Unit 3 CN - Computer Network Notes Unit 3

B.tech (Dr. A.P.J. Abdul Kalam Technical University)

Unit-3 Network layer:-

Responsibility:- ① Host to Host (source to Destination) source m/c to Destination m/c

② Logical Address (IP Address)

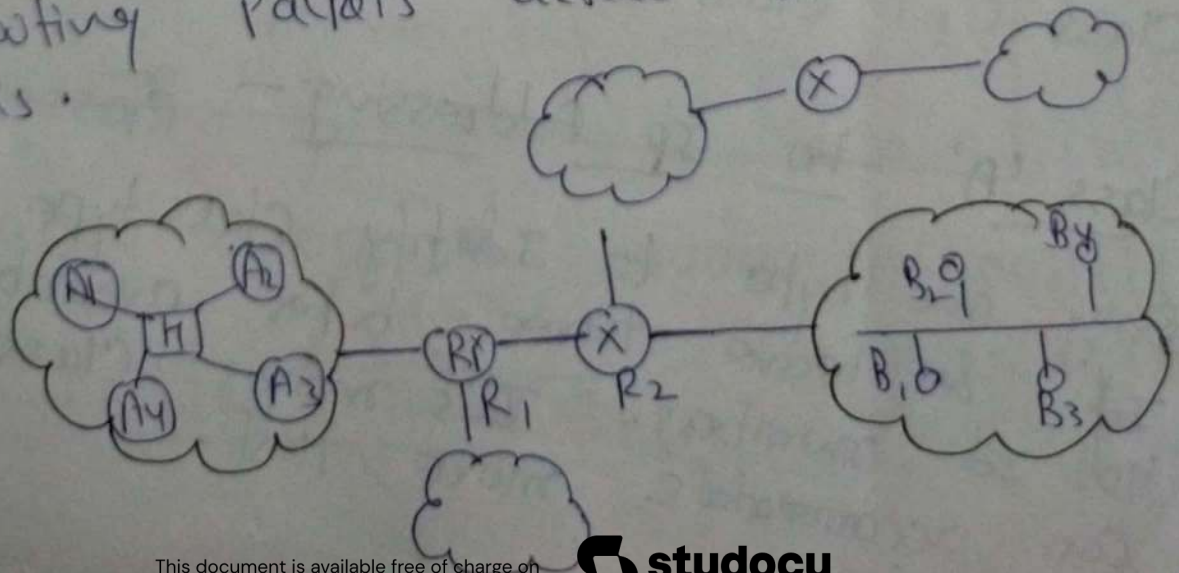
Network Id | Host Id

③ Routing methods

④ fragmentations (Packet)

The Primary function of the network layer is to enable differed networks to be inter-connected. It does this by forwarding packets to network routers which rely on algorithms to determine the best path for the data to travel.

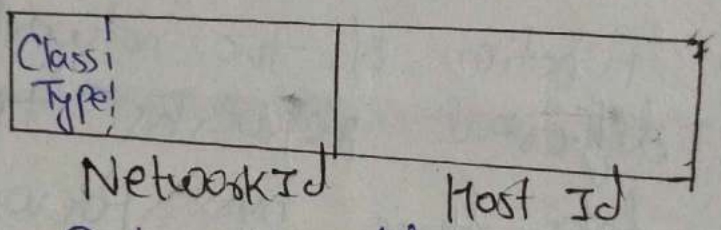
The most important Protocol of this layer is Internet Protocol or IP. It is the standard for routing Packets across inter connected networks.



Addressing: → The Internet requires an additional addressing convention: An address that identifies the connection of a host to its network.

Two types of Addressing → Classful Addressing
→ Classless Addressing

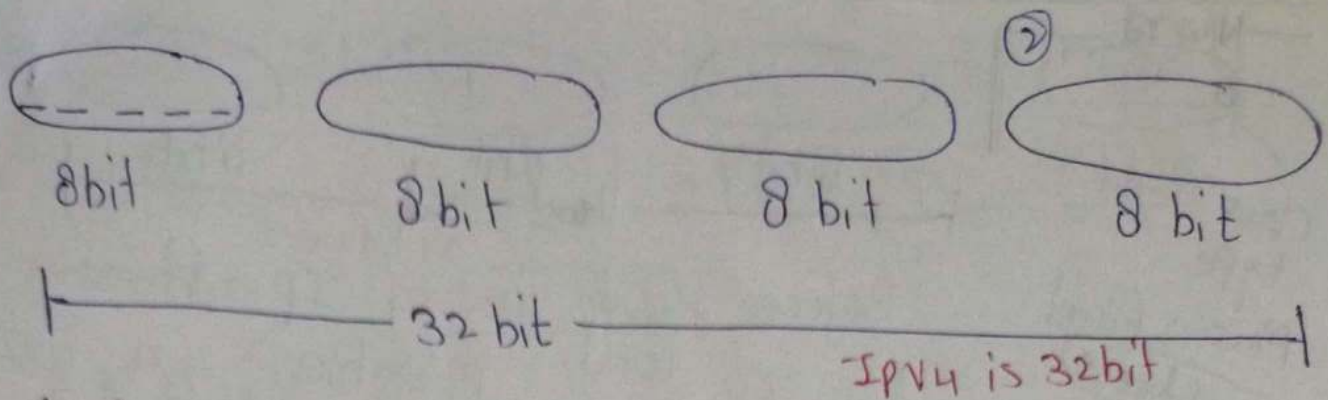
- Each Internet address consists of four bytes (32 bits) defining fields: Network Id (Class type also) Host Id. These parts are of varying lengths, depending on the class of the address.



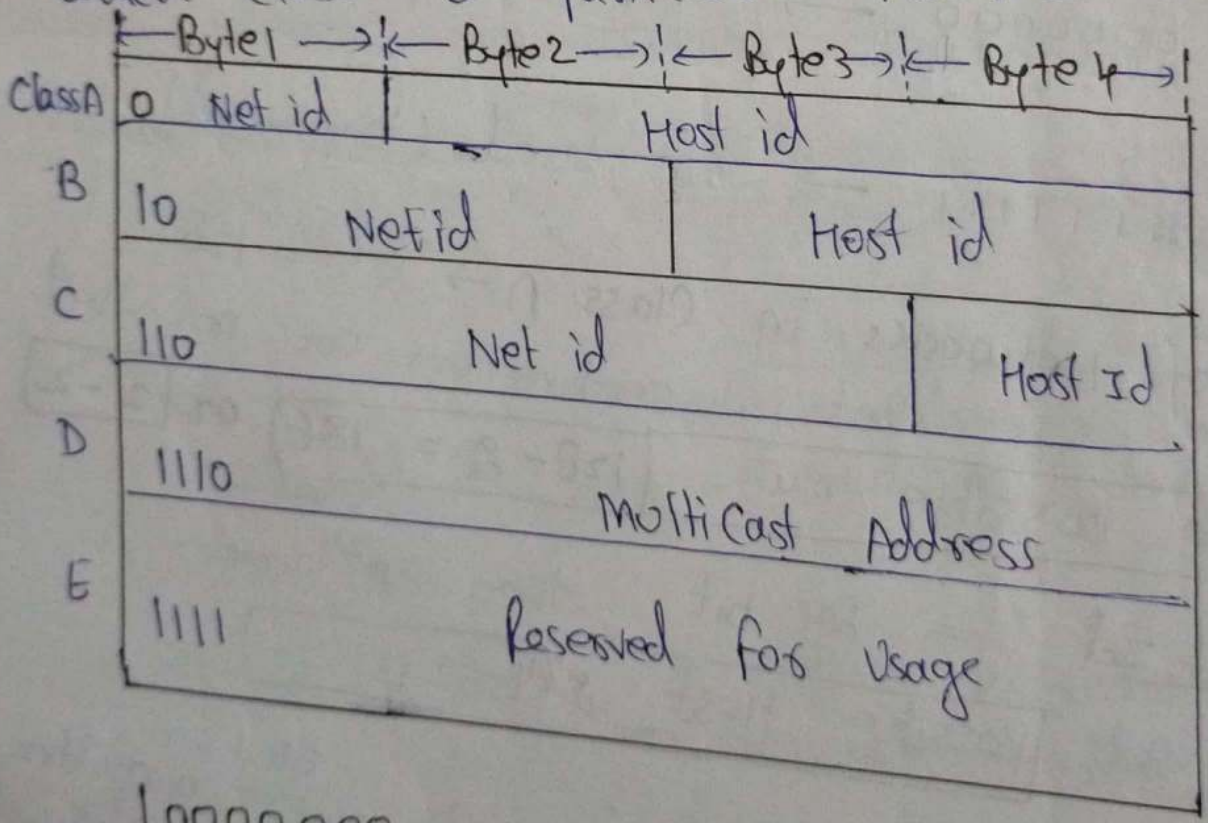
- An Internet Address is made of four bytes (32 bits) that define a host connection to a network.

Classes:- There are currently five different length Pattern in use - Class A, Class B, Class C, Class D & Class E.

Class 'A' in Ip Addressing:- Class A uses Only one byte to Identify class type & Network Id & leave three bytes available for Host Id numbers. This means Class A n/w Can accommodate more Host.

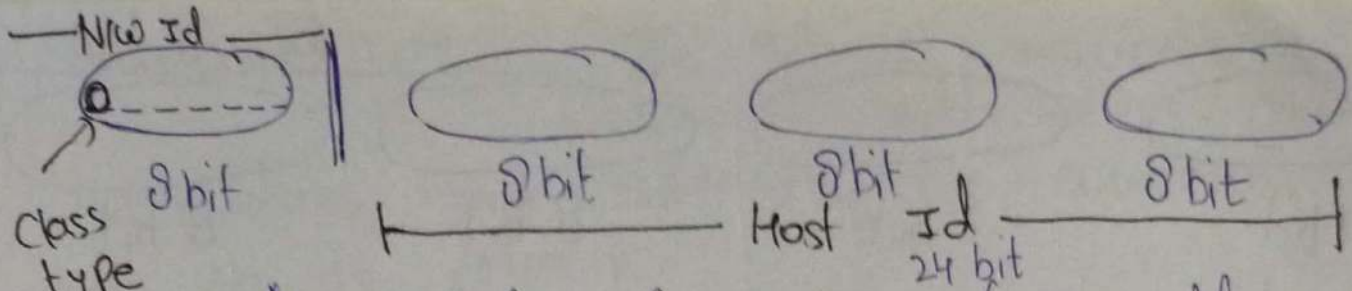


Dotted decimal Notation:- To make 32 bit form shorter & easier to read, Ip addresses are usually written in decimal form with decimal points seperating two bytes - dotted decimal notation. First byte of an address in decimal form allows us to determine to which class a particular Address belongs.



10000000 . 00001011 . 00000011 . 00011111

Ip address → 128 . 11 . 3 . 31



IP address

Before fixing no. of IP addresses were possible $= 2^n = 2^{32}$

① 1 bit is fixed to define Class type

So ⇒ **No of IP addresses possible = 2^{31}**

② ⇒ Network Id. 1 bit fixed, 7 bits are left (combinations)

$= 2^7$ (maximum)

Fixed ↓

0→ 0 0000000 → not used by any organization

1 0000000

⋮

127→ 0 1111111 → not used (Diagonised)

No of Networks in Class A → $2^7 = 128$

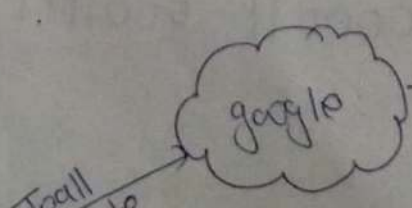
But 2 combinations are not used.

then possible n/w | 128 − 2 = 126 used | or $2^7 - 2$

③ Host Id = 24 bit then 2^{24} max.

But **Possible Host $2^{24} - 2$**

Ex.



To all google host Broadcast

64.0.0.0 → 64.255.255.255

First Reserved whole n/w last address

no Host

64.0.0.0 → n/w address

So 64.0.0.1 → 1st host

64.255.255.255 → Broad Cast To all host that's why no Protocols

Class Range of A:-

0.0.0.0 (From) — 127.255.255.255 (To)

0 - 127

Ex: 93.31.1.245 , 4.23.145.90

↳ 64.0.0.8 (To Identify the nw address of IP address then use default mask.

Default mask of Class A: 255.0.0.0

Apply AND operation b/w default mask & IP address to Identify the network Id.

→ 64.0.0.8 (Host)
255.0.0.0

```
01000000.0.0.00001000
11111111.0.0.00000000
--------------------
01000000.0.0.00000000
```

64.0.0.0

Ex: Find the Class of each address, net Id, Host Id & network Address also:-

4.23.145.90

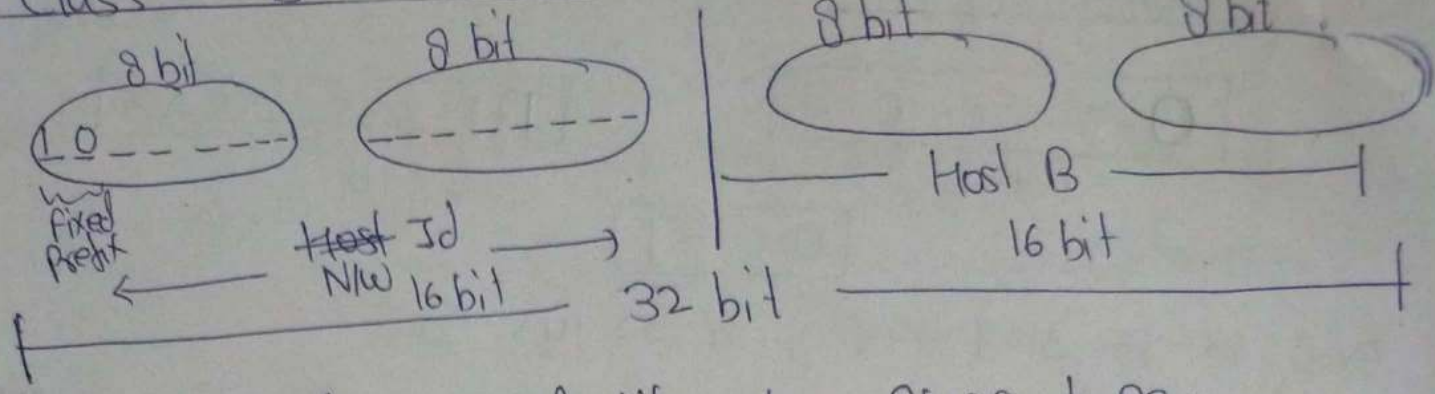
93.31.1.245

Sol: "Class A"

- Masking extracts the network address from an IP address.

- Class A addresses were designed for large organizations with a large no. of hosts or routers.

Class 'B' →



- Prefix is used to identify two class type.

10 000000 → 128
10 000001
10 000010
10 :

10 111111 → 191
128 64 32 16 8 4 2 1

Default mask = 255.255.0.0

128
32
16
12
3
191

(5) Range: 128.0.0.0 — 191.255.255.255

(1) No of address (IP) = 2^{30} Possible.

(2) Network Id = 2^{14} = 16384
$2^6 \times 2^8 = 2^{14}$

Possible N/w = 2^{14}

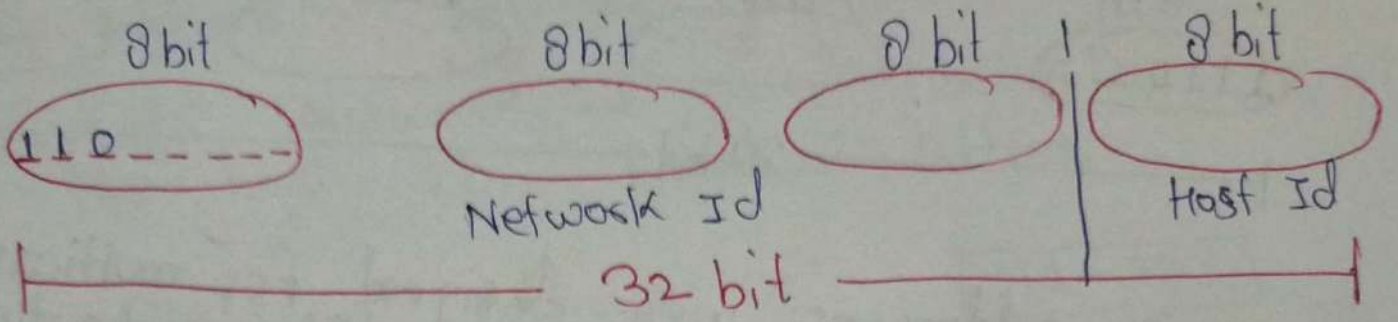
(3) Host Id: 2^{16} = 65536
but used = $2^{16} - 2$ = 65534
↙ ↘ Broadcast
n/w address Host all

Ex: 130.2.3.4 → ClassB

135.65.13.9 → 128.0.0.0 n/w address.
n/w Add: 135.67.0.0 128.0.255.255 ~~last host~~
Broadcast.

" Class B addresses were designed for mid-size organizations with tens of thousands of attached hosts or routers.

Class 'C' in IP addressing: (4)



110 00000 → 192
110 00001
110 00010
. . . .
110 11111 → 223

Range = 192 - 223

(1) No of IP addresses $= 2^{29}$

(2) No. of Networks:

2^{21}

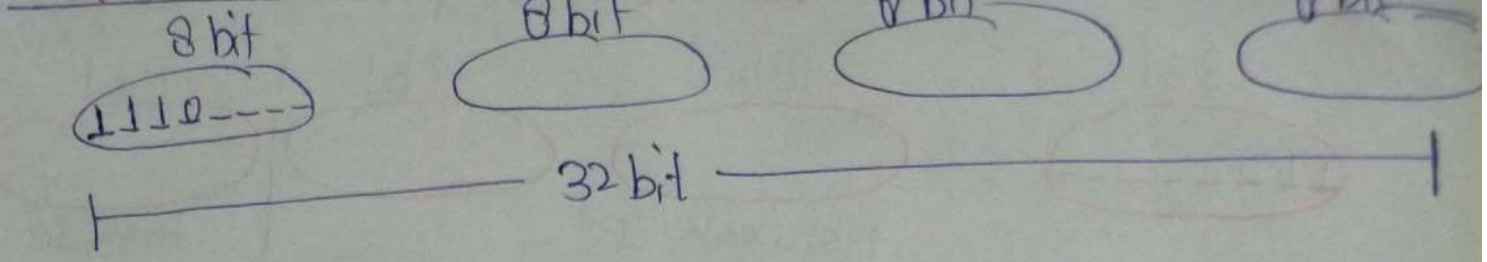
(3) No. of Host $= 256 - 2$

Usable = 254

(4) default mask = 255. 255. 255. 0

Class C addresses were designed for small organizations with a small no. of attached hosts or routers.

Class 'D'



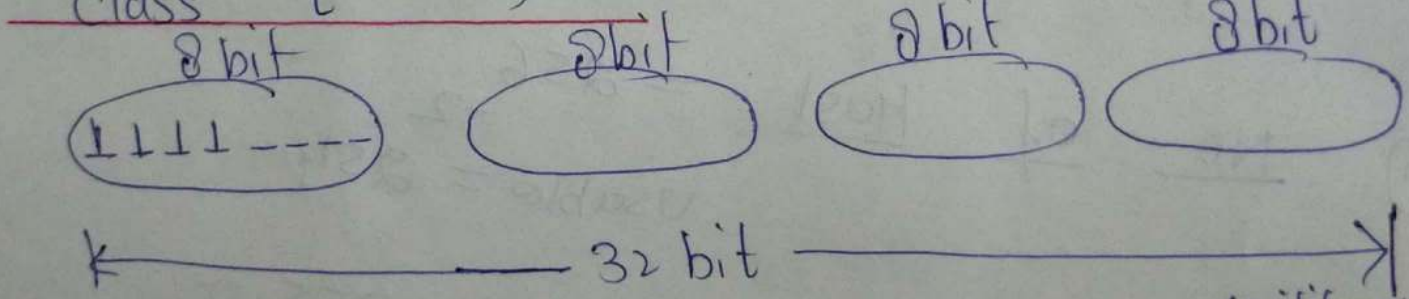
Class D addresses were designed for multicasting. Each address in this Class is used to define one group of hosts on the Internet. (Emailing groups)

8bit
1110.0000 → 224
:
1110.1111 → 239

No. of IP addresses in D = 2^{28}

The Internet authorities wrongly predicted a need of 2^{28} groups. This never happened & many addresses were wasted here.

Class 'E' →



(military)

Class E addresses were used for future use, only a few were used, resulting in another waste of addresses.

In Classful Addressing, a large part of the available addresses were wasted.

No of IP addresses: 2^{28}

Range: 1111 0000 → 240

1111 1111 → 255

240-255

'Numericals'

Ip address: 201. 20. 30. 40
130. 1. 2. 3

Calculate Network Id, 4th Host ID, last Host ID, Broadcast Address.

Sol: Class: → Address 'C' [192-223]
'201'

Nw Id:

mask
255. 255. 255. 0

```
  201. 20. 30. 40
  255. 255. 255. 0      AND
  ---------------
  201 . 20 . 30 . 0
```

4th Host ID ⇒ 201. 20. 30. 4

Last Host ID ⇒ 201. 20. 30. 254

Broadcast Address ⇒ 201. 20. 30. 255

for any network limited: [255. 255. 255. 255]

Problems with Classful Addressing:-

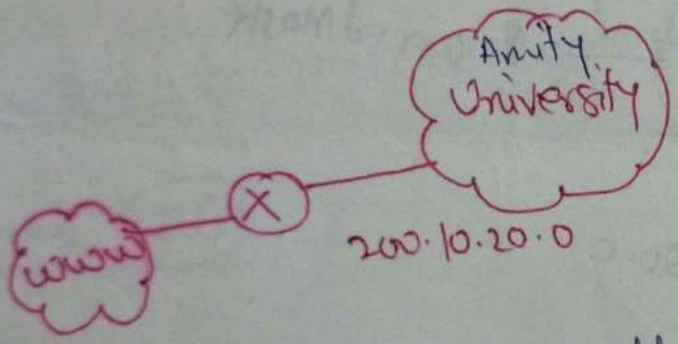
- Wastage of Ip addresses
- Maintenance is time Consuming
- More prone to error.

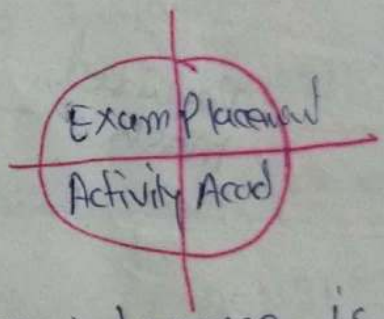
2^{24} = 1 Crore
no one org has 1 crore host generally.

Subnetting ①

"Dividing the big network into small networks"

⇒Subnetting was introduced in the era of Classful addressing. If an organization was granted a large block in Class A or B, it could divide the addresses into several contiguous groups & assign each group to smaller networks called subnets. Subnetting increases the number of 1s in the mask.





- Maintenance is easy
- Security

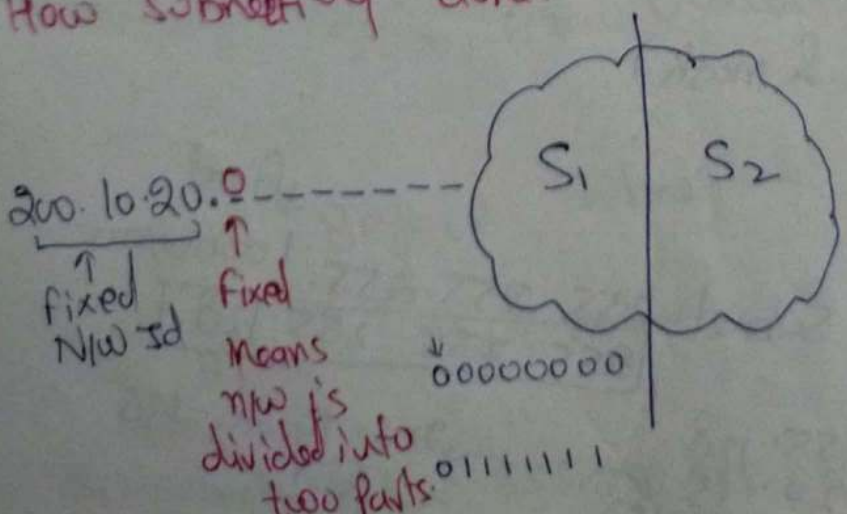
200.10.20.0 → network address

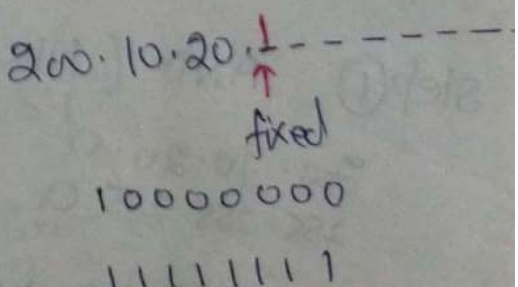
200.10.20.255 → Broadcast

200 ↑ Class C

useable Address Host ⇒ 254

How subnetting done:—

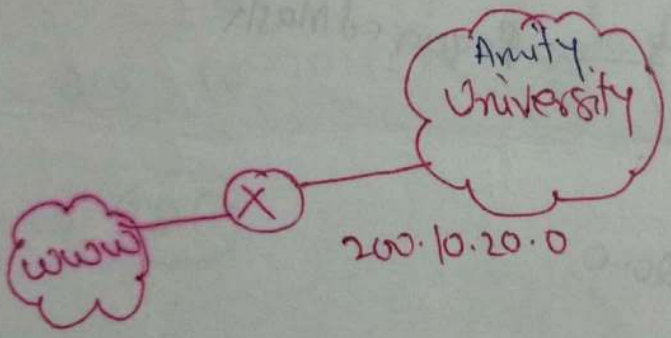


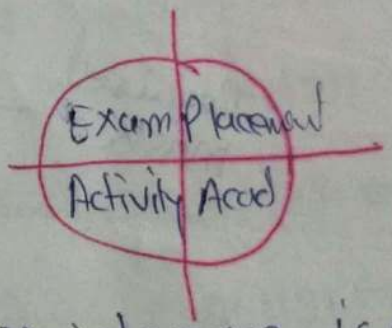


Subnetting ①

"Dividing two big network into small networks"

⇒Subnetting was introduced in two era of Classful addressing. If an organization was granted a large block in Class A or B, it could divide the addresses into several contiguous groups & assign each group to smaller networks called subnets. Subnetting increases the number of 1s in the mask.





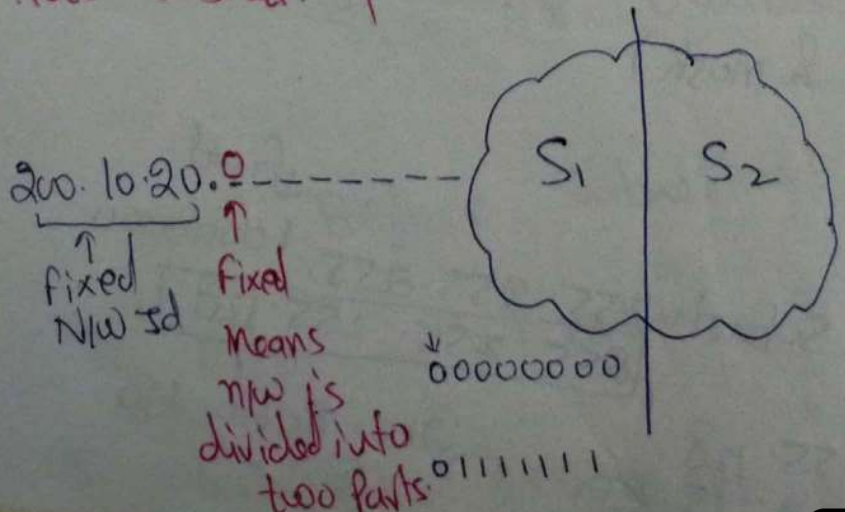
- Maintenance is easy
- Security

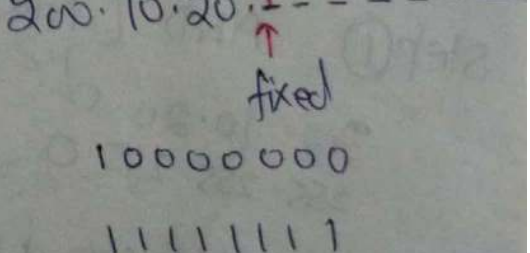
200.10.20.0 → network address

200.10.20.255 → Broadcast

↑ Class C useable Address Host ⇒ 254

How subnetting done: —





S_1 ← Subnet Id

200.10.20.0
to
200.10.20.127
↑ Broadcast Add.

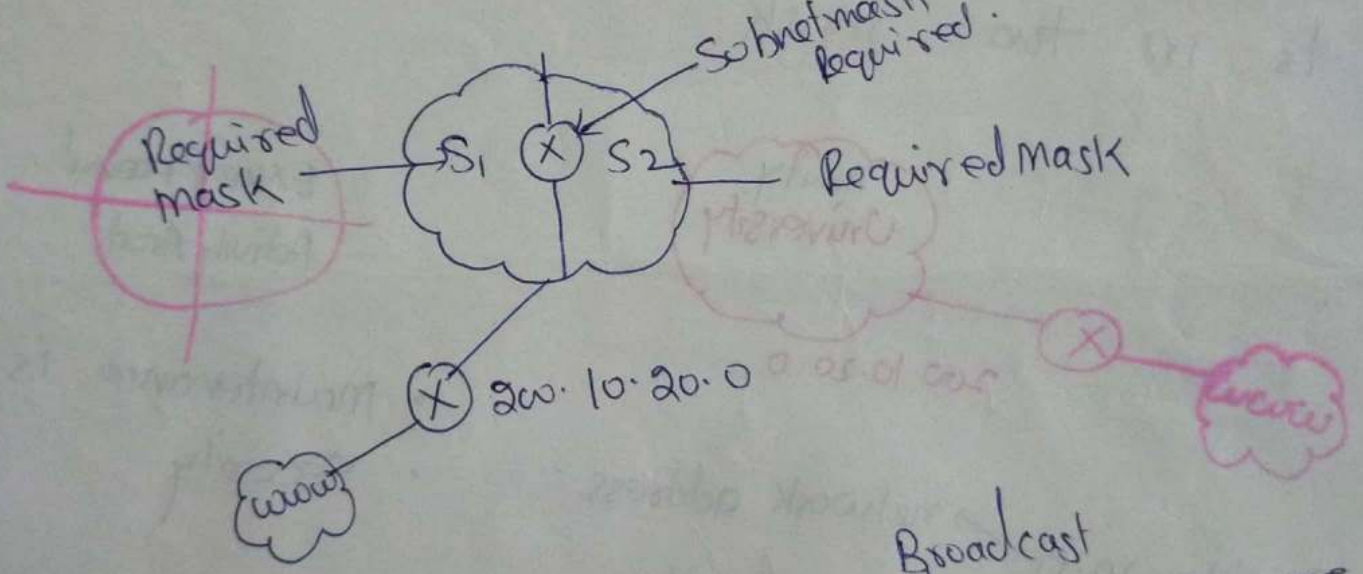
S_2 ← Subnet Id

200.10.20.128
to
200.10.20.255
↑ Broadcast

Host Useable = 126

Host = 126

Before Subnetting Useable = 254
After Subnetting " = 126 + 126 = 252



S_1 Id 200.10.20.0

Whole N/w Id 200.10.20.0

Broadcast
S_2 Id 200.10.20.255

Whole Broad = 200.10.20.255

Step ① AND (N/w Id & Mask)

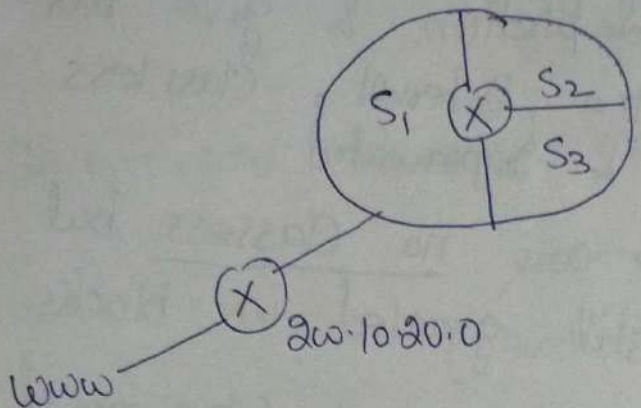
200.10.20.0
255.255.255.0

Step ② Mask for Subnet 255.255.255.10000000 (fixed)
255.255.255.128

Ex: 255.255.255.128
200.10.20.15 → S_1

200.10.20.130 → S_2

Variable length Subnetting:

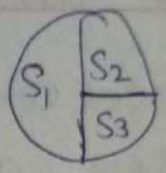


(S1) 200.10.20.0 0 0 0 0 0 0 0 0 ← fixed
to
0 1 1 1 1 1 1 1

200.10.20.0 ← Subnet
to
200.10.20.127 ← Broadcast (S1)

$S_1 \Rightarrow$ (126)

(2)



0-255
= 254

① above lw address
other 2 above so

S_2 200.10.20.1 0 0 0 0 0 0 0 ← fixed fixed
to 1 0 1 1 1 1 1 1

S_3 200.10.20.1 1 0 0 0 0 0 0 ← fixed
to
1 1 ϕ ϕ 1 1 1 1

S_2 = 200.10.20.128 ← Subnet
to
200.10.20.191 ← Broad
64-2 = 62

S_3 = 200.10.20.192 ← Subnet
to
200.10.20.255 Broadcast

S_3 = 62 Useable

Total Before Subnetting = 254

After subnetting = 256-6
= 250

S_1 Subnet Mask = 255.255.255.128

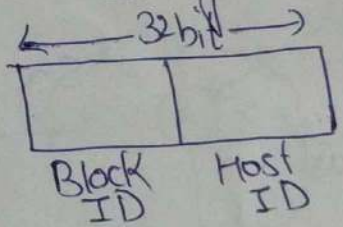
S_1 & S_3 Subnet Mask
255.255.255.192

Classless Addressing :- 1993

. To overcome address depletion & give more organizations access to the Internet, classless addressing was designed & implemented.

. In this scheme there are no classess but the addresses are still granted in blocks.

Address Block: The size of the block (the no. of addresses) varies based on the nature & size of the entity.



Block
↳ may be act as N/w Id but not fixed.

Notation: — In IPv4 addressing, a block of addresses can be defined as

x.y.z.t	n

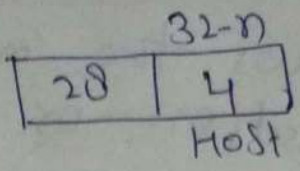
in which x.y.z.t defines one of the addresses and the /n defines the mask.

/n notation completly define the whole block (the first address, last address & no. of addresses)

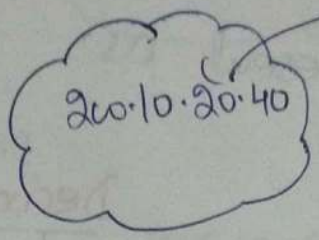
/n → mask
/n → no. of bits represent block / network

Ex: 200.10.20.40/28 → Block Id.

200.10.20.40/28 (3)



28 bits are represent as 1's to define n/w or Block.



any Host In network bol
what is N/w Id.

To find Network Id requires Mask (Default) So 28 bit showing network Id uses bit then Continuous 28 (1's) will be used to find Mask.

11111111 . 11111111 . 11111111 . 1111 0000
8 8 8 4

→ 255. 255. 255. 240

Default mask of this n/w

255.255.255.240
AND 200.10.20.40
200.10.20.32

N/w Id:

either

200.10.20.0010 1000
28 bit Can't Change
Host (0000) convert
00100000

200.10.20.32/28

~~Restriction:-~~

The form /n shows the mask. This notation is called slash notation or Classless Interdomain Routing (CIDR) notation.

If we use this notation /n is classful addressing this can be represent as:

Class	Binary	Decimal	CIDR
A	11111111 00000000 00000000 00000000	255.0.0.0	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	/16
C	11111111 11111111 11111111 00000000	255.255.255.0	/24

Restriction CIDR:

(1) The addresses in a block must be contiguous, one after another.

(2) The number of addresses (Host) in a block must be a power of 2 (1, 2, 4, 8 - -)

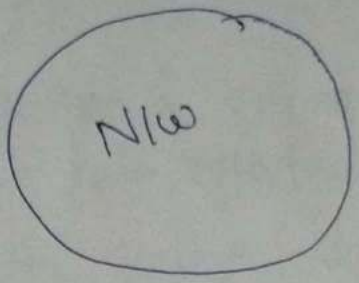
(3) The first address must be evenly divisible by the number of addresses.

n/w address
~~Sig of block~~
number of addresses.

255.10.20.32
16 ↓
0010 0000,
if 24 means 4 bits are zero then ok.

→ Block 32

Subnetting in CIDR



195.10.20.10000000

N/w Id Host Id already zero

N/w Id 195.10.20.128/26

195.10.20.128/26

195.10.20.129/26

195.10.20.10000001

N/w Host

N/w Id 195.10.20.10000000

→ 195.10.20.128/26

No N/w bit can be changed, only Host bits variations are possible.

Subnetting → It can be applied only in 6 bits.

195.10.20.10000000

fixed

195.10.20.100 00000

to

100 11111

195.10.20.128 → Host

to → N/w

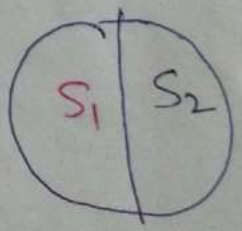
195.10.20.159 → Broadcast

Use = 30

195.10.20.128/27

to

195.10.20.159/27



195.10.20.101 00000

fixed

195.10.20.101 11111

195.10.20.160/27 → N/w

to

195.10.20.191/27 → Broad

Use = 30

One more bit fixed /27

IPv4

- Internet Protocol Version 4 is the delivery mechanism used by the TCP/IP Protocols.
- IPv4 is unreliable & connectionless datagram Protocol – a best ~~de~~ effort delivery service.
- Packets in IPv4 layer are called Datagrams. & IPv4 is a connectionless Protocol for a packet switching network that uses the datagram approach. This means that each datagram is handled independently & each datagram can follow a different route to the destination.

IPv4 — Connection less
IPv4 — Datagram service

VER 4bit	HLEN 4bit	Service 8 bit	Total length 16 bit
Identification 16 bit		Flag 3bit	Fragment offset 13 bit
Time to Live 8 bits	Protocol 8 bits	Header checksum 16 bits	
Source IP address 32 bits			
Destination IP address 32 bits			
Options & Padding (optional)			

65515 + 20 = 65535

2^{16}

= Datagram — Header size = min 20 – 60 Bytes. (160 bit – 480 bit)
Datagram — Payload (Pure data) = 0 – 65515 Bytes
min max

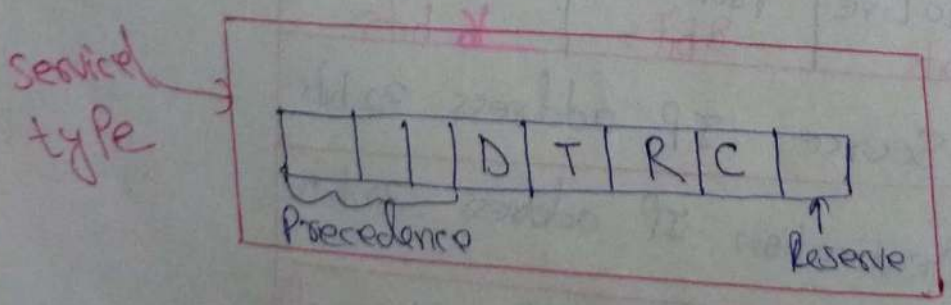
A datagram is a variable length packet consisting of two parts: Header & Data. The header is 20 to 60 bytes in length & contain information essential to routing & delivery.

Description of each field is in order →

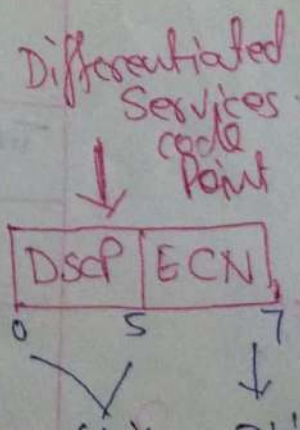
① Version:- This field tells that IPv4 software running in the processing machine that the datagram has the format of Version 4. (0100) 4bit is fixed for IPv4.

② Header length:- 4bit field defines the total length of the datagram header. This field is needed because the length of ~~variable~~ header is variable between (20-60 bytes)

③ Services:- This field previously called service type is now called Differentiated services.



D: Minimize delay
T: Maximize throughput
R: Maximize Reliability
C: Minimize Cost



⑦ Checksum:- It is 16 bit field used for error detection.

⑧ source address:- This 32 bit field defines the IPV4 address of the source. This field must remain unchanged during the time the IPV4 datagram travels from source to destination.

⑨ Destination address:- This field also must unchanged during the time data Travels.

Fragmentation:-

Identification 16 bit	Flag 3 bit	Fragment offset 13 bit

A datagram can travel through different networks.

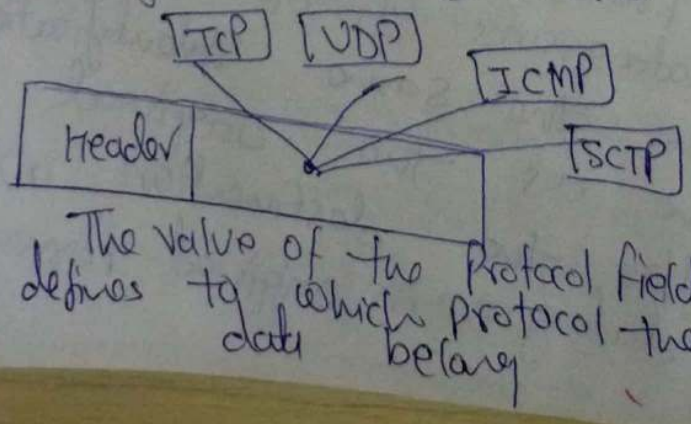
① Identification: This 16 bit field identifies a datagram originating from the source host. To guarantee uniqueness at receiver end, the IPV4 Protocol uses a counter to label the datagrams. In other words all fragments have the same identification number, the same as the original datagram. It helps the destination in reassembling the datagram in original form.

④ Total length:- This is a 16 bit field that defines the total length (header plus data) of the IPv4 datagram in bytes. To find the length of data coming from upper layer, subtract the header length from the total length. 2^{16}

Length of data = Total length − Header length

⑤ Time to live:- (8 bit) This field is needed because routing tables in the internet can become corrupted. A data gram may travel between two or more routers for a long time without ever getting delivered to the destination host. This field limits the lifetime of a data gram. $2^8 = 256$ (0-255)

⑥ Protocol:- This 8 bit field defines the higher level protocol that uses the services of the IPv4 layer. IPv4 datagram can encapsulate data from several higher level protocols such as TCP, UDP, ICMP & IGMP. It specifies the final destination Protocol to which the IPv4 data gram is delivered.



The value of the Protocol field defines to which protocol the data belong

Value	Protocol
1	ICMP
2	IGMP
6	TCP
17	UDP

(2) Flag:- This is 3 bit field. First bit is reserved. The second bit is called do not fragment.

DF — set 1 → No fragment
DF — set 0 → fragment

| R | DF | MF |

(3) More fragment:-

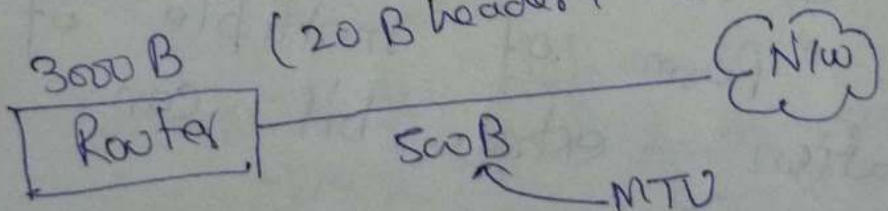
set 0 — It means this is the last or only fragment

set 1 — Datagram is not the last fragment

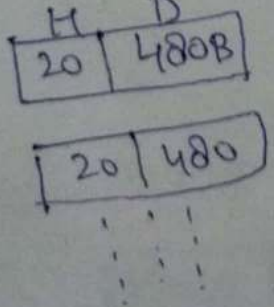
(3) offset: This 13 bit field shows the relative position of this fragment with respect to the whole datagram. (no of bytes ahead packet)

MTU:- Maximum Transfer Unit: Total size of datagram must be less than this max size.

3000 B (20 B header + 2980 B)



$\left\lceil \frac{2980}{480} \right\rceil = 7$



P_7	P_6	P_5	P_4	P_3	P_2	P_1	
1480+20	500	500	500	500	500	500	
(120)							
0	1	1	1	1	1	1	MF
960	480	0	offset				

480 → 1 byte

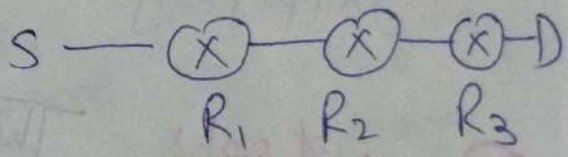
Options & Padding :-

Size : 0 – 40 bytes

Header range : 20 – 60 bytes

- If it is 20 bytes then options are not used.
- If it is 60 bytes then options can be used.

- Record Route



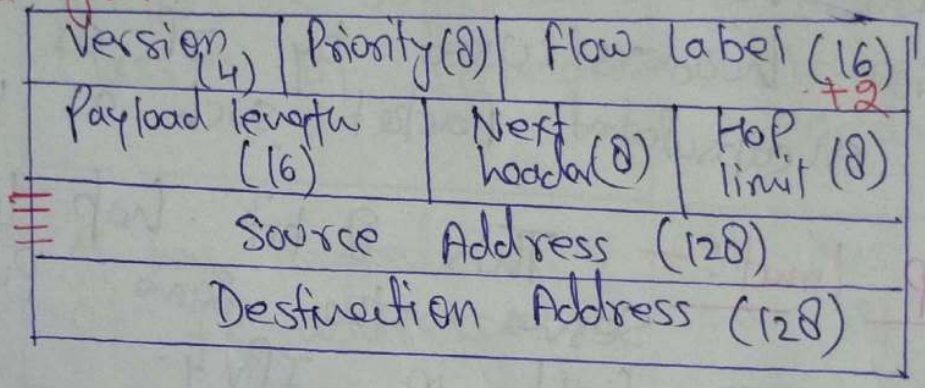
- Source Routing
  - ↳ Strict Source Routing
  - ↳ Loose Source Routing

} Source already explain route

- Padding
  - ↳ Header size should be in form of multiple of 2 so in situation extra bit can be added.

IPv6 (4)

- Requirement (IOT, more devices)
- Address 128 bit = 2^{128} addresses
- Larger Address space
- Better header format
- Support for more security.
- Data gram Service



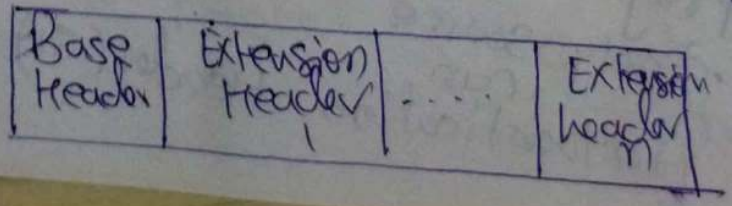
(1) Version (4bit) = 0110, Define the version no. of the IP.

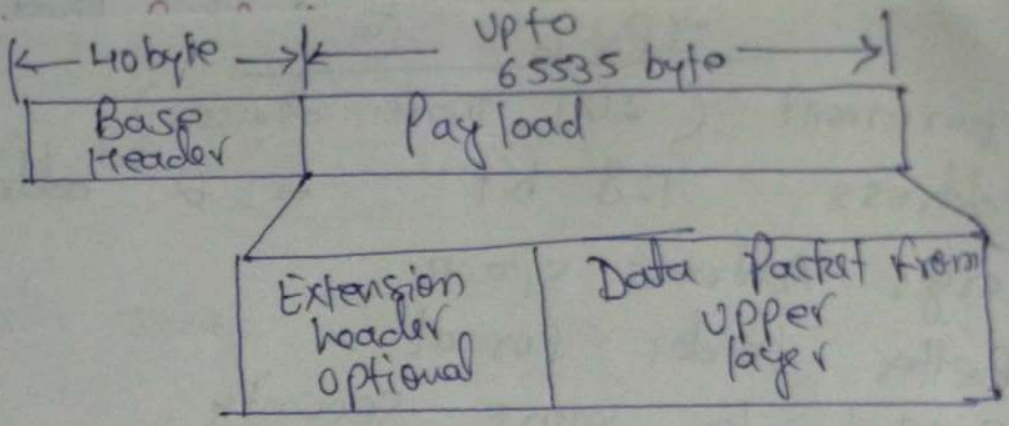
(2) Priority → Defines the Priority of the Packet with respect to traffic congestion.

(3) Flow label (16 bit) → It is designed to Provide special handling for a Particular flow of Data. (Virtual Circuit) (Reservation)

(4) Pay load length:- It defines the length of the IP data gram excluding the header. 2^{16} = 65535 byte.

(5) Next Header:- Base Header = 40 Bytes





The next header is either one of the optional extension headers used by IP or the header of an encapsulated Packet such as UDP or TCP.

(6) Hop limit:- This 8 bit hop limit field servos the same purpose as the TTL field in IPV4.

(7) Source Address:- Identifies the original source of the datagram.

(8) Destination:- Identifies the final destination of the datagram.

Extension Headers:

(1) Routing Header
(2) Hop by Hop (0)
(3) Fragment Header (44)
→ only source can.
(4) Authentication Header (51)
(5) Destination options (60)
(6) Encapsulating security.

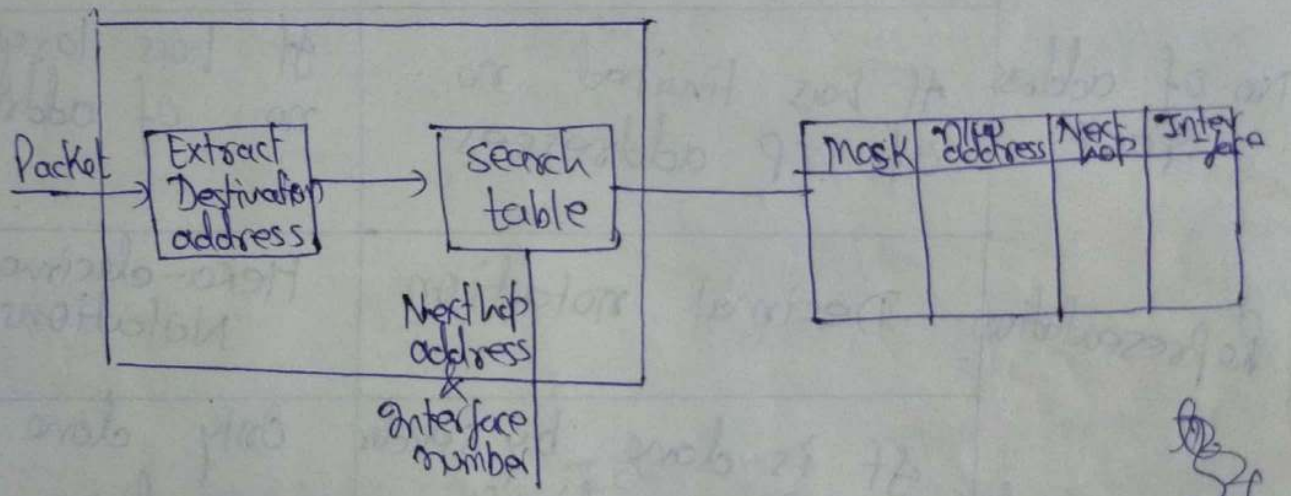
Comparision b/w IPv4 & IPv6 (5)

	IPV4	IPV6
Address length	IPv4 is a 32 bit address.	IPV6 is a 128 bit address.
Classes	It has 5 different classes of IP address	It does not contain IP addresses.
No of address space	It has limited no. of IP addresses	It has large no. of addresses
Representation	Decimal notation	Hexa-decimal Notations.
fragmentation	It is done by sender & forwarding routers.	Only done by senders.
Transmission	IPV4 is Broad-Casting	IPV6 is multicasting
security	It does not Provide encryption & Authantication	It Provides Encryption
No. of Octets	It consist of 4 Octets.	It consists of 8 fields & each contains 2 octets.

upto .1

Routing Protocols

- Forwarding refers to the way a Packet is delivered to the next station.
- Routing refers to the way routing tables are created to help in forwarding.
- Routing Protocols are used to continuously update the routing tables that are consulted for forwarding & Routing.



Forwarding Process in Classless

Routing Protocols

- Intra domain
  - Distance Vector routing Protocol (Information)
  - Link State (OSPF) Open shortest Path First
- Inter domain
  - Path vector (Border Gateway Protocol)

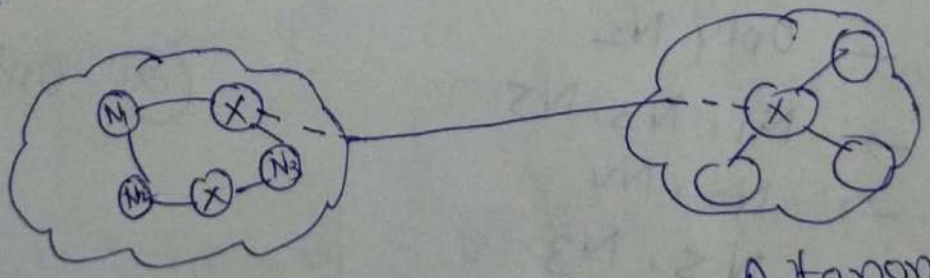
Unicasting (60)

Routing table: ⓐ A host or router has a routing table with an entry for each destination or combination of destinations to route IP Packets. It can be either static or Dynamic.

- static → entered manually
- Dynamic → updated Periodically by using Protocols such as RIP, OSPF, or BGP.

- Internet is divided into Autonomous systems. An Autonomous System is a group of networks & routers under the authority of single administration. Routing inside an autonomous System is referred to as intradomain routing.

Routing between autonomous system is referred to as interdomain Routing.



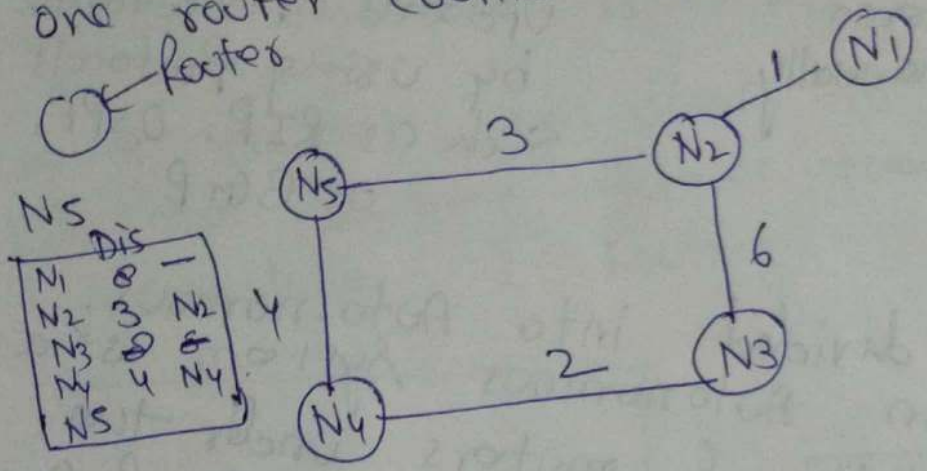
Autonomous System

Autonomous System

Distance Vector Routing:-

A DVR protocol in data networks determines the best route for data packets based on distance. It measures the distance by the no of routers a packet has to pass, one router counts as one hop.

router



N_1 table's

Dest	Dist	Next
N_1	0	N_1
N_2	1	N_2
N_3	∞	—
N_4	∞	—
N_5	∞	—

N_5

	Dis	
N_1	∞	—
N_2	3	N_2
N_3	∞	—
N_4	4	N_4
N_5		

N_2's table

	Dis	
N_1	1	N_1
N_2	0	N_2
N_3	6	N_3
N_4	∞	—
N_5	3	N_5

N_3

	Dis	
N_1	∞	—
N_2	6	N_2
N_3	0	N_3
N_4	2	N_4
N_5	∞	—

N_4

	Dis	
N_1	∞	—
N_2	∞	—
N_3	2	N_3
N_4	0	N_4
N_5	4	N_5

(1) share with only Neighbor

(2) Only Distance vector share.

At N_1 → Only N_2
At N_2 → N_1, N_3, N_5
At N_3 → N_2, N_4
At N_4 → N_5, N_3
At N_5 → N_2, N_4

At N_1 → N_2

1
0
6
∞
3

new table

$N_1 \rightarrow N_2$ & $N_2 \rightarrow N_4$

N_1's new table.

Dest	Dis	Next
N_1	0	N_1
N_2	1	N_2
N_3	1+6=7	N_3
N_4	∞	—
N_5	1+3	N_5

Link State Routing Protocol:—

Link state Routing is a technique in which each router shares the knowledge of its neighborhood with every other router in the internetwork.

Keys to understand the Algorithm:—

In link state routing, four sets of actions are required to ensure that each node has the routing table showing least cost node to every other node.

(1) Creation of the states of the link by each node called link state Packet.

(2) Dissemination of LSP to every other router called flooding in an efficient & reliable way.

(3) Formation of a shortest Path tree for each node (Dijkstra Algorithm)

(4) Calculation of routing table based on the shortest Path tree.

At $N_5 \rightarrow N_2, N_4$ (1)

N_2
1
0
6
∞
3

N_4
∞
8
2
0
4

N_5 new table

N_1	4	N_2
N_2	3	N_2
N_3	6	N_4
N_4	4	N_4
N_5	0	N_5

$3+1=4$

$N_5 \rightarrow N_4$ & $N_4 \rightarrow N_4$

$N_5 \rightarrow N_2$ & $N_2 \rightarrow N_4$

$N_5 \xrightarrow{3} N_2 \rightarrow N_1$ ← distance vector

or

$N_5 \rightarrow N_4 \rightarrow N_1 \rightarrow 8$

$N_5 \rightarrow N_2 \not\rightarrow N_2 \rightarrow N_2$

$3 \quad \& \quad 0 \quad = \quad 3$

Algorithm: (1) A router transmits its distance vector to each of its neighbours in a routing packet.

(2) Each router receives & saves the most recently received distance vector from each of its neighbours.

(3) A router recalculates its distance vector when:

(1) It receives a distance vector from a neighbour containing different information than before.

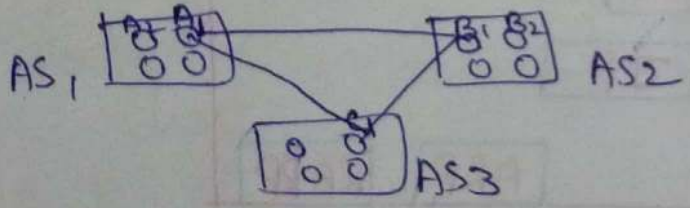
(2) It discovers that a link to a neighbor has gone down.

Link State Routing :-

- It is a method in which each router shares its neighbourhood's knowledge with every other router in the internetwork.
- It uses link state routers to exchange messages that allows each router to learn the entire ~~knowledge~~ network Topology. Based on this, each router is then able to compute its routing table by using the shortest Path computation.

Path Vector (Inter domain):

- It is an exterior routing Protocol proved to be useful for inter-domain.
- In this routing, a router has list of N/ws that can be reached with the Path to reach each one.
- As the name suggest it tells us the Paths.



A_1 → speaker node
B_1 → speaker node
C_1 → speaker node.

Each speaker node maintains its routing table.

AS1 → A_1 table.

Dest	Path
A1	AS1
A2	AS1
A3	AS1
A4	AS1

routing table → AS1 ⟶ AS

A1 tables.

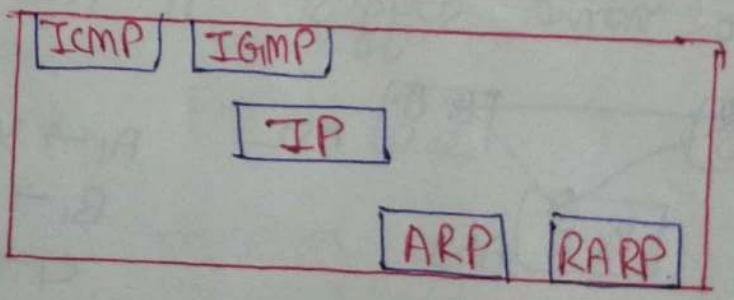
Dest	Path
A1	AS1
A4	AS1
B1	AS1 – AS2
.	

Address Resolution Protocol (ARP)

- ARP is a Communication Protocol used to find the MAC address of a device from its IP address. This Protocol is used when a device wants to communicate with another device on a LAN or Ethernet.
- Most of the Computer use logical address (IP) to send / receive messages, however, the actual communication happens over the physical address (MAC address).

IP ⟶ [ARP] ⟶ MAC Address

N/w layer Protocol:

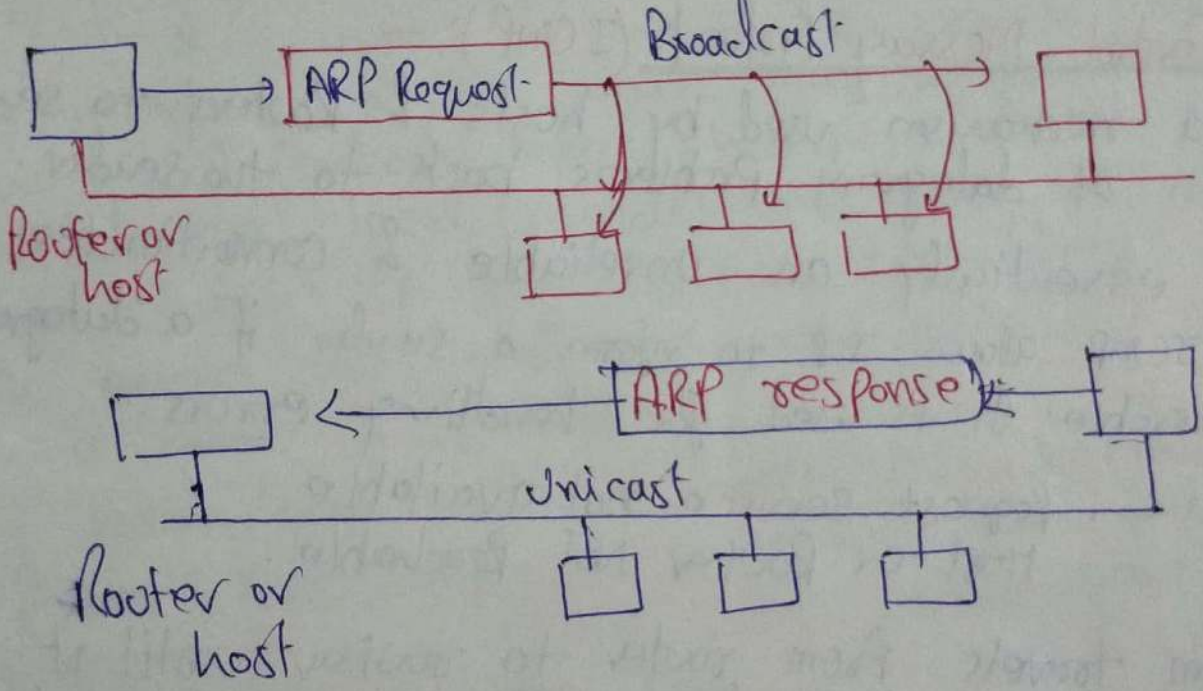


When one host wants to communicate with another host on the network, It needs to resolve the IP address of each host to the host hardware address.

- When a host tries to interact with another host, an ARP request is initiated. If the IP address is for the local n/w, the source host checks its ARP cache to find out the hardware address of the destination.
- If the correspondence hardware address is not found, ARP broadcasts the request to all the local hosts.

• All host receive the broadcast & check their own IP address. If no match is discovered the request is ignored.

• The destination host that finds the matching IP address sends an ARP reply to the source host along with its H/w address thus establishing the communication. The ARP cache is then updated with the hardware address of the destination host.



ARP header →

Ethernet etc Hardware Type	Protocol Type (IPV4, IPV6)
Hardware Length MAC Length	Protocol length / Operations Request-1, Reply-2
Sender H/w address (6 Byte)	
Sender Protocol Address (4B for IP)	
Target H/w address	
Target Protocol Address	

Reverse Address Resolution Protocol: It allows a host to discover its Internet address when it knows only its Physical address.

- The host wishing to retrieve its Internet address broadcasts an RARP query packet that contains its Physical address to every host on its Physical n/w. A server on the network recognizes the RARP packet & returns the host's Internet address.

Internet Control Message Protocol (ICMP):-

- ICMP is a mechanism used by hosts & Routers to send notification of datagram Problems back to the sender.
- IP is essentially an unreliable & connectionless Protocol. ICMP allows IP to inform a sender if a datagram is undeliverable. It is used for handling errors.
- Messages:-
  - Request service not available
  - Host or Router Not Reachable.

A datagram travels from router to router until it reaches to its final destination. If a router is unable to route or deliver the datagram because of congestion, ICMP allows it to inform the original source. It sole function is to report Problems not correct them.

Internet Group Management Protocol (IGMP) →

It has been designed to help a multicast router identify the hosts in a LAN that are members of a multicast group. It manages the membership of hosts & routing devices in multicast groups. IGMP allows devices to join a multicast group.

Network Address Translation :-

To access Internet, one Public address is needed, but we can use a Private IP address in our Private network. The idea of NAT is to allow multiple devices to access the Internet through a single Public address. To achieve this the translation of a Private IP address to a Public IP is required.

- **Working** → Generally the border router is configured for NAT, the router which has one interface in the local n/w & one interface in the global (outside) n/w. When a packet traverse outside the local (inside) n/w, then NAT converts that local IP to Global IP address. When Pkt enters the local n/w, the global IP is converted to a local IP address.

If NAT runs out of addresses, no address is left in pool configuration then packet will be dropped & an ICMP host unreachable Pkt to the destination is sent.

Mask Port no! Two Host A & B request for the same destination, on same Port no, on the host side, at same time. If NAT only does translation of IP addresses then both of their IP would be masked by Public IP address of the router, Thus receiving a reply, it will be unclear to NAT as to which reply belongs to which host, so Avoid this problem, NAT masks the source Port no. as well as makes an entry in the NAT table.

NAT inside & outside:- Inside refers to the addresses which must be translated, outside refers to the addresses which are not in control of an organization.

Advantages:
- NAT conserves legally registered IP addresses.
- It Provides Privacy as the device's IP address, sending & receiving the traffic, will be hidden.
- Eliminates address renumbering when a network envolves.

Disadvantages:
- Translation results in switching Path delays.
- Certain applications will not function while NAT is enabled.