Network Layer in the Internet → The principals that drove design of network layer in the Internet are discussed in RFC 1958.

- Priciples →

(1) Make sure it works

(2) keep it simple

(3) Make clear choices

(4) exploit modularity

(5) Expect hetrogenity

(6) Avoid static options and parameters

(7) Look for a good design

(8) Restrict when sending and tolerent when receiving

(9) Think about scalability

(10) Consider performance and cost.

• NOTES AREN'T Complete

[As course is taught on slides after a point]

[And some parts are missing anyways]

- Problems with Computer Networks

① Communication problem

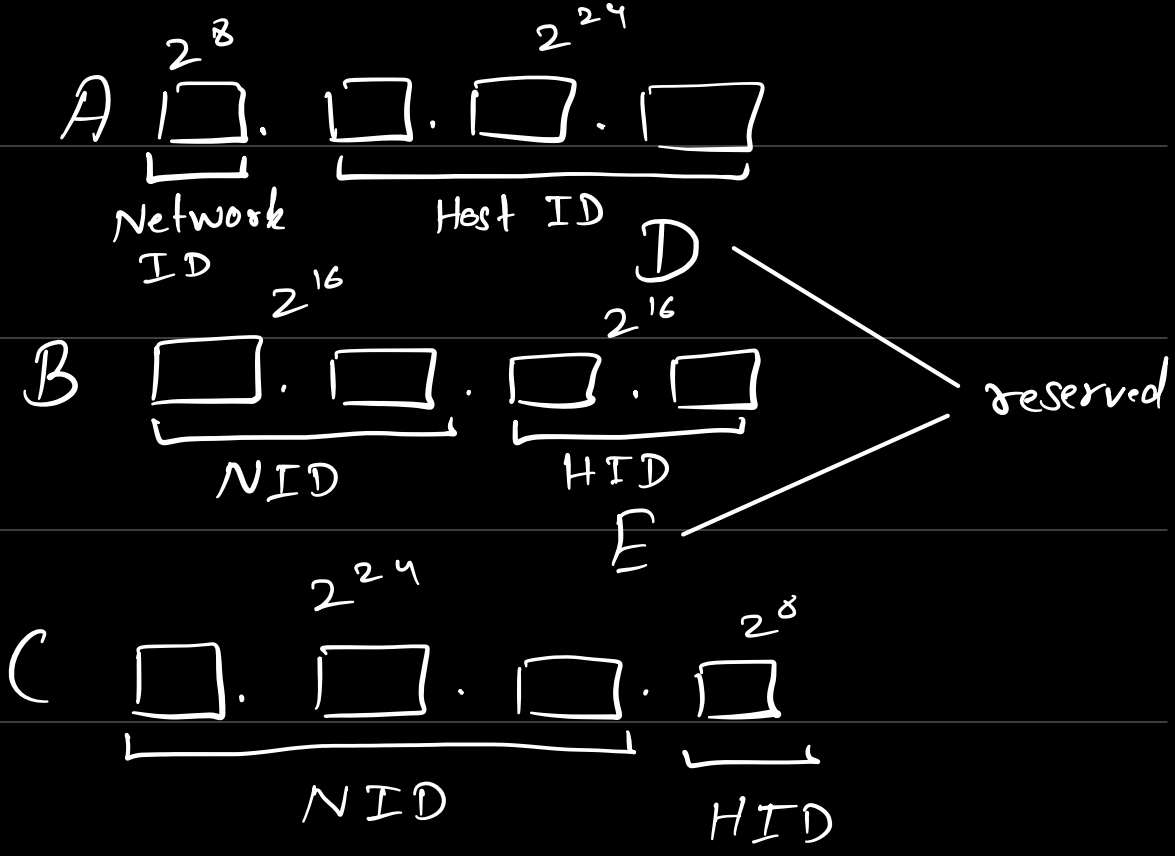
② Connection problem

③ Identification problem

- The communication problems can be avoided by the use of protocols.
- Connection problems can be avoided by the use of standardized devices in the network.
- Identification problem can be solved in three ways → ① Identify the network (logical addressing)
② Identify the host in the network → (physical addressing)
③ Identify process within the host. → (Service point addressing)

- Logical Addressing → (IPv4) → 32 bits.

5 classes are there



- Class A → It ranges from 1-126.

  The first bit is always zero and hence $(2^7 - 2)$ Networks

  Hosts ⇒ $2^{24} - 2$

- Class B → It ranges from 128-191

  First two bits 10 and fixed

- Class C → It ranges from 192 - 223 and first three bits are 110 and fixed.

- Class D → Ranges from 224 to 239 and first 4 bits are 1110 and fixed.

- Class E → Ranges from 240 - 255 and 1st 4 bits are 1111 and fixed.

	N/w		Host
A	$2^7 - 2$	×	$2^{24} - 2$
B	2^{14}	×	$2^{16} - 2$
C	2^{21}	×	$2^8 - 2$

- Total IP adresses available

→

• Adress Blocks → In classless adressing when an entity small or large needs to be connected to the internet It is granted a range of adresses.

The size of the block varies based on nature and size of entity.

• Restrictions → ① The adress in a block must be contigious.

② The no. of adresses in a block must be a power of 2.

③ The first adress must be evenly divisible by no. of addresses.

Block

205.16.37.32
205.16.37.33
⋮
205.16.37.47

Cond^n 1 → satisfied

n 2 → n

n 3 → n

205 . 16 . 32 . 37

$256^3, 256^2, 256^1, 256^0$

$= \frac{3440387360}{16} = 215024210$

- **MASK** → A mask is a 32 bit number in which the n leftmost bits are 1s and 32-n rightmost bits are zeros. In classless adressing the mask for a block can take any value from 0-32.

x . y . z . t / n ← mask.

- **First Adress** → It is found by setting 32-n rightmost bits in binary notation of adress to zeros.

- **Last Adress** → It is found by setting

32-n rightmost bits in binary notation of address to 1.

- **No. of addresses** → It is calculated by the formula 2^{32-n}.

Ex. A block of addresses is granted to a small organization. One of the addresses is 205.16.37.39/28 = n
What is the 1st Address of block.

11001101 00010000 00100101 01100111
0000

n = 28

32 − n = 4 ⇒ so last 4 bits becomes 0

first adress

11001101 00010000 00100101 00100111

1st Add: 205.16.37.32

Last : 205.16.37.47

no. of adresses = 16. (2^n)

- Alter Method

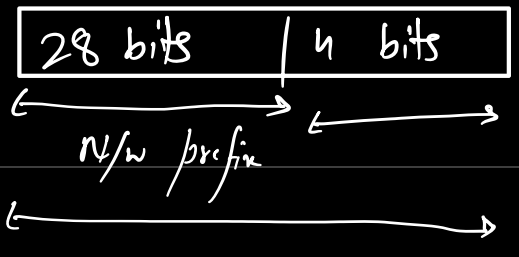
1st Add → And operation b/w adress and mask.

Last Add → OR operation b/w adress and complement of mask.

No. of adress → ① Complement the mask
② Interpret as a decimal no. and add 1 to it.

- **Network Adresses** → The first adress in a block adress is always adress of the network.

- **Two - Level Hierarchy** → In this there isn't any concept of subnetting. The n- left most bits of x.y.z.t/n defines the Network. It is also known as prefix. Similarly 32-n rightmost bit defines the host. It is known as Suffix of the network.

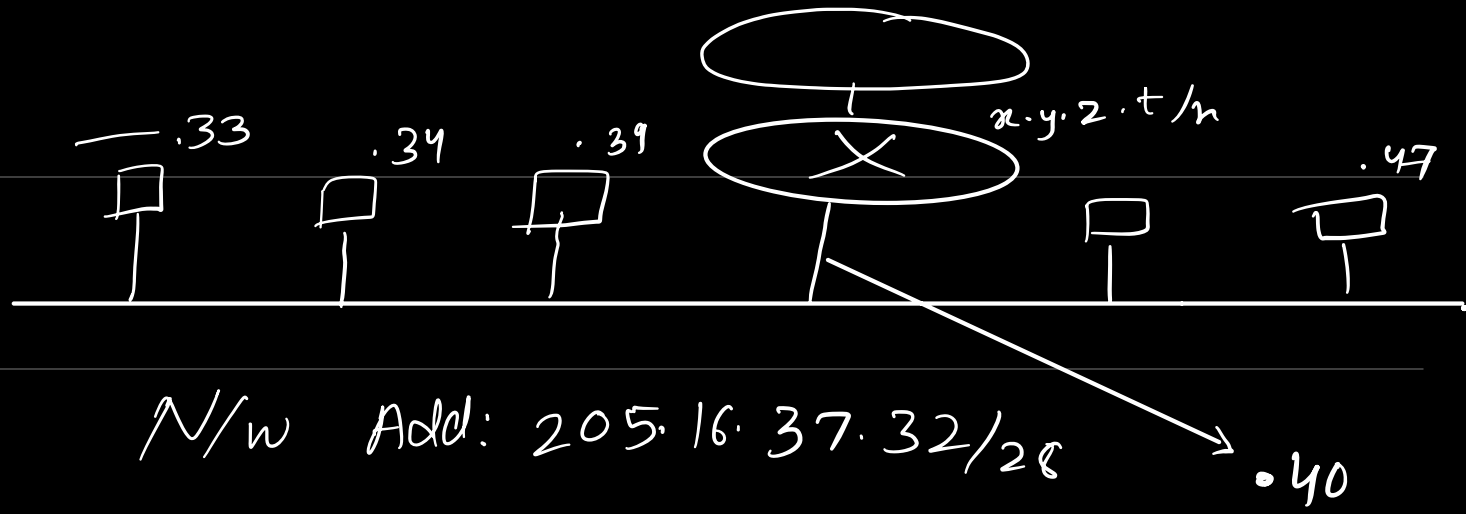


- **Three Level Hierarchy** → It utilizes the concept of subnetting.

- An organization that is granted a large block of adresses may want to create clusters of network and divide those networks in diff. Cluster called subnet.

All messages are sent to the routers adress that connects the organization to rest of the internet.

- The routers routes the messages to appropriate subnets.
- The organization needs to create small sub-blocks of adresses each assigned with specific subnets.



N/w Add: 205.16.37.32/28

- Each organization has its own mask and each subnet has its own.

Ex. Suppose an organization is given the block 17.12.14.0/26 which contains 64 adresses. The org. has 3 offices and needs to divide adresses into 3 sub blocks of 32, 16 and 16 adresses.

- New Masks:

$$2^{32-n_1} = 32 \Rightarrow n_1 = 27$$

$2^{32-n_2} = 16 \Rightarrow n_2 = 28$

$n_3 = 28$

Subnet 1 : → 17 . 12 . 14 . 29 / 27 → leftmost

Host : 00011001 00001100 00001110

00011101

Mask (27): 11111111 11111111 11111111 11100000

Subnet : 17 . 12 . 14 . 0

Subnet 2 : 17 . 12 . 14 . 45 / 28

Host : 00010001 00001100 00001110

Mask : 11111111 11111111 11111111 11110000

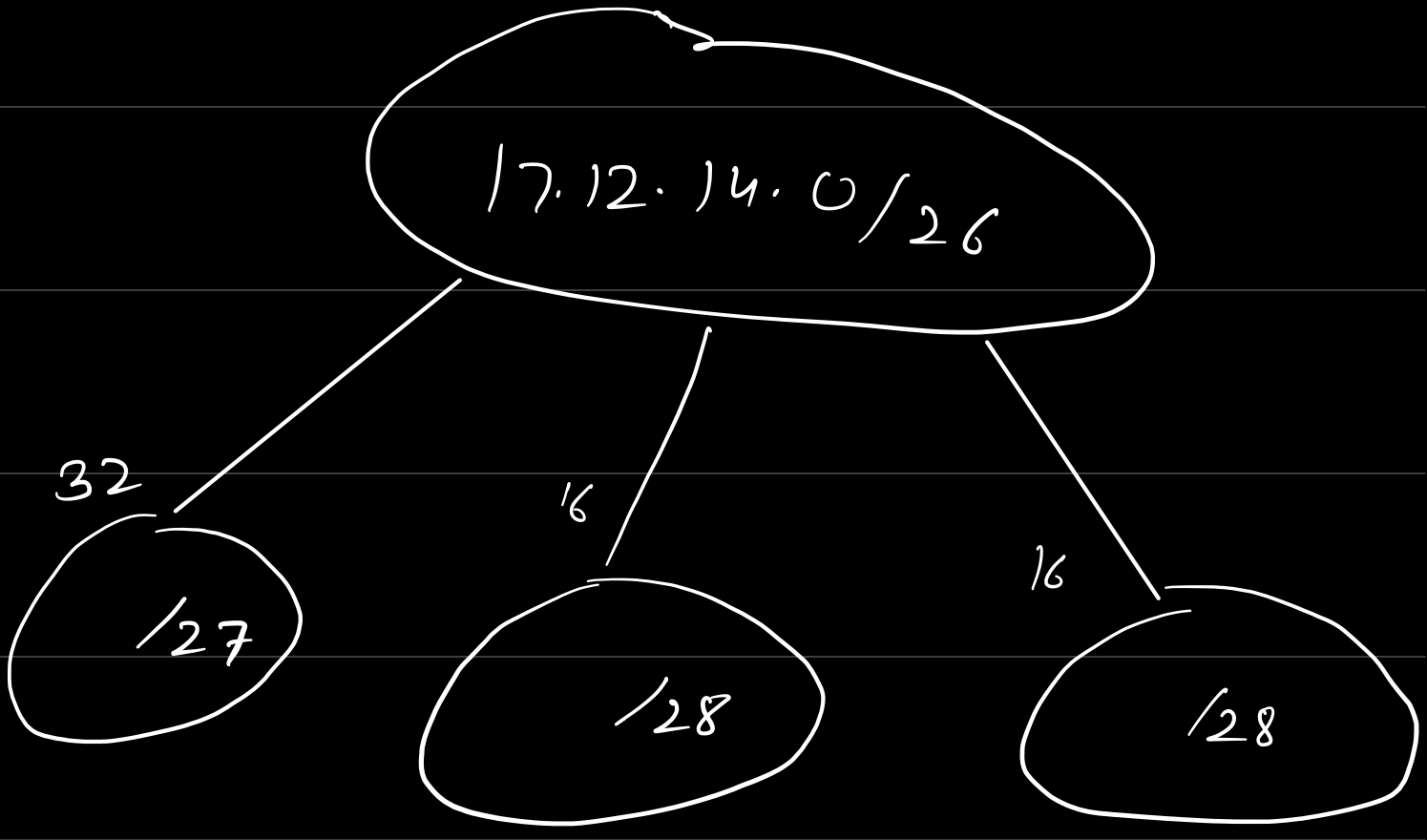
Subnet : 17 . 12 . 14 . 32

Subnet 3: 17.12.14.50 /28

Host : 00010001 00001100 00001110

Mask : 11111111 11111111 11111111 1111 0000

Subnet : 17.12.14.48



- NOTE → Apply the mask of network of

the whole organization to any of the adresses to obtain the network Adress.

ex. 17.12.14.51/26

Host: 00010001 00001100 00001110

Mask: 11111111 11111111 11111111 11000000

Host & Mask = 17.12.14.0

- Adress Allocation: ICANN

↓

Internet corporation for assigned names and Adresses.

ex. An ISP is granted a block of adresses starting with 190.100.0.0/16

The ISP needs to distribute these adresses to three groups of customer

11 0011

128 64 32 16 8 4 2 1

00 110011

as follows →

1. 1st grp has 64 customers each need 256 adresses
2. 2nd group has 128 customer each needing 128 adresses.
3. 3rd 128 ——— 64 adresses.

Design the sub blocks and find out how many adresses are still available after allocation

Group 1:

Adresses → 256

No. of bits to define a host

$= \log_2 256 = 8$

Prefix length = 32 − 8

= 24

1St: 190.100.0.0/24 to 190.100.0.255/24

2ND: 190.100.1.0/24 to 190.100.1.255/24

:

:

63th 190.100.63.0/24 to 190.100.63.255/24

Group 2: 128 adresses

$\log_2 128 = 7$

Prefix → 32 − 7 = 25

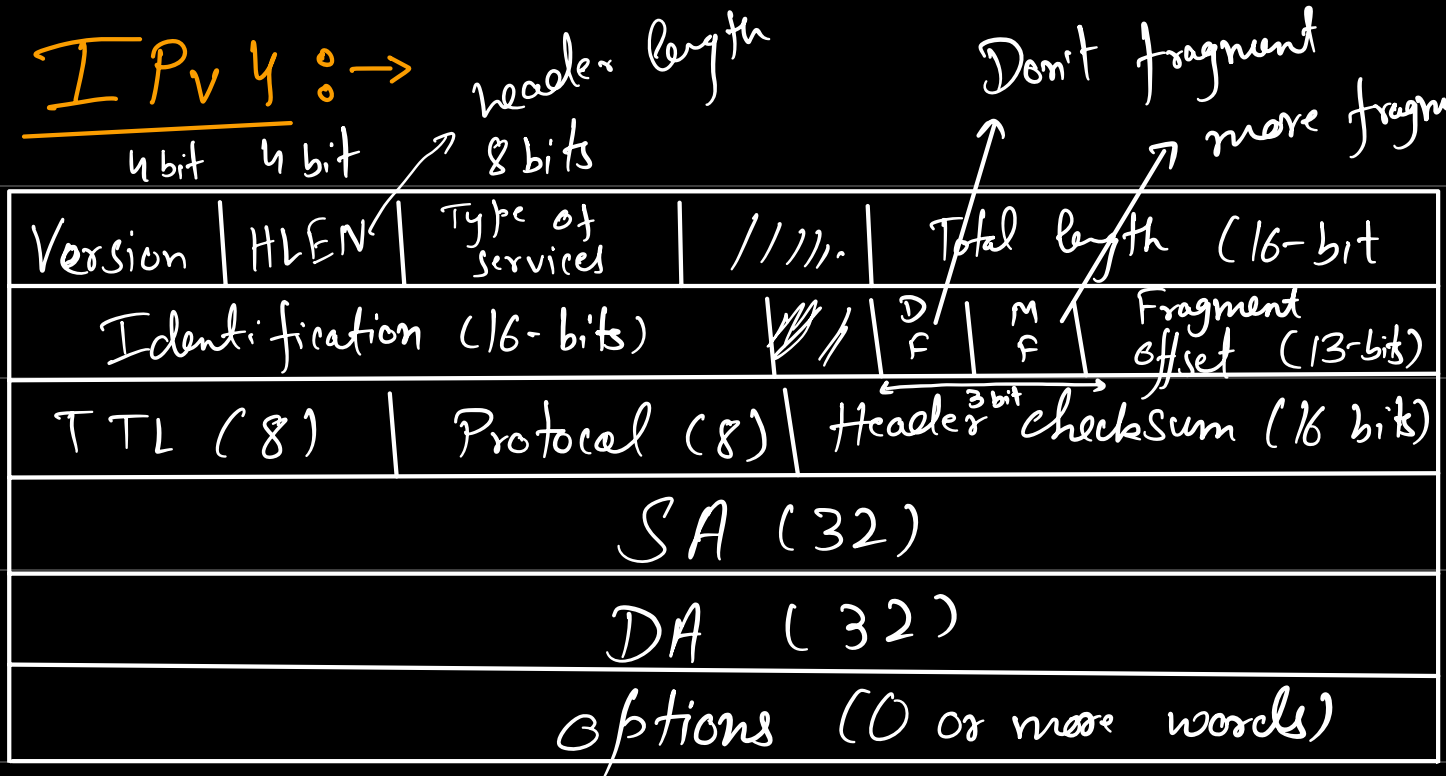
1st: 190.100.64.0/25 to 190.100.64.127/25

2nd: 190.100.64.128/25 to 190.100.64.255/25

3rd:

Similarly Group 3:

IPv4 :→



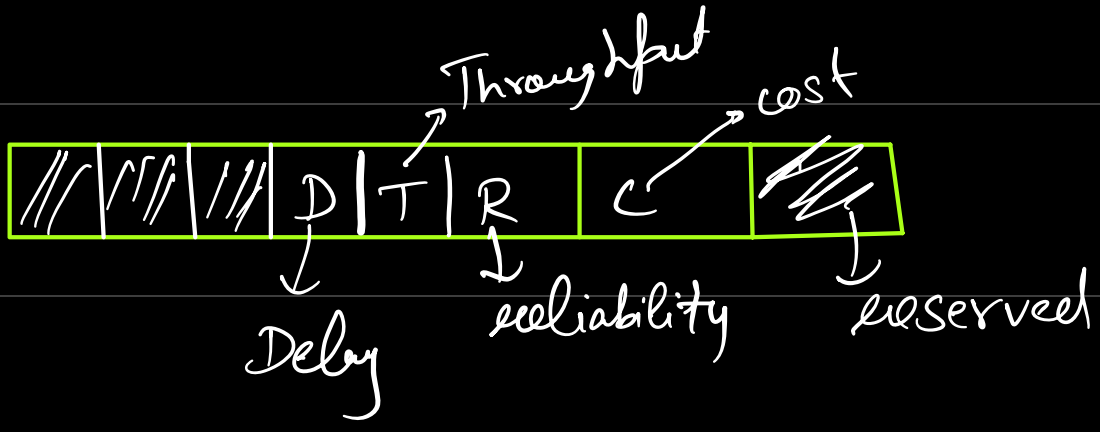
- Total length is the length of data and length of header.
- Identification is used in the process of fragmentation.
- Flags and fragmentation offset is used in fragmentation.
- TTL expands to time to live
- Protocol → RFC 1700 provides a documentation

for protocols utilized for IP

- Options include Security, strict Source routing, loose Source routing, record route, time stamp.

IPv4

- Types of Services



0 0 0 0 → Normal

0 0 0 1 → with minm cost msg. should be sent

0 0 1 0 → Maxm reliability

0 1 0 0 → " Throughput

1 0 0 0 → Minm delay.

- The first three bits provide priority of datagram during congestion.

- NOTE → Length of header is b/w 20 – 60 Bytes.
  ↓ without options.

- If the header length uses 4 Byte word.

Ex. An IPv4 packet has arrived with first 8 bits as

01000010

The reciever discards it. Why?

→ 0100 0010 → header length → converted in decimal

0100 ↓ Version

0010 ↓ $2 \times 4 = 8 < 20$ ↓ Std.

That's why

- **IPv4** → ① It is a connection less unreliable and uses datagram protocol
② It provides best effort delivery service. [No error & flow control is supported by IP]

- **IPv6** →

Limitations of IPv4

→ ① Adress depletion

② Strategies and reservation of resources isn't provided

③ No encryption and authentication

- Adv. of IPv6 →
① Larger adress space
② Better header format

③ Inclusion of new options

④ It allows for extentions.

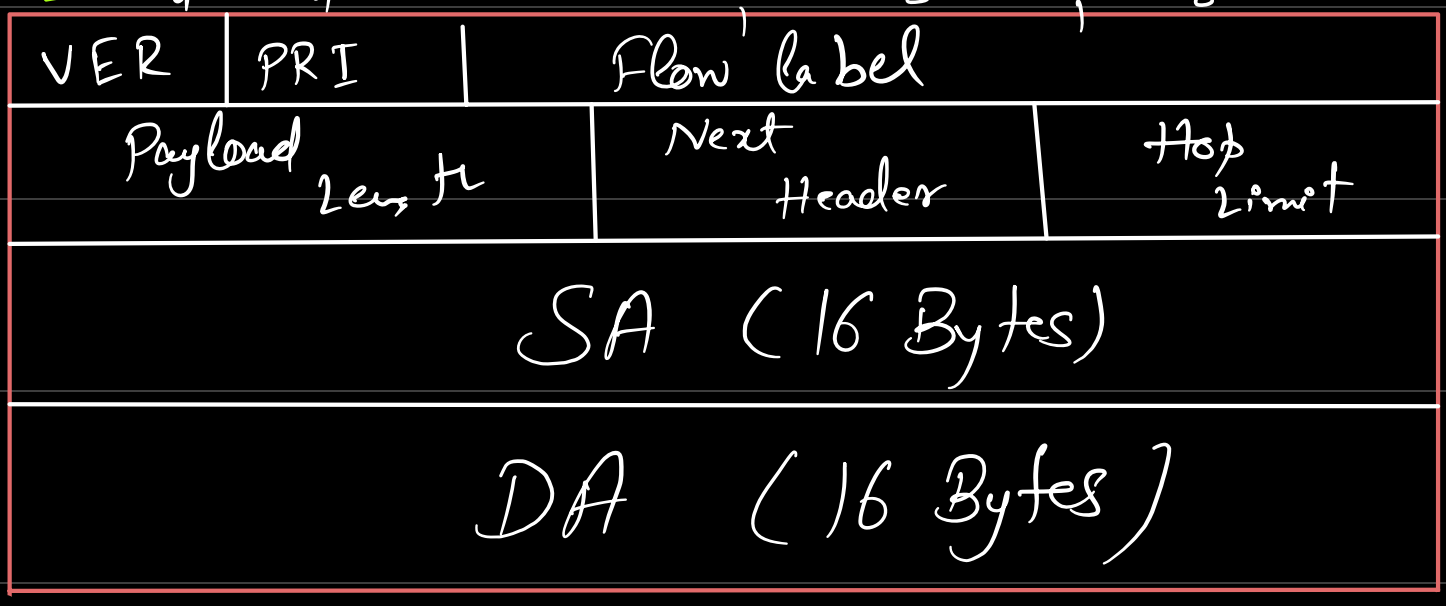
⑤ Support resource allocation

⑥ More Security.

→ confidentiality

→ Integrety (data is intact)

- **Packet Format**



- PRI → priority
- Traffic congestion is of Two Types

① Congestion Control Traffic

0-7 → PRI

→ ① No specific traffic
② Background Data
③ Unattended data traffic
④ Reserve)
⑤ Attended bulk data traffic
6. (Reserved)
7. Interactive traffic
8. Control traffic.
↓
control messages

② Non-congestion control Traffic

8-15 → PRI

- Flow Label → • Flow of packets from a particular source to a particular destination

- Payload Length → • Length of datagram excluding header

- Assignment → Compare b/w IPv4 & IPv6

• Transition from IPv4 to IPv6

Methods →

① Dual Stack → Padh lena.

② Tunneling → Code used is 41 by

③ Header Translation

→ ① IPv6 mapped adress is changed to IPv4 by extracting the rightmost 32 bits.

② The value of IPv6 priority field is discarded.

③ Tos bits in IPv4 is set to 0. ↓ Type of services.

④ Checksum for IPv4 is calculated and inserted

⑤ IPv6 flow label is ignored.

⑥ Extention headers is converted to options.

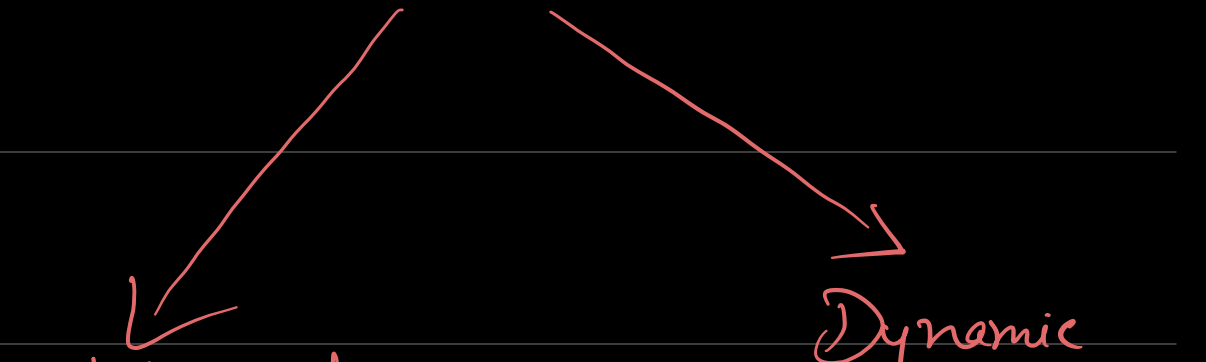
⑦ Legth of IPv4 header is calculated.

⑧ Total legth of IPv4 header field is calculated.

Sender IPv6

reciever IPv4.

Adress Mapping



Static →

Table is stored in each machine of the network.

Limitations → ① The NICs can change

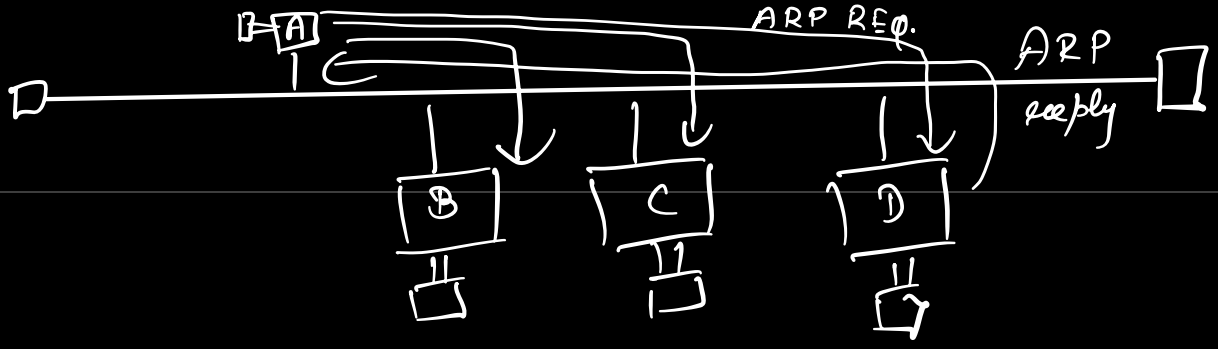
② Physical adress chages with every in some LANs such as that provided by

apple and is known as Local Talk

③ Mobile devices change physical network due to which physical adress chages.

- Dynamic -> Each time the machine knows one of the two adresses It can use a protocal to find the other one. (ARP, RARP, BOOTP, DHCHJ

- Logical to Physical Adress mapping
- ARP → adress resolution protocal.

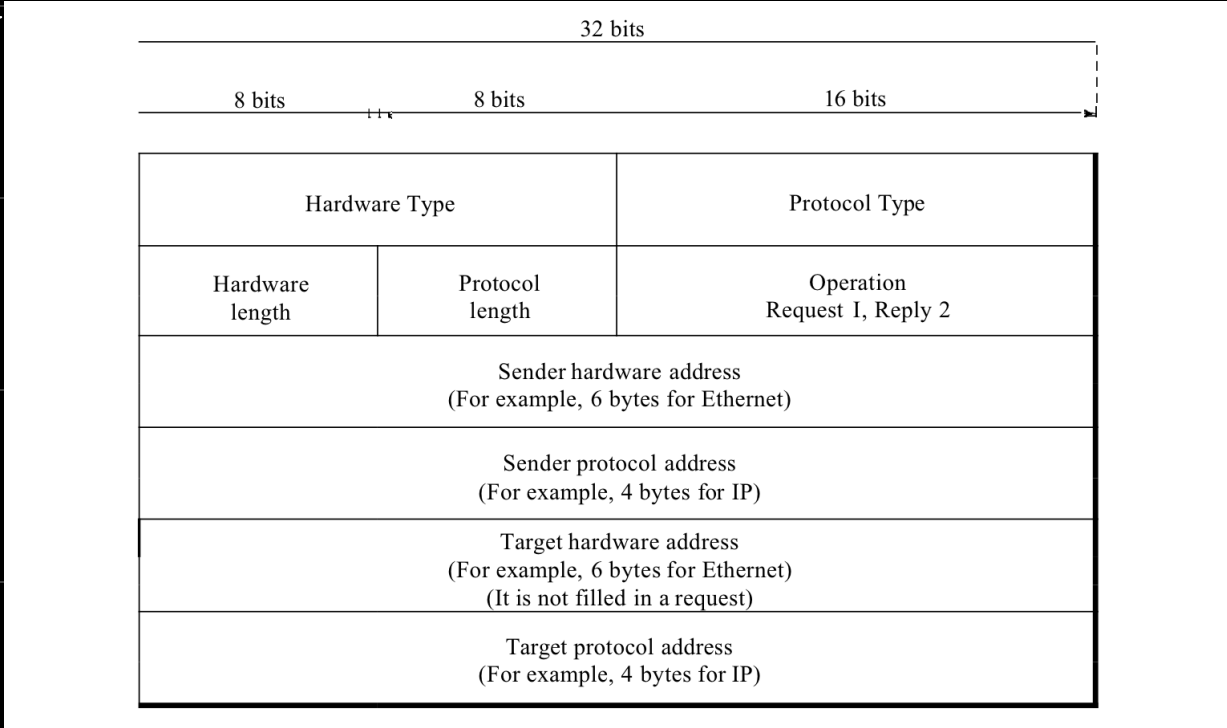


ARP 192.168.1.3

① ARP request
↓
- issued by machine which needs to find physical address
- A broadcast message

② ARP Reply
↳ unicast message.

ARP



4 Cases of Target IP

→ Case I → When source and adress are in same network.

Target IP is destination adress of IP datagram.

Case II → Source and destination are on diff network.

→ Target IP of routes.

Case III → Router recieves a packet from source to be sent to a host on another network.

⇒ IP adress of appropriate

Router.

Case IV → Router is sending a packet to be sent to a host in the same network

→ destination adress of IP datagram.

- PA → LA mapping →

There are certain conditions where in such kinda mapping is req.

(1) Existence of diskless station

(2) Non-availability of enough

IP adresses.

1st protocol

① RARP → • Reverse adress resolution protocol

• The target adress is known but physical adress in unknown.

Limitation → • Broadcasting is done at DLL

The physical broadcasting adress doesn't pass the boundries of a network.

② BOOT P → Bootstrap protocol

(Application Layer protocol)

① Client or Server application layer processes wherein all of them are in same network.

② Relay management wherein BootP client and server are in diff network

- Relay agent knows unicast address of BootP server.

Limitation → ① BootP request is broadcast and can't pass through any router.

② Not a dynamically configured protocol.

(3) DHCP → dynamic host config. protocol.

- Adress allocation
  - Static
  - Dynamic
- Configuration
  - Manual (Static)
  - Automatic (Dynamic)
- For static adress allocation →
  1. DHCP acts as BootP does for static adress allocation
  2. It is backward compatible with BootP
  3. A host with bootp client can request a static

adress from DHCP Server.

- **Dynamic**

→ • It uses a second database with a pool of adresses which make it dynamic

- It is used for lease based allocation especially for the mobile users.

- **ICMP** → Internet control message Protocol.

There are 2 defficiencies of IP vis'a vis

① Lack of Error control
② Lack of Assitance mechanisms

There are two type of message supported by ICMP →

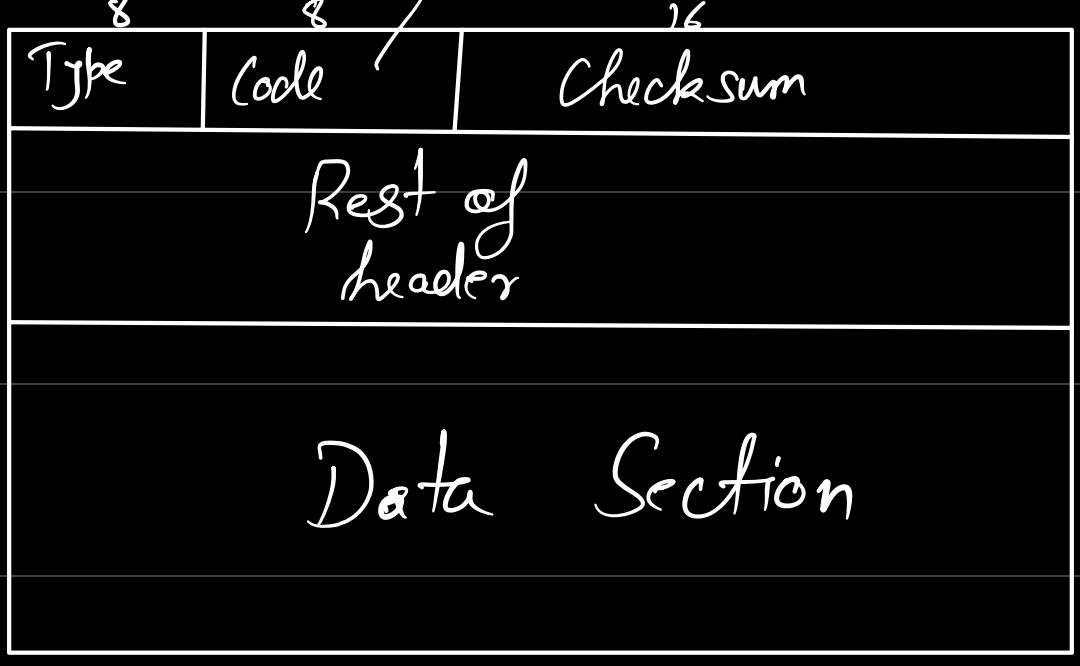
① Error reporting → It reports problems that a router or a host may encounter while processing IP packets.

② Query messages → Occurs in pairs and helps a host or network manager get specific info from routers or another host.

Use of query messages

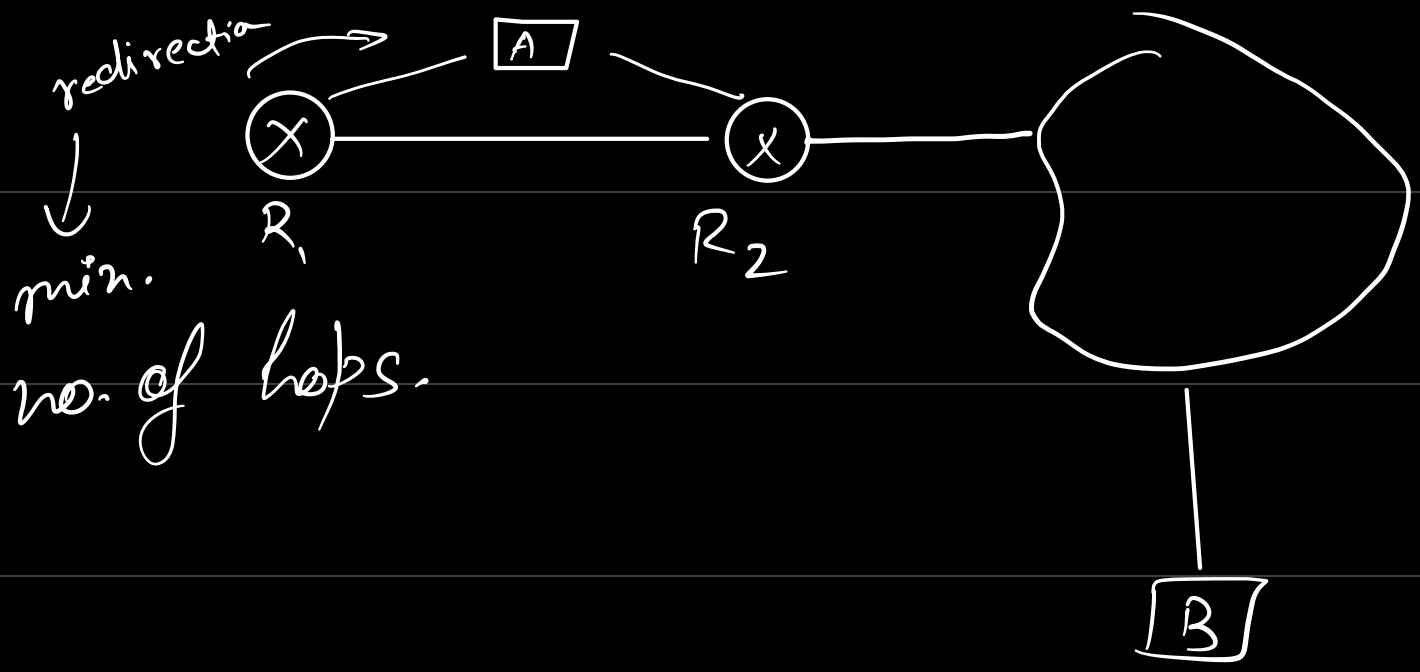
- Router helps a node in redirection
- Helps to discover routers
- Sometimes nodes can discover their neighbours also.

reason for type of message



Packet format of ICMP.

- Error Reporting -> ICMP always reports the error messages to original Source
- Some of the examples are
  1. Destination unreachable
  2. Source Quenching
  3. Time exceeded.
  4. Parameter problems
  5. Redirection.



- Query → It is used to diagnose the network problems

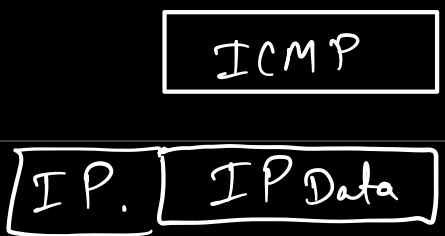
Some examples are

① Echo request and reply.

② Timestamp req. & reply.

③ Adress mask req. & reply

④ Router solisitation and advertisement.



- **IGMP →** (Slides se padha wha tha bs)

IP protocol can be involved in two types of communication:

① Unicasting
② Multicasting

- IGMP → Internet group management Protocol.

(necessary but not sufficient for multicasting)

4 parts

→ ① Group magement
② IGMP messages.

- Group mangement → · IGMP