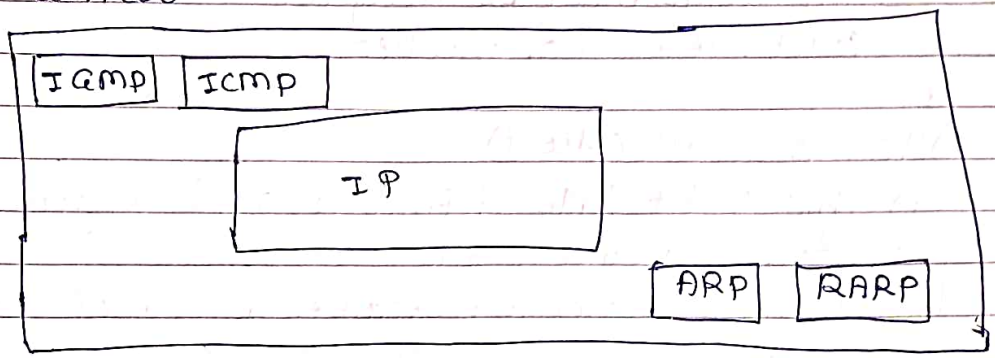
5. Internet Protocol

Page No:
Date:

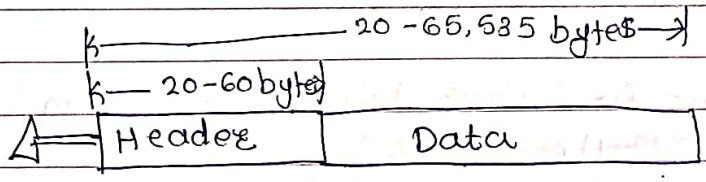
IP Datagram format

i) IP was designed as best effort delivery protocol but it lacks some features such as flow control & error control.



IP datagram

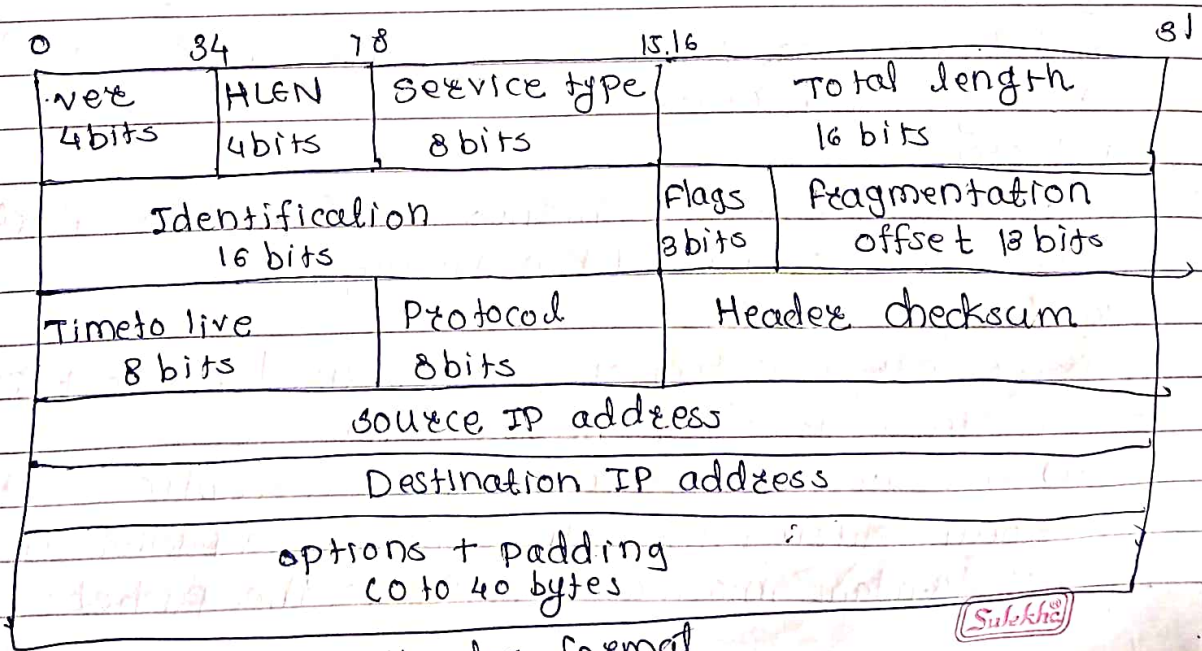
i) Packets in a network layer called datagram



a) IP datagram.

ii) Fig. @ shows IP datagram format, datagram is a variable length packet consisting of two parts header & data.

iii) The header is 20 to 60 bytes in length & contains information essential to routing & delivery.



b. Header format

Sulekha

1) version (VER)

i) 4 bit field defines the version of the IP protocol. currently version is 4

ii) All fields must be interpreted as specified in the fourth version of the protocol.

2) Header length (HLEN)

i) This 4-bit field defines a total length of the datagram header in 4 byte words.
This field is needed because length of the header is variable (bet. 20 & 60 bytes)

ii) when there are no options, the header length is 20 bytes & value of this field is 5

3) Service Type
In the original design of IP header, this field was referred to as type of service, which defined how the datagram should handled.

4) Total length

i) This is 16 bit field that defines total length of IP datagram in bytes.

5) Identification
This field is used in fragmentation

6) Flags
This field is used in fragmentation

7) Fragmentation offset
used in fragmentation

8) Time to live.
A datagram has a limited lifetime in it's travel through an internet.

9) Protocol
8 bit field defines higher level protocol that uses the services of the IP layer.

10) Checksum

i) The error detection method used by most TCP/IP protocols is called the checksum

ii) The checksum protects against corruption that may occur during the transmission of a packet, it is redundant information added to the packet.

11) Source address
i) This 32 bits field defines the IP address of source.
12) Destination address
This 32-bit field defines the IP address of destinatio

Fragmentation & Reassembly

* Fragmentation
i) It is done by the network layer when max. size of datagram is greater than max. size of data that can be held in a frame i.e MTU.
ii) The network layer divides datagram received from transport layer into fragments so that flow is not disrupted.
iii) Source side does not require fragmentation due to wise segmentation by transport layer i.e instead of doing segmentation at transport layer & fragment at the nlw layer, the transport layer looks at datagram data limit & frame data limit & does segmentation in such way that resulting data can easily fit in a frame without need of fragmn
iv) Receiver identifies frame with identification (16 bits) field in the IP header, each fragment of frame has same identification number.
v) Receiver identifies sequence of frames using fragmen offset (13 bits) field in the IP header.
vi) overhead at nlw layer is present due to the extra header introduced due to fragmn.

Fields in IP header of fragmentation
i) Identification (16 bits)
use to identify fragments of the same frame.
ii) Fragment offset (13 bits)
use to identify sequence of fragments in the frame it generally indicates no. of data bytes preceding or ahead of the fragment.
iii) More fragments (MF = 1 bit.)
Tells if more fragments are ahead of this fragment i.e if MF = 1 more fragment are ahead of this fragment & if MF = 0 it is last fragment

iv) Don't fragment (DF = 1 bit)
If we don't want the packet to be fragmented then DF is set i.e DF = 1

Reassembly of Fragments.

1) It takes place only at the destination & not at routers since packets take an independent path so all may not meet at a router & hence need of fragmentation may arise again.

DATE / /

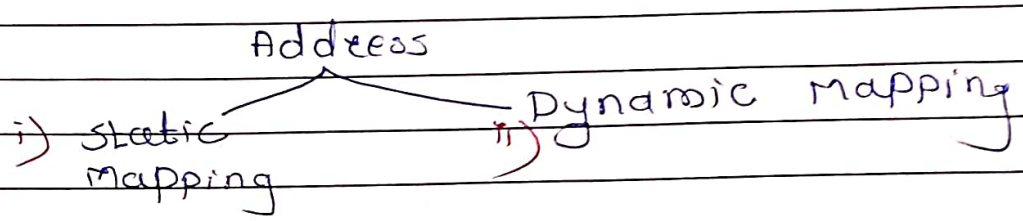
Address Mapping

→ i) The logical addresses in the TCP/IP protocol suite are called IP addresses & are 32 bit long.

ii) Physical address is local address, it should be unique locally ~~implemented in hardware~~.

It is called physical address because it usually implemented in hlw.

e.g - physical addresses are 48-bit MAC addresses in Ethernet protocol.



i) Static Mapping

a) It means creating table that associates logical address with physical address.

b) This table is stored in each machine on the network, each m/c that knows IP address of another machine but not it's physical address can look it up in table.

But some possibilities to change physical add:

i) machine could change it's NIC

ii) In some LANs such as local Talke, the physical address change every time the computer is turned on.

iii) Mobile computer can move from on physical n/w to another

ii) Dynamic Mapping

- In dynamic mapping each time machine knows the logical address of another machine so it can use protocol to find the physical address

- Two protocols are designed to perform dynamic mapping

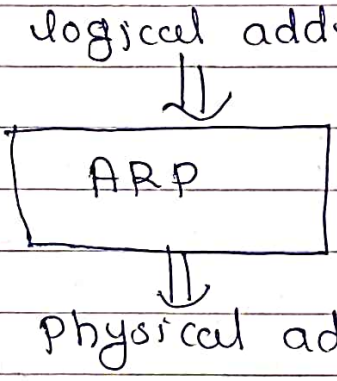
i) ARP — maps logical to physical

ii) RARP — maps physical to logical.

ARP (Address Resolution Protocol)

(mapping logical to physical Address)

i) ARP finds the physical address also known as media access control (MAC) address of a host from its known IP address.



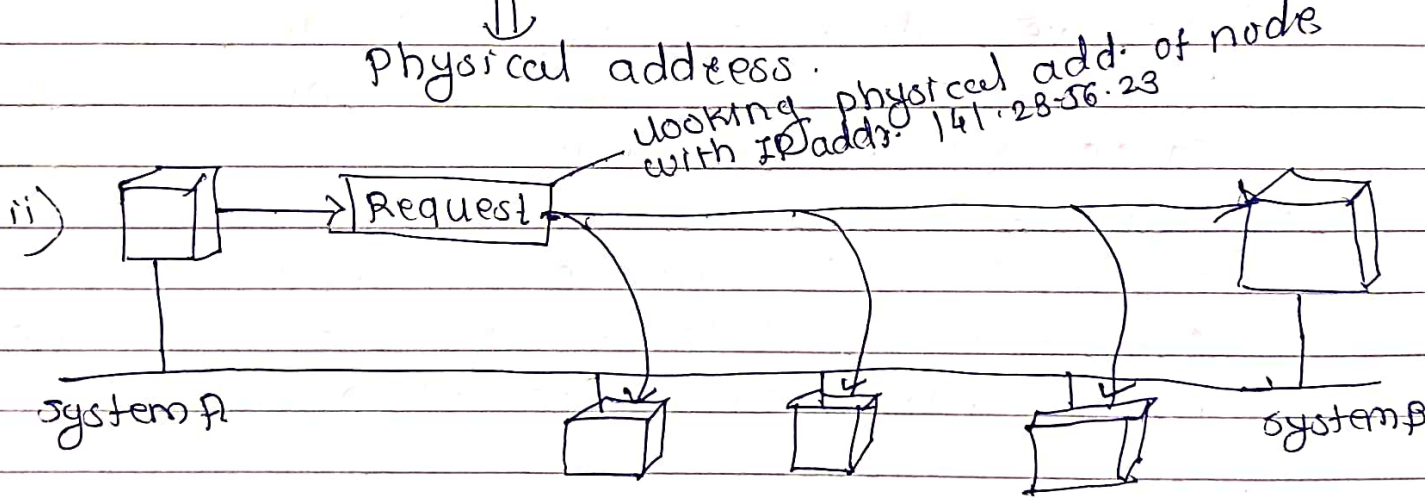


fig (a) ARP request is broadcast

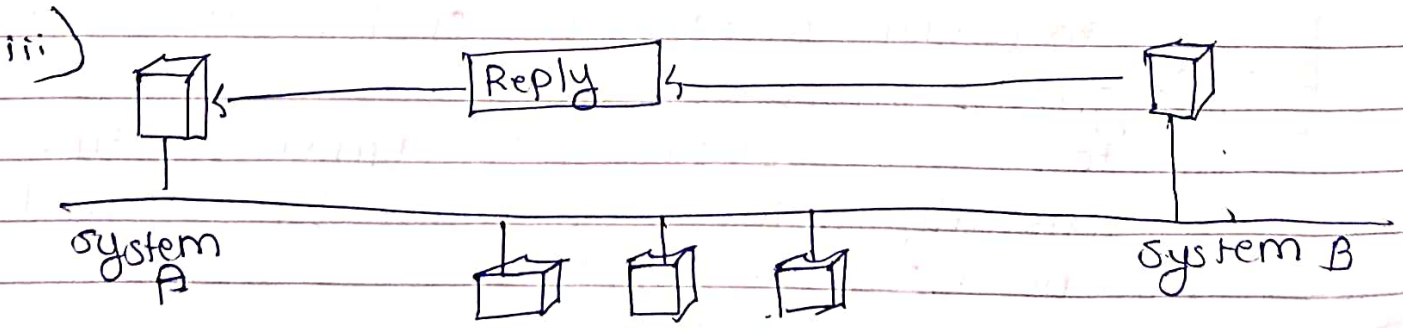


fig (b) ARP reply is unicast

Page No :
Date :

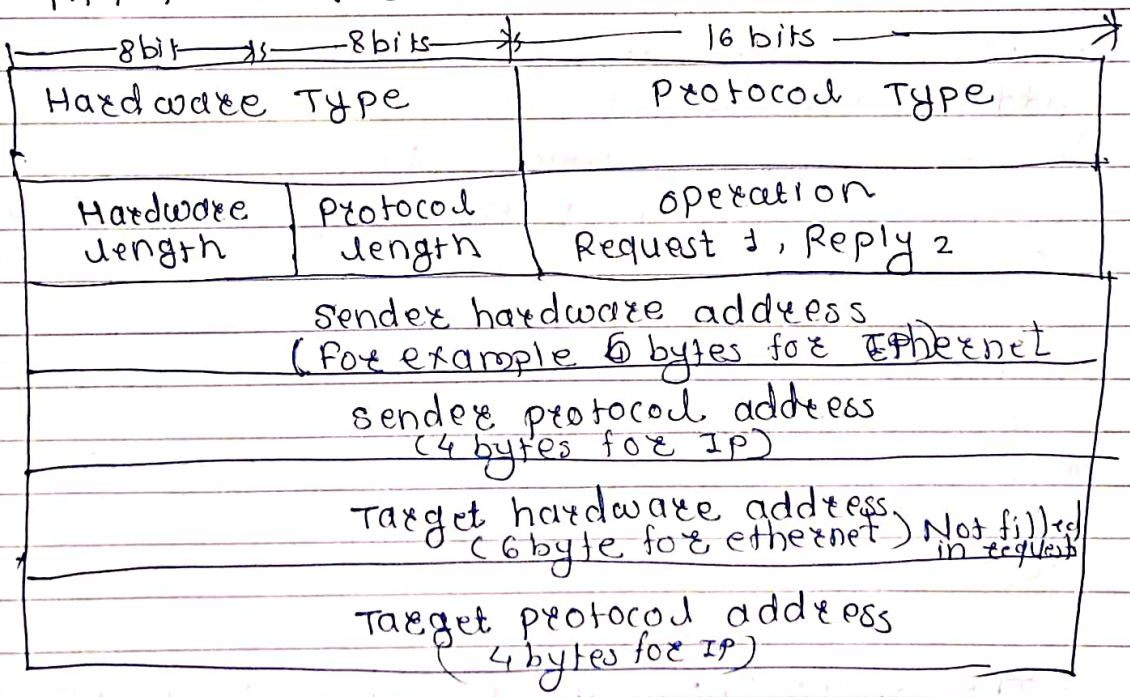
Following steps are involved in logical to physical mapping

1) The host or router sends an ARP query packet. the arp query packet includes the physical & IP address of the sender & the IP address of the receiver. As the sender does not know physical add. of the receiver, ARP query is broadcast over the network.

2) Every host or router on the network receives & processes the ARP query packet, but only the intended recipient recognizes its IP address & sends back ARP response packet.

3) The ARP response packet contains the recipients IP & physical addresses, the ARP response packet is unicast to the inquirer by using physical address received in the query packet.

ARP Packet format.



1) Hardware type

i) 16 bit field defining the type of network on which ARP is running.

ii) Each LAN has assigned an integer based on its type. e.g. ethernet is given type 1.

2) Protocol type

This is a 16-bit field defining protocol

e.g value of this field for the IPv4 protocol is 080016, ARP can be used with any higher level Protocol.

3) Hardware length
This is an 8 bit field defining length of physical address in bytes, ethernet value is 6

4) Protocol length
i) This is an 8 bit field defining the length of the logical address in bytes.
ii) IPv4 protocol value is 4,

5) Operation
i) This is 16 bit field defining type of packet
ii) Two packet types are defined :
ARP request (1) &
ARP reply (2)

6) sender hardware address.
i) This is variable length field defining physical ad. of the of the sender.
ii) For IP protocol this field is 4 bytes long.
7) Target hardware address.
i) This is variable length field defining physical address of the target
ii) e.g → ethernet, this field is 6 byte long.
iii) For ARP request msg, this field is all 0s because sender doesn't know the physical adde. of target

8) Target protocol address.
i) This is a variable length field defining the logical address of the target.
ii) For IPV4 protocol, this field is 4 bytes long.

ARP operation

1) The sender knows the IP address of the target, we
2) IP asks ARP to create an ARP request message, filling in the sender physical address, the sender IP address & target IP address, the target physical address field is filled with 0s
3) The message is passed to the data link layer where it is encapsulated in a frame by using the physical address of the sender as source address & physical broad cast address as the destination address.

4) Every host receives the frame, becoz frame contains a broadcast destination addr., all stn remove msg & pass it to ARP, all machines except one targeted drop packet, target machine recognizes it's IP address.
5) The target machine replies with an ARP reply msg that contains it's physical addr. the msg is unicast
6) The sender receives reply msg. It now knows the physical addr. of the target machine.
7) The IP datagram, which carries data for the target machine, is now encapsulated in a frame & is unicast to the dest.

RARP

i) Reverse address Resolution Protocol finds the logical address for machine that knows only it's physical address.
ii) To create an IP datagram, host needs to know it's own IP address.
iii) The IP addr. of machine is usually read from it's configuration, file stored on a disk file.
iv) However, diskless machine is booted from Rom which has min booting info.

RARP operation

i) A RARP request is created & broadcast on the local network.
ii) Another machine on the local nw that knows all the IP addresses will respond with RARP reply.
iii) The requesting machine must be running RARP client program, the responding machine must be running a RARP server program.

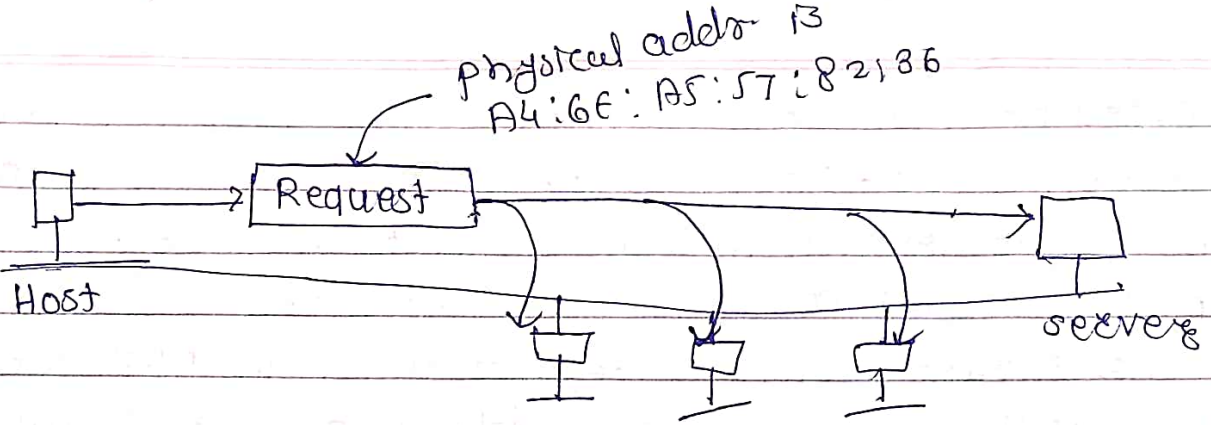
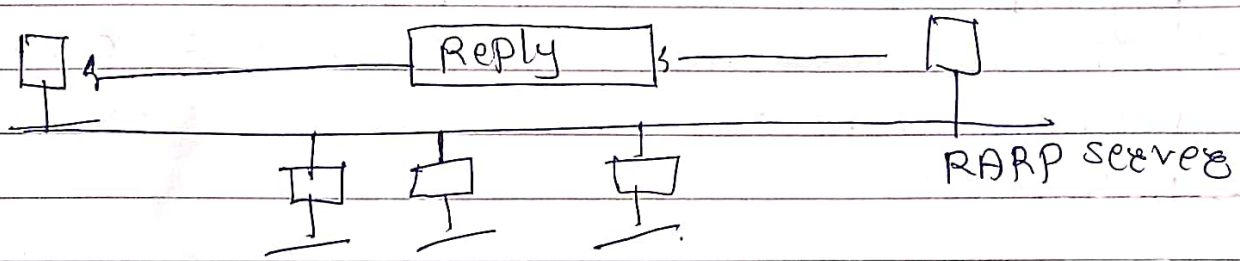


fig ⓐ RARP request is broadcast



* Proxy ARP

i) A proxy ARP is an ARP that acts on behalf of set of hosts, whenever 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 it's own hardware addr. after the router receives the actual IP packet, it sends the packet to the appropriate host/router

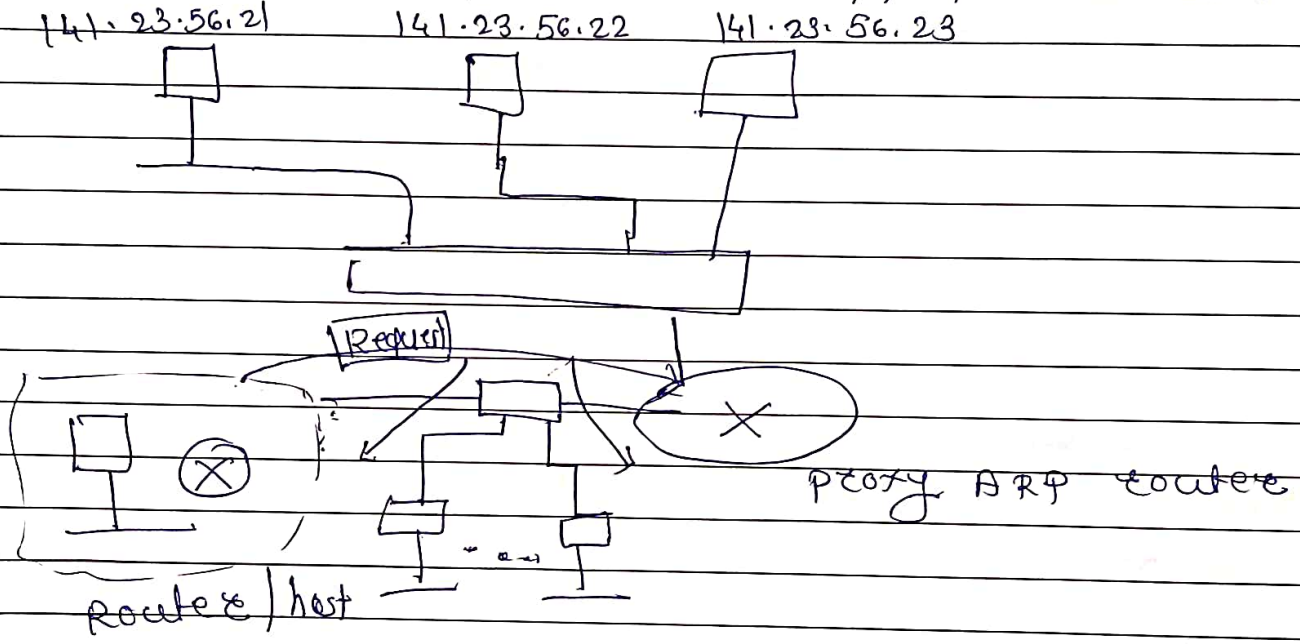


fig. Proxy ARP

i) Admin may need to create subnet without changing the whole system to recognize subnetted addresses. solution is Proxy ARP.

ii) Pro Router acts on behalf of all of the hosts installed on the subnet, when it receives an ARP request with target IP address that matches the address of one of it's proteges, it sends an ARP reply & announces it's hlw address as the target hlw address, when router receives the IP packet, it sends the packet to the appropriate host.

ICMP

i) IP provides unreliable & connectionless datagram delivery. IP protocol has two deficiencies : lack of error control & lack of assistance mechanism.

ii) It has no error reporting or error correcting mechanism.

iii) ICMP has been designed to compensate for above two deficiencies. It is companion to the IP protocol.

Types of messages.

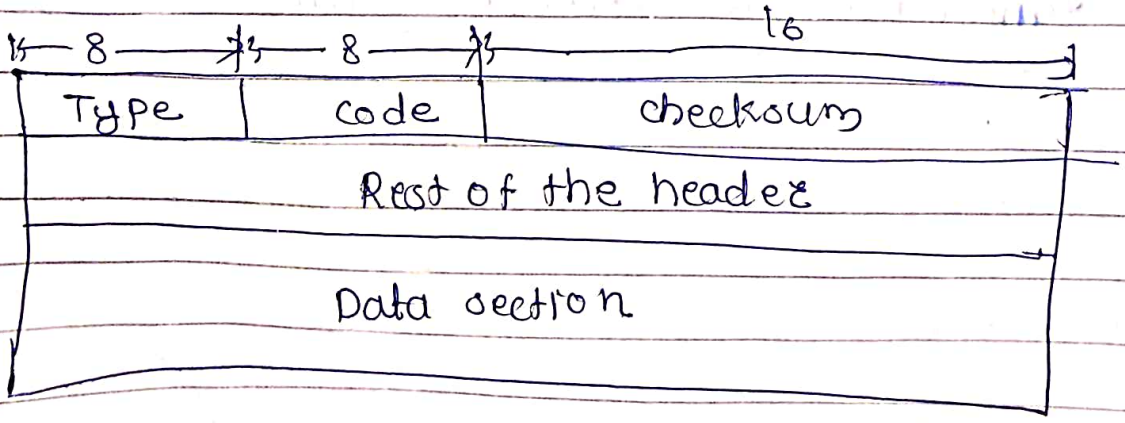
ICMP are divided into two parts

i) Error reporting msg → it report problems

ii) Query msg.

msg format

ICMP msg has an 8 byte header & variable size data section



3) Hardware length
This is an 8 bit field defining length of physical address in bytes, ethernet value is 6

4) Protocol length
i) This is an 8 bit field defining the length of the logical address in bytes.
ii) IPv4 protocol value is 4

5) Operation
i) This is 16 bit field defining type of packet
ii) Two packet types are defined
ARP request (1) &
ARP reply (2)

6) sender hardware address.
i) This is variable length field defining physical add of the of the sender.
ii) For IP protocol this field is 4 bytes long.

7) Target hardware address.
i) This is variable length field defining physical address of the target
ii) e.g → ethernet, this field is 6 byte long.
iii) For ARP request msg, this field is all 0s because sender doesn't know the physical adde. of target

8) Target protocol address.
i) This is a variable length field defining the logical address of the target.
ii) For IPV4 protocol, this field is 4 bytes long.

ARP operation

1) The sender knows the IP address of the target, we
2) IP asks ARP to create an ARP request message, filling in the sender physical address, the sender IP address & target IP address, the target physical address field is filled with 0s
3) The message is passed to the data link layer where it is encapsulated in a frame by using the physical address of the sender as source address & physical broad cast address as the destination address.

i) The 1st field ICMP type defines type of msg.
ii) code field specifies reason for the particular msg type
iii) checksum field used for securing ICMP header
iv) The rest of the header is specific for each msg type
v) The data section in error messages carries info. for finding original packet that had the error.
vi) ICMP query msg. the data section carries extra info. based on type of query.

Error Reporting Messages

i) One of the main responsibilities of ICMP is to report errors.
ii) It doesnot correct errors, it simply reports them
iii) Error correction is left to higher level protocols

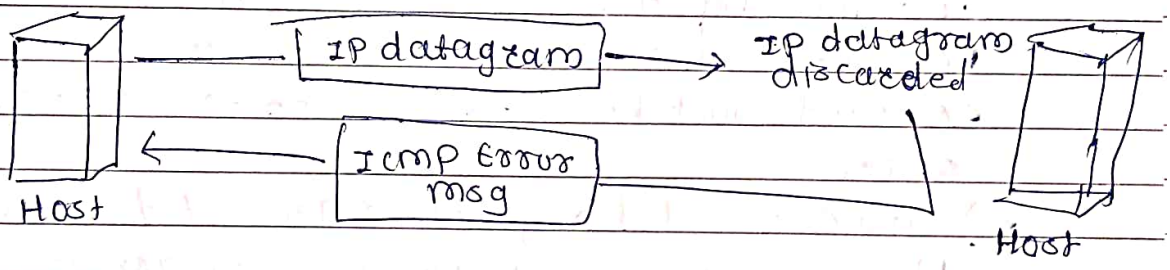
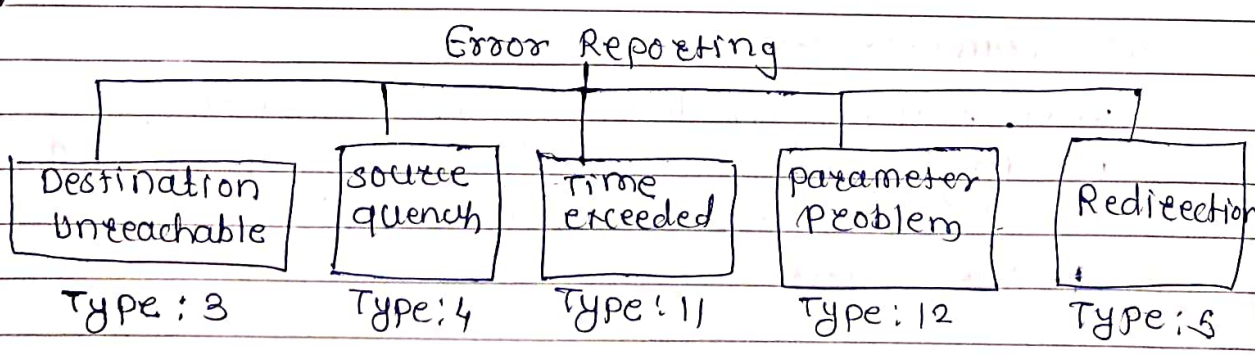


fig. ICMP error Reporting msg.



1) Destination Unreachable
i) when router cannot route datagram, the datagram is discarded & router sends destination unreachable message back to the source host that initiated the datagram.

2) Source quench:

i) The source quench msg in ICMP was designed to add kind of flow control to the IP.

ii) when routers discards datagram due to congestion, it sends source quench msg. to the sender of datagram. The msg. has two purposes

a) First it informs source that datagram has been discarded

b) second, it warns the source that there is congestion somewhere in path & that source should slow down the sending process.

3) Time exceeded

i) Each datagram contain Time to live field that controls this situation, when TTL reaches 0 after decrementing, the routers discards the datagram. however when the datagram is discarded, a time exceeded must be sent by router to the original source.

ii) Time exceeded msg is also generated when not all fragments that make up a msg arrive at the dest. host within certain time limit

4) Parameter problem

when destination discovers an ambiguous or missing value in any field of the datagram, it discards the datagram & sends parameter problems back to the source.

5) Redirection

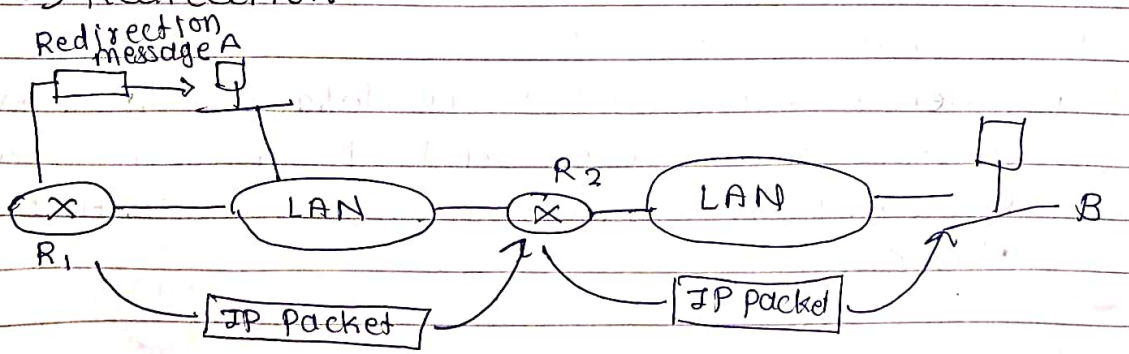
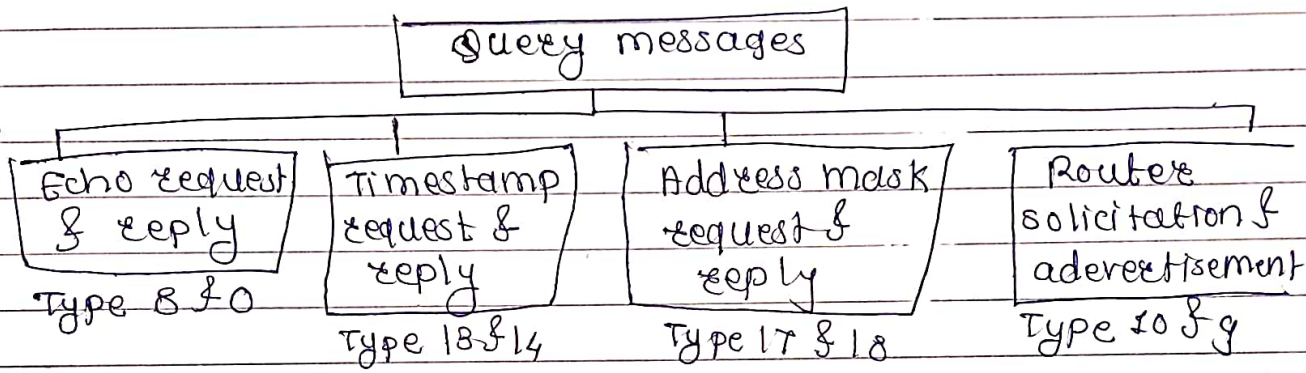
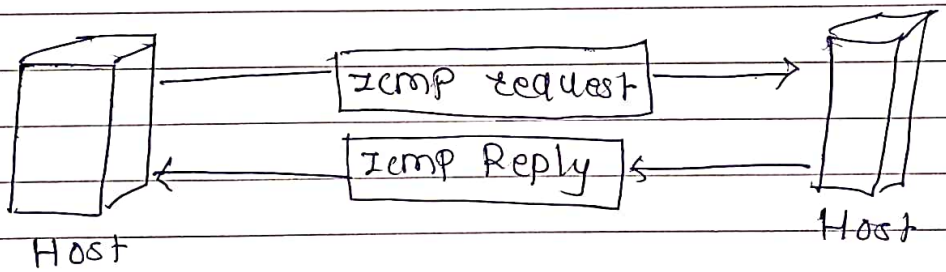


fig. Redirection concept.

i) Router R2 is obviously the most efficient routing choice but host A did not choose Router R2. The datagram goes to R1 instead.
ii) Router R1 after consulting it's table, finds that packet should have done to R2
iii) It sends packet to R2 & at the same time, sends a redirection msg to host A
iv) Host A's routing table can now be updated

(II) ICMP Query messages

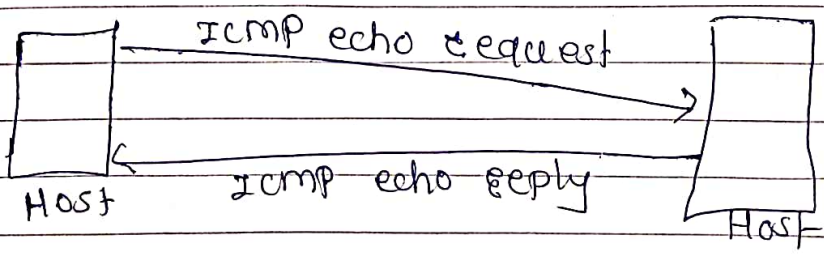




frg. ICMP query message

1) Echo request & Reply

i) It is designed for diagnostic purposes
ii) The combination of that msg determines whether two systems can communicate with each other.
iii) It confirms that immediate router are receiving, processing & forwarding IP datagrams



Date :

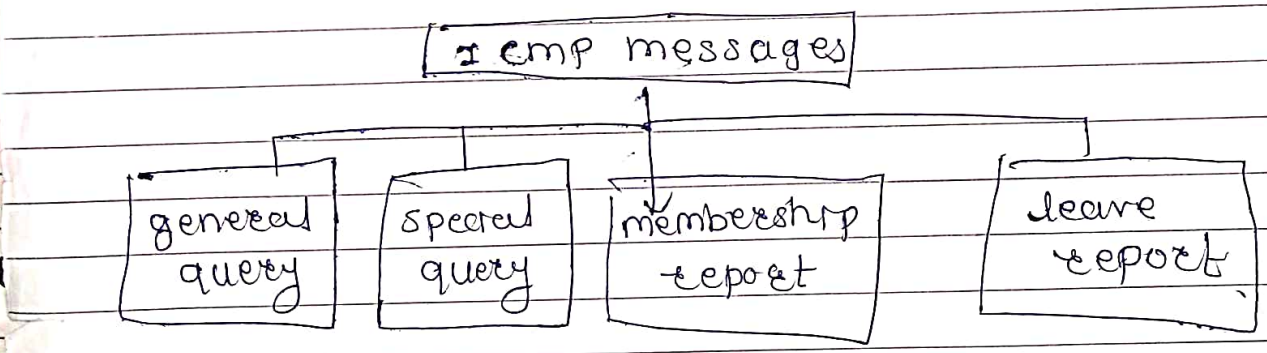
IGMP (Internet Group Membership protocol)

i) IGMP is basically companion of IP
ii) It not multicasting routing protocol but it is protocol that manages the group membership
iii) This protocol is used in streaming, video, gaming & web conferencing tools.

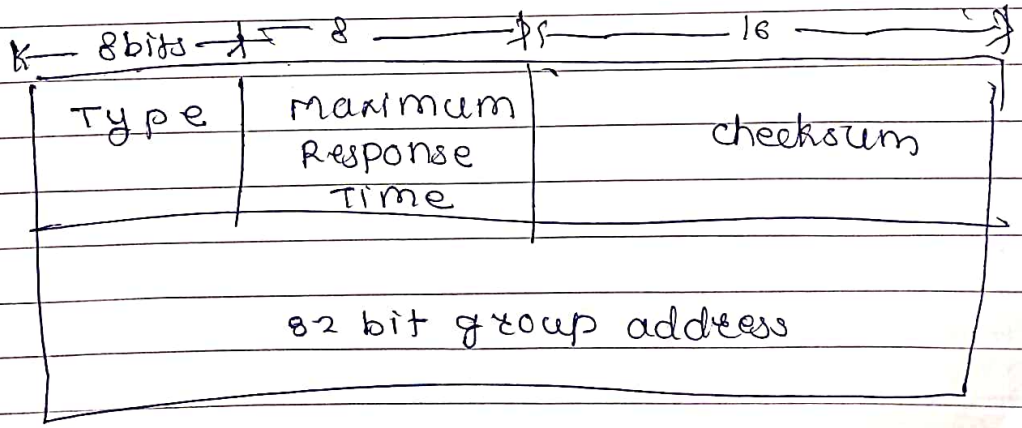
IGMP messages

i) There are two versions of IGMP
IGMPv1 & IGMPv2
ii) The version IGMPv2 has 3 types of msg
a) query
b) membership report
c) Leave report

iii) There are two types of query msg
a) general
b) special



* message format



TEJ MY BRAIN
DATE / /

ICMP Message

ICMPv3 has two types of msg:

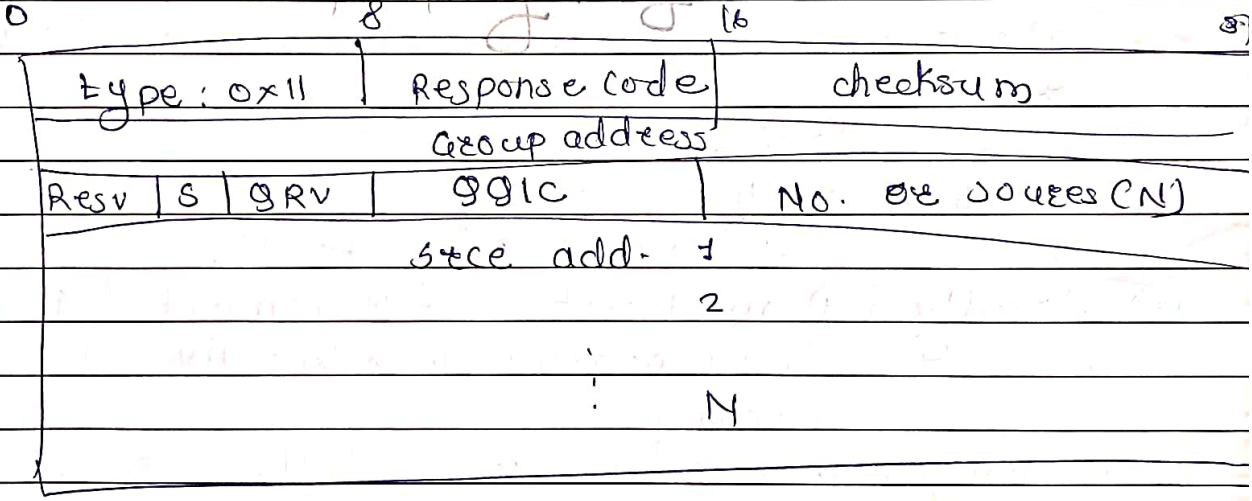
- membership query
- membership report

ICMP

- membership report

General
Group specific
Group & source specific

Membership query Msg format



1) Type → 8 bit, defines type of msg
   - value is 0x11 for membership query msg
2) Max. Response code → 8 bit
   define response time of recipient of query
3) Checksum → 16 bit
   Holding checksum
4) Group Address → 32 bit is set to 0 in general query msg
   set to IP multicast being queered when sending group specific / group & source specific query msg

Resv → 4 bit
reserved for future & it is not used

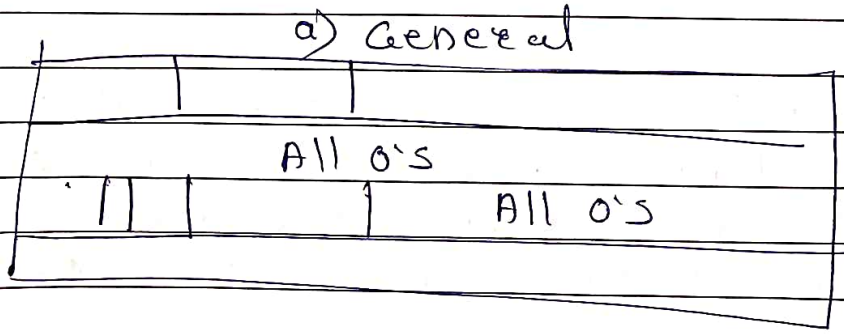
S → 1 bit supress flag
set to 1 → receiver of the query msg should suppress the normal timer updates

QRV → 3 bit is called querier's robustness variable. It is used to monitor the robustness in n/w

QQIC → 8 bit. is called querier's query interval code.
- used to calculate querier's query interval

N → 16 bit,
defines 32 bit unicast source addresses attached to the query
∴ 0 = general query
Non zero → g & g,

source Address → multiple 32 bit field list the N source address.

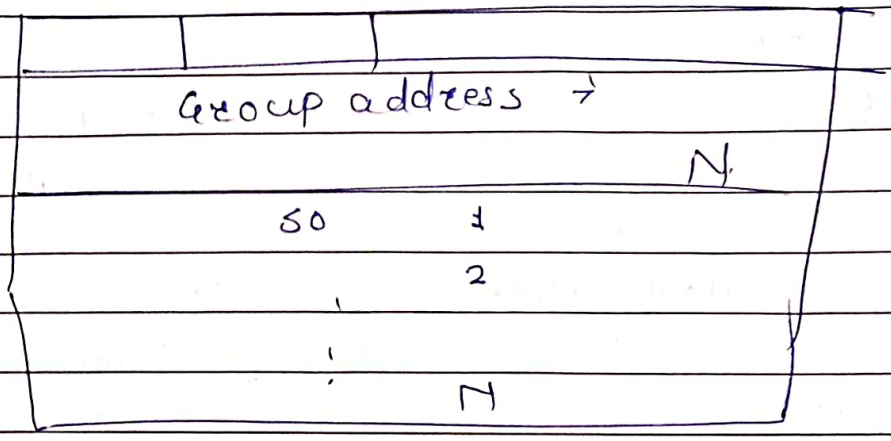


b) Group specific

Group address es
All 0'

DATE / /

c) Group & source specific



a) General

The queries router probes each neighbor to report the whole list of it's group membership.

b) Group specific

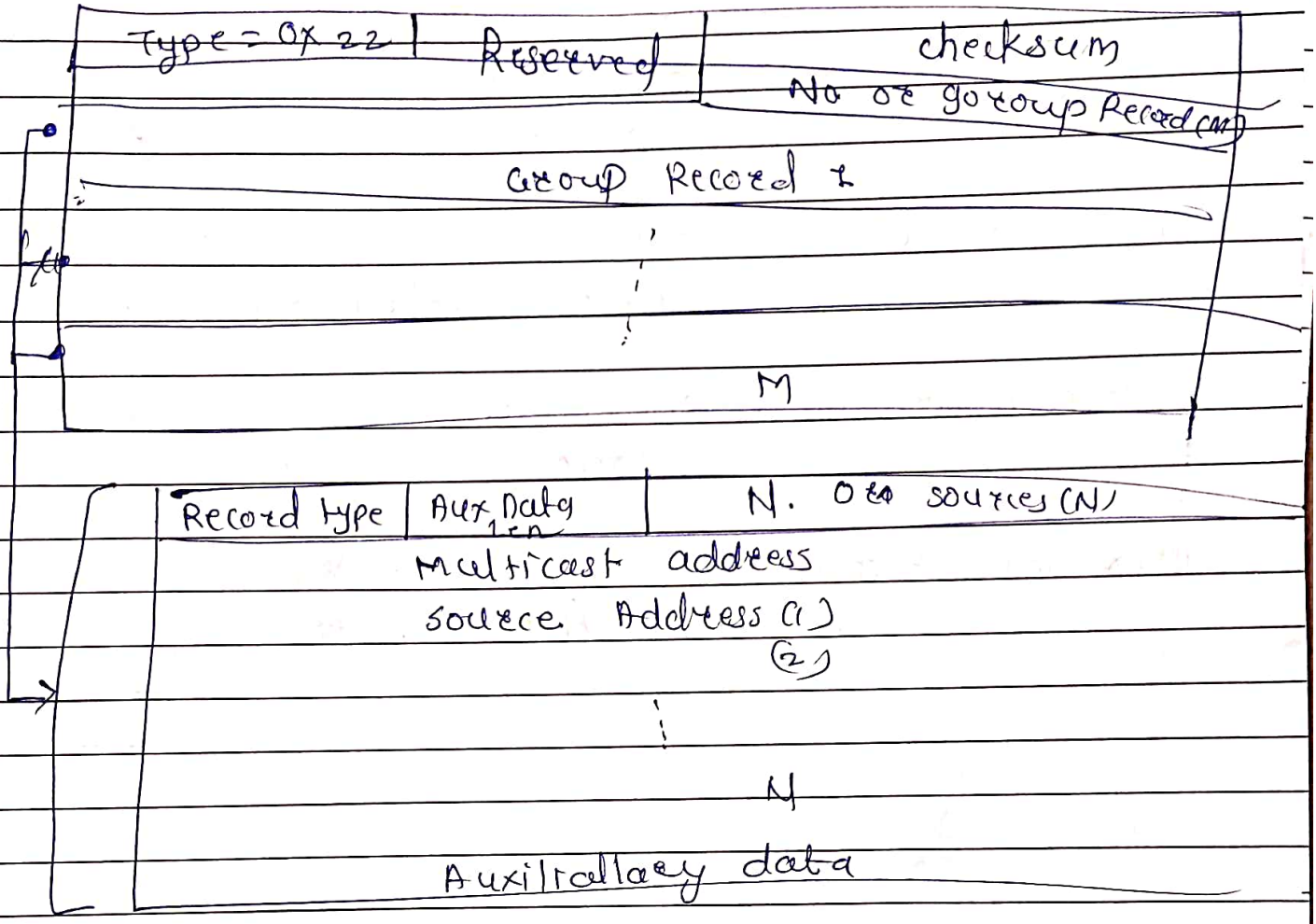
queries router probes each neighbor to report if it is still interested in specific multicast group.

- multicast group address is defined as x.z.z.t in group address field of the query

c) Group & source specific

queries router probes each neighbor to report if it is still in specific multicast group x.y.z.t coming from any of N sources whose unicast addresses are defined in this packet.

Membership



Type → Define type

checksum → Error detection

No. of Group Records (M) – 16 bit, defines no. of group records carried by packet

No. of Group Record

supplement collected data from external src

TEJ MY BRAIN
DATE / /

Aux Data len → 8 bit defines length of auxiliary data included in each group record

0 = No auxiliary

Non zero → length of data in words 32 bits

N. → 16 bit defines no. of 32 bit Multicast source Addresses attached to the report

Source Addresses → Multiple 32 bit field list the M source addresses.

Aux data → contains any auxiliary data that maybe included in report msg.