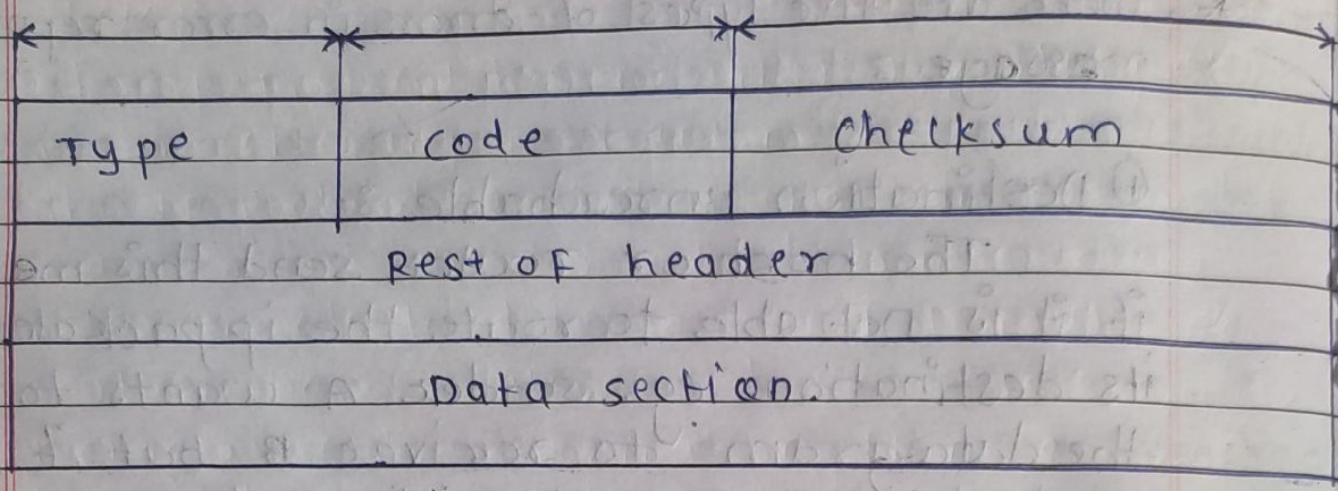
* Messages -

1) ICMP messages divided into broadcast categories error reporting messages and query messages.
2) The error reporting messages report problems that a router or host may encounter when it processes an IP packet.
3) The query messages which occurs in pairs, help a host or a network manager get specific information from a router or another host. Ex - Nodes can discover their neighbours.

Category	Type	Message
Error reporting message	3	Destination unreachable
	4	Source quench
	11	Time exceeded
	12	Parameter problem
	5	Redirection
Query messages	8 or 0	Echo request or reply
	13 or 14	Timestamp request or reply

* Message Format -

1) An ICMP message has 8 bit header and variable size data section. General format of the header is different for each msg type. The first 4 bytes are common to all.



2) ICMP type defines type of the message, code field specify reason for the particular message type. last part is checksum field. The rest of the header specifies for each msg type. Data section in error messages carries information for finding ~~information~~ original packet that had the error.

* Error-reporting message-

1) One of the responsibility of ICMP is to report errors. Although technology has produced reliable trasmission media, errors still exit and must be handled.

2) IP is unreliable protocol means error checking and control are not concern of IP. ICMP was designed in part to compensate for this shortcoming, ICMP does not correct errors it simply reports them.

3) Error correction is left to the higher level protocols error masseges are always sent to the original source because the only information available in the datagram about the route is the source and destination IP addressess. ICMP always reports error masseges to original source.

Date: / /

* There are five types of errors in error reporting message :

① Destination unreachable :-

The host or router send this message if it is not able to route the ip packate to its destination. eg. sender A wants to send the datagram to receiver B but it is not received by B then the intermediate router will discard the datagram and send the destination unreachable message to A.

② Source quench :

Host/ router send this msg if there is congention in the network or the source is sending packates at the higher rate which the router can't handle. eg... if sender A is sending data packets at a high data rate which the router is unable to handle then it will discard the packet and send a source quench message to A to tell it to send the packets at a lower rate. Now After receiving the message A will either stop or slow down sending of the packets.

③ Time Exceeded :

The host or router send this message if, a it decrements the time to live value of the datagram to # zero or destination address. does not ~~re~~ receive all the packets in the specified ~~tim~~ time interval.. eg... a packet is sent from a layer having 1000 units to the layer having 200 units.

then the packet is divided into five fragments if all the fragments don't reach the destination in a set time all fragments are discarded and the time exceeded msg is sent to original source.

④ Parameter problem :-
The host / router sends the message if some parameter is not properly set in the datagram. It is used to indicate errors in the header field of the datagram

⑤ Redirection :-
The host / router sends this msg to update the routing table of the host.
eg.. sender A wants to send the message to receiver B and there is router between them, then A sends the data to router and router sends msg to B. and redirection msg to A. so that A can update its routing table.

* query message -
1) In addition to error reporting ICMP can also diagnose some network problems. This is accomplished through the query message. A group of five different pairs of message designed for this purpose. only two request pairs are used echo request & reply and time-stamp request & reply.

- echo request and reply -

1) Echo request & echo reply messages are designed for diagnostic purpose. Network managers and users utilize this pair of messages to identify network problems.
2) A host or router can send echo-request msg to another host or router. The host or router that receives an echo request msg creates an echo reply msg, and returns it to the original sender.
3) An echo request msg can send by host or router and echo reply msg send by host/router that receives an echo request msg.
4) Echo request & echo reply messages can be used by network managers to check the operation of the IP protocol.
5) Echo request & Echo reply msg can test the reachability of host. this is usually done by invoking ping command.

Type 8: Echo request
Type 0: Echo reply.

Type 8 or 0	Code: 0	checksum
Identifier		sequence number
optional data sent by the request msg; repeated by the reply msg		

- Timestamp request and reply msg -

1) Two machines can use the timestamp request and timestamp reply msg. To determine the round trip time needed for an ip datagram to travel between them.

2) Timestamp request and timestamp reply msg can be used to calculate the round trip time bet" source and destination machine even if their clocks are not synchronized.

3) # sending time = received timestamp - originat timestam

Receiving time = Returned time - transmit timestamp.

Round trip time = sending time + Receiving ti

4) The timestamp request and timestamp reply msg can be used to synchronize two clock in two machines if the exact one way time duration is known.

Timedifference = Received timestamp - (origin timestamp field + one way time duration.)

* Checksum - (see chapter 2nd.)

* Debugging tools -

1) There are several tools that can be used internet for debugging. We can find a host/ router is alive or running. We can trace route of the packet we introduce two tools that use ICMP for debugging - ping and traceroute.

- ping -

1) It stands for Packet internet groper. It is utility that helps one to check if a particular IP address is present or not. Ping works by sending a packet to specified address and waits for reply. It also measures round trip time & reports errors.
2) Also used in checking if computers on local networks are active.

- TraceRoute -

1) It is a utility that traces a packet from your computer to host. And will also shows the no. of steps require to reach their along with time by each step.
2) Traceroute words by sending the packets of data with a low survival time. which specifies how many steps can the packet survive before it is return.
3) If any of the host come by with request timeout it denotes network congestion and reason for slow loading webpages.

Page No.:
Date: / /

* IP -

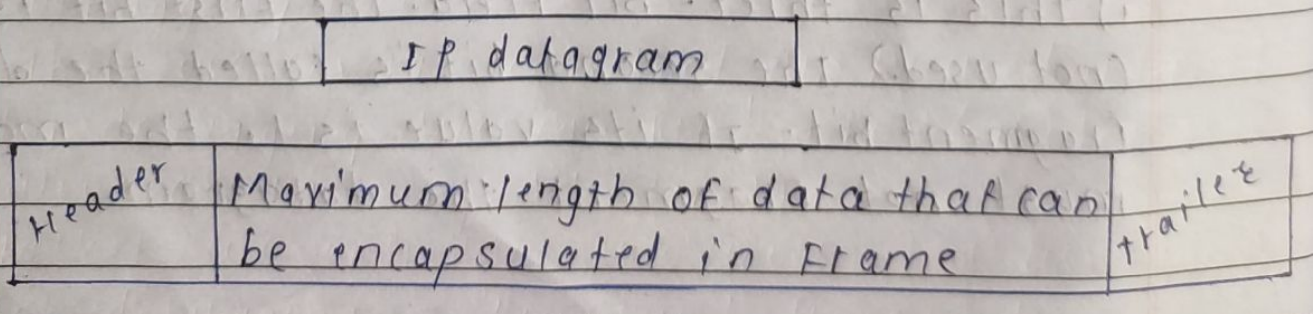
• Fragmentation -

1) Fragmentation is done by the network layer when the maximum size of datagram is greater than maximum size of data that can be held in a Frame. i.e. its maximum Transmission unit the network layer divides the datagram received from the transport layer into fragments so that data flow is not disrupted.

> Maximum Transfer unit (MTU) -

1) A maximum transmission unit also called as MTU, is a term used in networking and operating systems. It defines the largest size of the packet that can be transmitted as a single entity in network connection. The size of MTU dictates amount of data that can be transmitted in bytes over a network.

2) A datagram can be fragmented by source host or any router in the path. The reassembly of datagram is done only by the destination host because each fragment becomes an independent datagram. only data in datagram is fragmented.



Frame.

- Fields Related to Fragmentation-
The fields that are related to fragmentation and reassembly of an IP datagram are the identification, flags and fragmentation offset fields -

➤ Identification-
1) This 16 bit field identifies a datagram originating from the source host. The combination of identification and source IP add. must uniquely define a datagram as it leaves the source host.
2) To guarantee uniqueness, the IP protocol uses a counter to label datagram. When datagram is fragmented, the value in the identification field is copied into all fragment. All fragments have same identification number, which is same as original datagram.
3) Identification number helps the reassembling the datagram. It knows that all fragments having same identificat? value should be assembled into one datagram.

➤ Flags-
1) this is three-bit field. The first bit is reserved (not used.) The second bit is called the do not fragment bit. If its value is 1, the machine must not fragment the datagram.