Unit - 2

IPv4 :-

IPv4 is a 32 bit addressing which is used in the IP layer layer of TCP/IP protocol suite. IPv4 stands for Internet Protocol Version 4. It is a addres that uniquely identifies the connection of a host or router to the internet.

IPv4 provides hierarchical addressing scheme which enables it to divide the network into sub-networks, each with well defined number of hosts.

Parts of IPv4 :-

(a) Network Part :- It indicates the distinctive variety that's appointed to network.

(b) Host part :- It uniquely identifies the machines of our networks. This part of IPv4 is assigned to every host. For each host, network Id is same, but the host Id is different.

(c) Subnet number :- This is nonobligatory part of IPv4. Local network have massive numbers of host which are divided into subnets and subnet number is assigned to them.

* IPv4 is universal in the sense that the addressing system must be accepted by any host that wants to connected to the Internet. That means global addressing.

Address Space :-

A protocol like IPv4 that defines addresses has an address space. An address space is the total number of addresses used by the protocol. If a protocol uses N bit to define the address, the address space is 2^N. IPv4 uses 32 bits, which means address space of IPv4 is 2^{32} or 4,294,967,296 (more than 4 billion). So, Theoritically if there is no restrictions, more than 4 billion devices could be connected to Internet.

Notations to show IPv4 address :-

Following are the three common notations to show an IPv4 address :-

(i) Binary Notation :-

In Binary Notation, the IPv4 address is displayed as 32 bits. Each octate is often reffered to as byte. So, it is common to hear IPv4 address referred to a 4-byte address. The following is example of an IPv4 address in binary notation :-

01110011 : 10010101 00000001 00000000

(ii) Dotted Decimal Notation :-

IPv4 is usually written in decimal form with a decimal point (dot) separating the bytes since it is more compatible.

Example :-

51.149.1.0 (Same as address in Binary Notation)

Each number in dotted decimal notation is a value ranging from 0 to 255.

(iii) Hexadecimal Notation :-

We sometimes see an IPv4 address in hexadecimal notation. Each hexadecimal digit is equivalent to 4 bits. This means 32 bit address has 8 hexadecimal digits. It is often used in network programming.

Example :-

10000001 00001011 00001011 11101111

↓

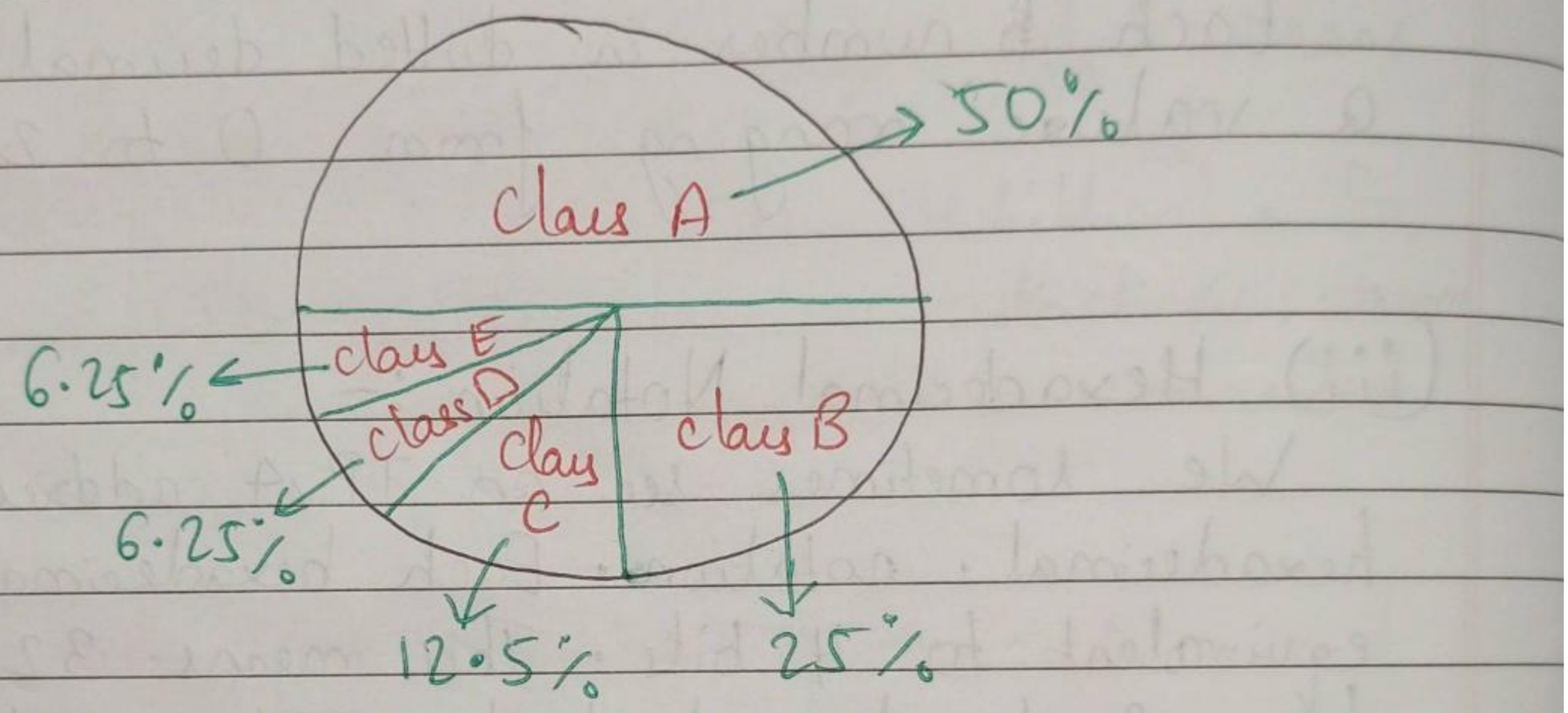
0X810B0BEF or $(810B0BEF)_{16}$

Classful Addressing

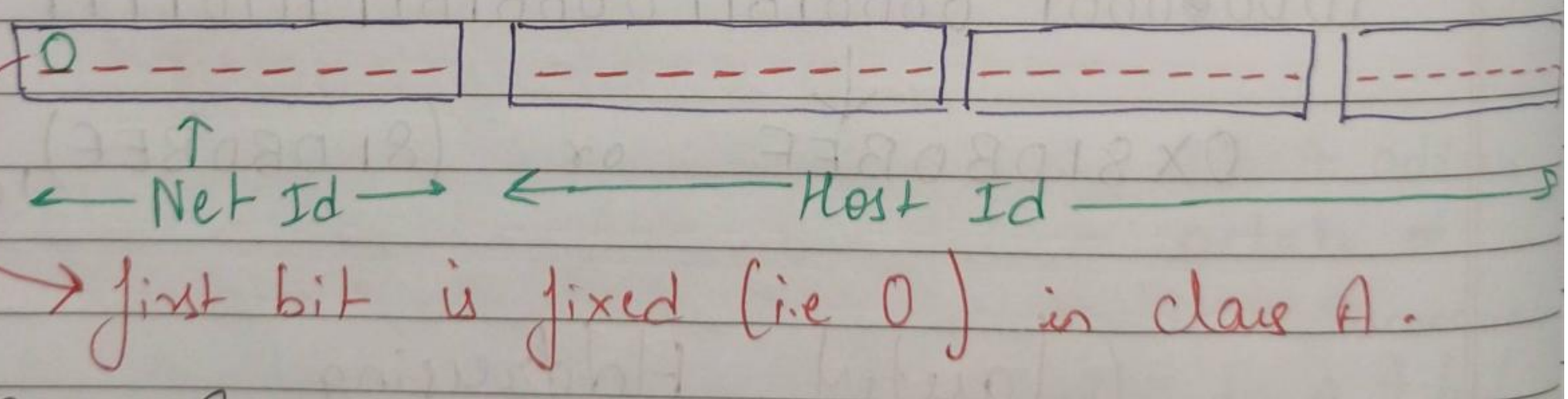
IP addresses when started a few decades ago used the concept of classes. This architecture is called classful addressing. In mid 1990s, a new architecture called classless addressing was introduced that supersedes the original architecture.

Classes :-

In classful addressing, the IP address is divided into five classes : A, B, C, D, and E. Each class occupy some parts of whole address space.



Class A :-



→ first bit is fixed (i.e 0) in class A.

→ Posible Range = 0 0000000 to 0 1111111 → 0 to 127.
(fixed)

→ Usefull range = 1 to 126.

→ No. of Network posible = 2^7 = 128

→ No. of usefull Network posible = $2^7 - 2$ = 126

→ Host Id possible :- 2^{24}
→ Host Id usefull :- $2^{24} - 2$

Total no. of IP address :- 2^{31}

Note :- When no. class is mentioned in Question, then total no. of IP possible = 2^{32}.

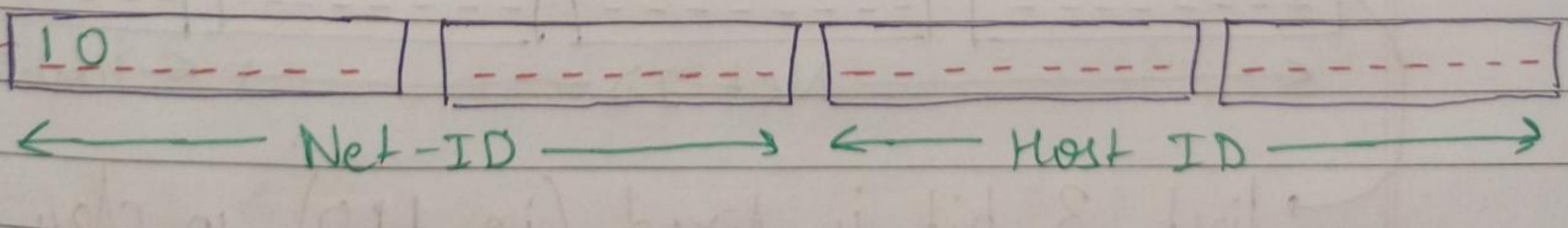
class A :- [0.0.0.0 — to — 127.0.0.0 / 0.255.255.255 — 127.255.255.255]

128 block ⇒ each block have 2^{24} address

16,777,216.

∴ Since each block contain 16777216 addresses many addresses are wasted in class A.

Class B :-



→ first 2 bit is fixed (i.e 10) in class B.

→ Possible Range = 10000000 → 128
fixed ← 10111111 → 191

→ Usefull range = 129 - 190

→ No. of Network possible = 2^{14}
→ No. of usefull network = $2^{14} - 2$

→ No. of Host possible = 2^{16}
→ No. of usefull host = $2^{16} - 2$

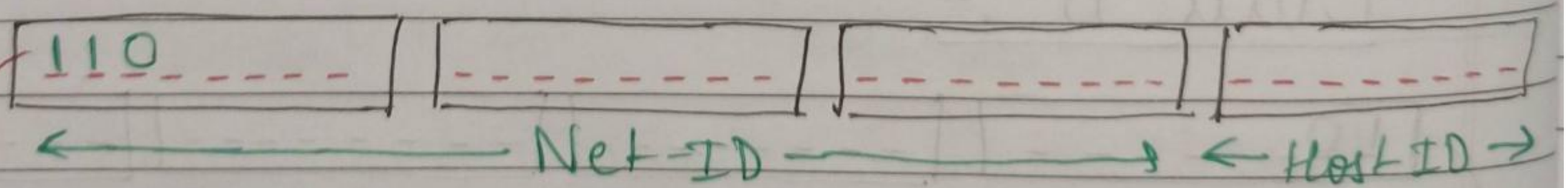
→ Total No. of IP possible = 2^{30}.

Class B :- 128.0.0.0 --- 191.255.255.255 -- to -- 191.0.0.0 --- 191.255.255.255

2^{14} Block, Each block has 2^{16} address

∴ Since there are 16384 block and each block has 65536 addresses, many addresses are wasted in class B.

Class C :-



→ first 3 bit is fixed (ie 110) in class C.

→ Possible range :- 11 0 00000 → 192 to 223
fixed ← 11 0 11111

→ usefull range :- 193 - 222

→ No. of Network possible = 2^{21}
→ No. of usefull network = $2^{21} - 2$

→ No. of host possible = 2^8
→ No. of usefull ~~net~~ host = $2^8 - 2$

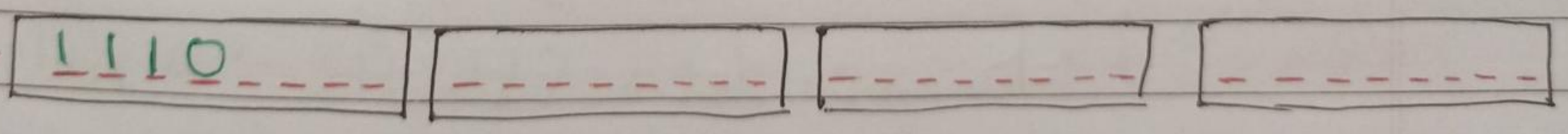
→ Total number of ID possible = 2^{29}

class C :- 192.0.0.0 — — 192.0.0.255 -- to -- 223.255.255.0 — — 223.255.255.255

2^{21} block, each block have 2^8 addres.
(2097152) (256)

* Each block contain 256 addresses. However not so much organization is as small as to be satisfied with class C block.

Class D :-

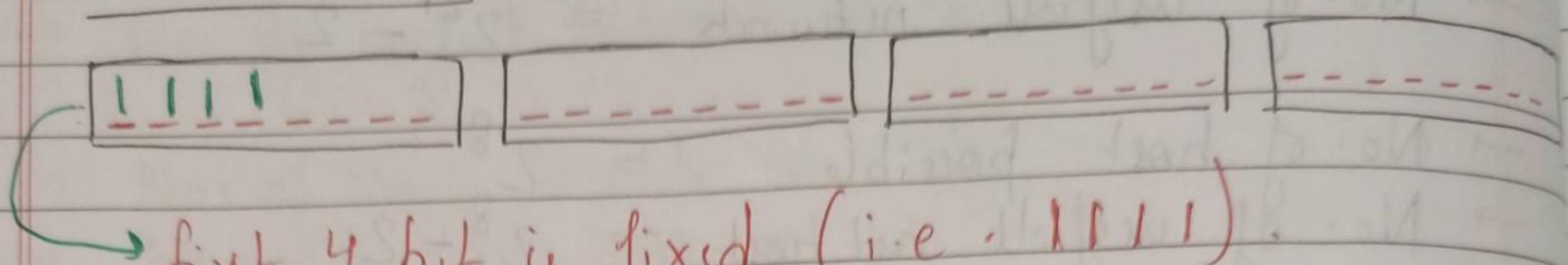


→ first 4 bit are fixed (i.e. 1110).

* It is designed for multicasting. It is mostly used in defence.

Total No. of Network possible = 2^{28}.

Class E :-



→ first 4 bit is fixed (i.e. 1111).

* It was designed for use as reserved addresses.

No. of Network possible = 2^{28}.

following Table Sumarise these clause :-

↓

CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

Recognizing Class :-

(a) Binary Notation :-

Check Bits (fixed bits) to recognize.

Class A :- [0 _ _ _ _ _ _] [ ] [ ] [ ]

Class B :- [1 0 _ _ _ _ _ _] [ ] [ ] [ ]

Class C :- [1 1 0 _ _ _ _ _] [ ] [ ] [ ]

Class D :- [1 1 1 0 _ _ _ _] [ ] [ ] [ ]

Class E :- [1 1 1 1 _ _ _ _] [ ] [ ] [ ]

(b) Dotted Decimal Notation :-

Check range wise. Value of first byte give class of address.

Class A :- [0 - 127] . [ ] . [ ] . [ ]

Class B :- [128 - 191] . [ ] . [ ] . [ ]

Class C :- [192 - 223] . [ ] . [ ] . [ ]

Class D :- [224 - 239] . [ ] . [ ] . [ ]

Class E :- [240 - 255] . [ ] . [ ] . [ ]

Subnet Mask :-

A subnet mask is a 32 bit number that mask an IP address and divides the IP address into network address and host address. Subnet mask is made by setting network bits to all '1' and setting host bit to all '0'.

Class A :- 11111111 00000000. 00000000 00000000

Network bit — Host bit

⇒ 255.0.0.0

Class B :- 11111111 . 11111111 00000000 00000000

Network bit — Host bit

⇒ 255.255.0.0

Class C :- 11111111 11111111 11111111 00000000

Network bit — Host bit

⇒ 255.255.255.0

* A subnet mask must be always a series of 1s followed by 0s.

Q. Calculate the network ID of 64.0.0.8.

Ans → * for MCQ :- for MCQ, just see the class and then get network ID by making all the host ID part = 0.

⇒ 64.0.0.0 in this question.

* for subjective Question :- for subjective question we will have to find it by doing AND operation on given ID & its subnet mask.

⇓

Sol → Given network ID = 64.0.0.8

64.0.0.8 = can be represented in binary as.

01000000.00000000 00000000 00001000

Since it belong to class A. So its

Subnet Mask = 255.0.0.0.

11111111.00000000 00000000 00000000

01000000 00000000 00000000 00001000

11111111 00000000 00000000 00000000

01000000 00000000 00000000 00000000

01000000 00000000 00000000 00000000

= 64.0.0.0.

So, Network ID = 64.0.0.0 Ans

Subnetting :-

When a bigger network is divided into smaller networks in order to maintain security, then that is known as subnetting. So maintainance is easier for smaller network.

Subnetting allows us to create multiple logical networks that exist without a single class A, B, C network. If we do not subnet we are only able to use one network from our class A, B, or C which is unrealistic.

In order to subnet a network, extend the natural mask with some of the bit from the host ID portion of address in order to creat a subnetwork ID. For example, given a class C network of 204.17.5.0 which has natural mask of 255.255.255.0, we can create subnet in this manner.

204.17.5.0 - 11001100.00001000.00000101.00000000

255.2558.255.224 - 11111111.11111111.11111111.11100000.

fixing 3 bit

Will make 2^3 subnets.

Divide a network into 2 subnets :-

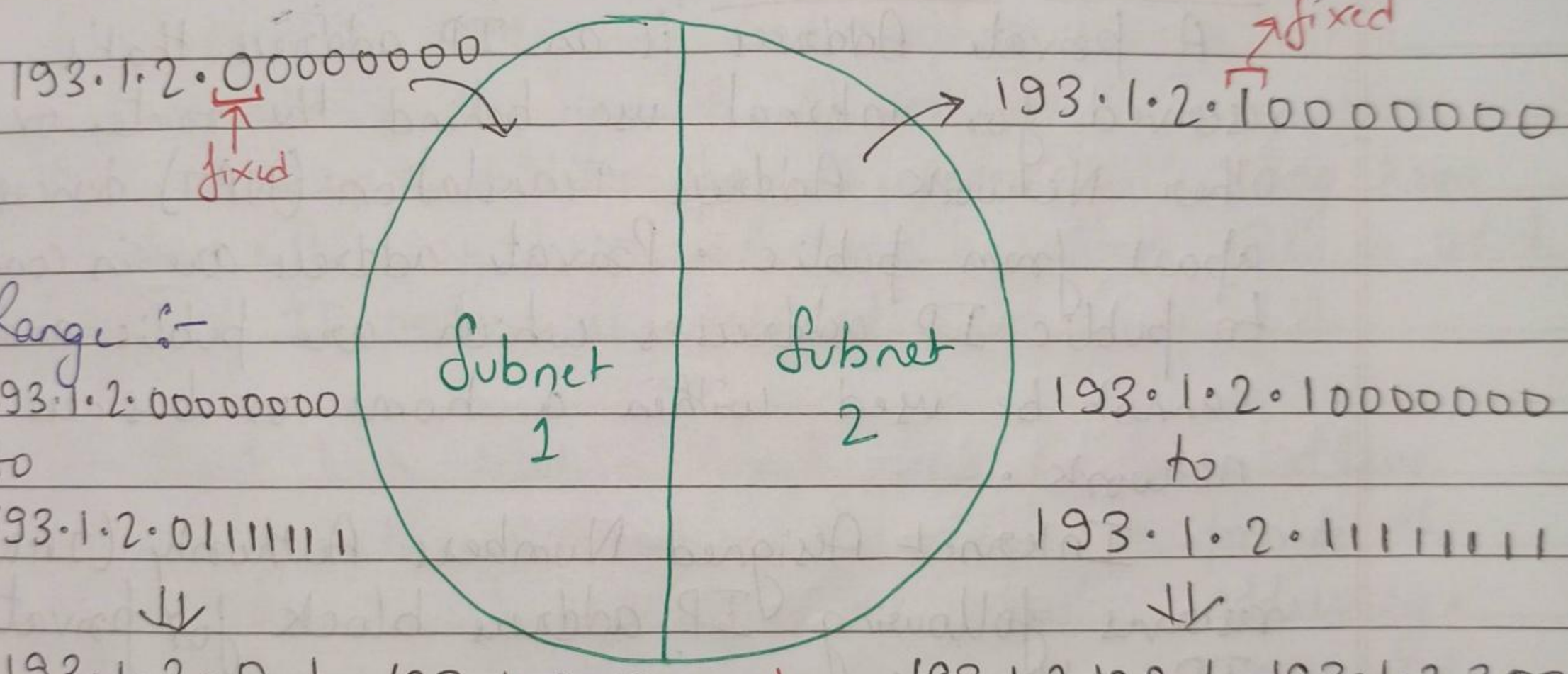
To divide a network into 2 parts, we need to choose one bit for each subnet from the host ID part.

for example :- for 193.1.2.0,

193.1.2.00000000

↑ Choose this bit [1st bit of host ID part].

Nid = 193.1.2.0



Range :-

193.1.2.00000000

to

193.1.2.01111111

⇓

193.1.2.0 to 193.1.2.127

⇓

No. of host possible = $2^7 = 128$

No. of usefull host = $2^7 - 2 = 126$

193.1.2.10000000

to

193.1.2.11111111

⇓

193.1.2.128 to 193.1.2.255

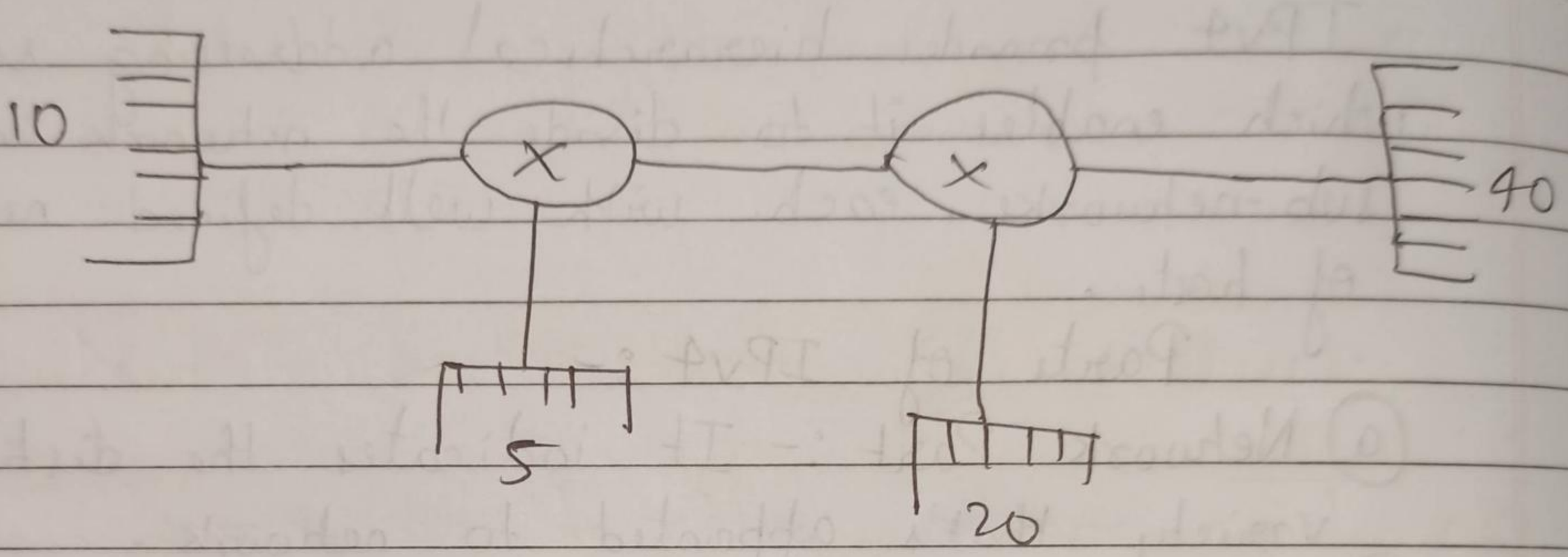
⇓

No. of possible host = $2^7 = 128$

No. of usefull host = $2^7 - 2$
= 126

*Not :- Similarly if we want to dinde into 4 subnet, then fix first 2^2 bit = 4 bit of host ID. i.e (01, 10, 00, 11)

To understand how subnetting is done and how we find subnet Id or subnet mask lets see an example.



Network Id = 197.10.10.0

Step 1 :- Given address = 197.10.10.0

Step 2 :- 11000101.00001010.00001010.00000000

Step 3 :- $2^n - 2 \geq 40$ ~~(fals~~

$n=1$ $2^1 - 2 \geq 40$ (false)

$n=2$ $2^2 - 2 \geq 40$ (false)

$n=3$ $2^3 - 2 \geq 40$ (false)

$n=4$ $2^4 - 2 \geq 40$ (false)

$n=5$ $2^5 - 2 \geq 40$ (false)

$n=6$ $2^6 - 2 \geq 40$ (true)

$\Rightarrow n = 6$

Step 4 :-

11000101 . 00001010 . 00001010 . 00000000
← 6 place

11000101 . 00001010 . 00001010 . 11000000

Step 5 :- 197 . 10 . 10 . 192 / 26 → CIDR.

Subnet Mask = ~~197 . 10 .~~
255 . 255 . 255 . 192.

Step 6 :-

first Subnet Id = 197 . 10 . 10 . 0 / 26.
2nd Subnet Id = 197 . 10 . 10 . 64 / 26
↓
(By adding 64 → 1st 1 from right value)

3rd Subnet Id = 197 . 10 . 10 . 128 / 26
4th Subnet Id = 197 . 10 . 10 . 184 / 26
5th Subnet Id = 197 . 10 . 11 . 65 / 26.

1st Subnet's Broadcast Id = 197 . 10 . 10 . 63
2nd Subnet's Broadcast Id = 197 . 10 . 10 . 127
3rd Subnet's Broadcast Id = 197 . 10 . 10 . 183
4th Subnet's Broadcast Id = 197 . 10 . 11 . 64.

* Special Addresses :-

1) 169.254.0.0 - 169.254.0.16
   ⇒ Link-Local addresses

2) 127.0.0.0 - 127.0.0.8 ⇒ Loop-back address

3) 0.0.0.0 - 0.0.0.8 ⇒ used to communicate within the current network.

Privat Addresses :-

A privat Address is an IP address that's reserved for internal use behind the router or other Network Address Translation (NAT) devices, apart from public. Privat address are in contrast to public IP addresses which are public and cannot be used within a home or buisness network.

Internet Assigned Numbers Authority (IANA) reserves following IP address block for private IP address :-

1) 10.0.0.0 to 10.255.255.255
2) 172.16.0.0 to 172.31.255.255
3) 192.168.0.0 to 192.168.255.255

Not :- Another range of privat IP is 169.254.0.0 to 169.254.255.255 but those addresses are for Automic Privat IP Adressing (APIPA) use only.

Classless Addressing :-

Classless Addressing is an improved IP addressing system. It makes the allocation of IP Addressing more efficient. It was replaces the older classful addressing system based on classes. It is also known as classless Inter Domain Routing (CIDR).

Subneting and supernetting in classful addressing does not solve the address depletion problem and made the distribution of addressing and routing process more difficult. With the growth of internet, it was clear that a larger address space is needed as a long term solution. A long term solution is called IPv6 in which lenght of IP address is increased.

A short term solution which uses the same address but changes the distribution of address to provide the fair share is devised is called classless addressing. In other words, the class privilege was removed from distribution to compensate the address deplition.

Rules for classless Addressing :-

1) No. of IP address should be contigous.
2) No: of address in a Blocks should be in power of 2.
3) First address of subnet should be divisible by the block size.

→ No. of host

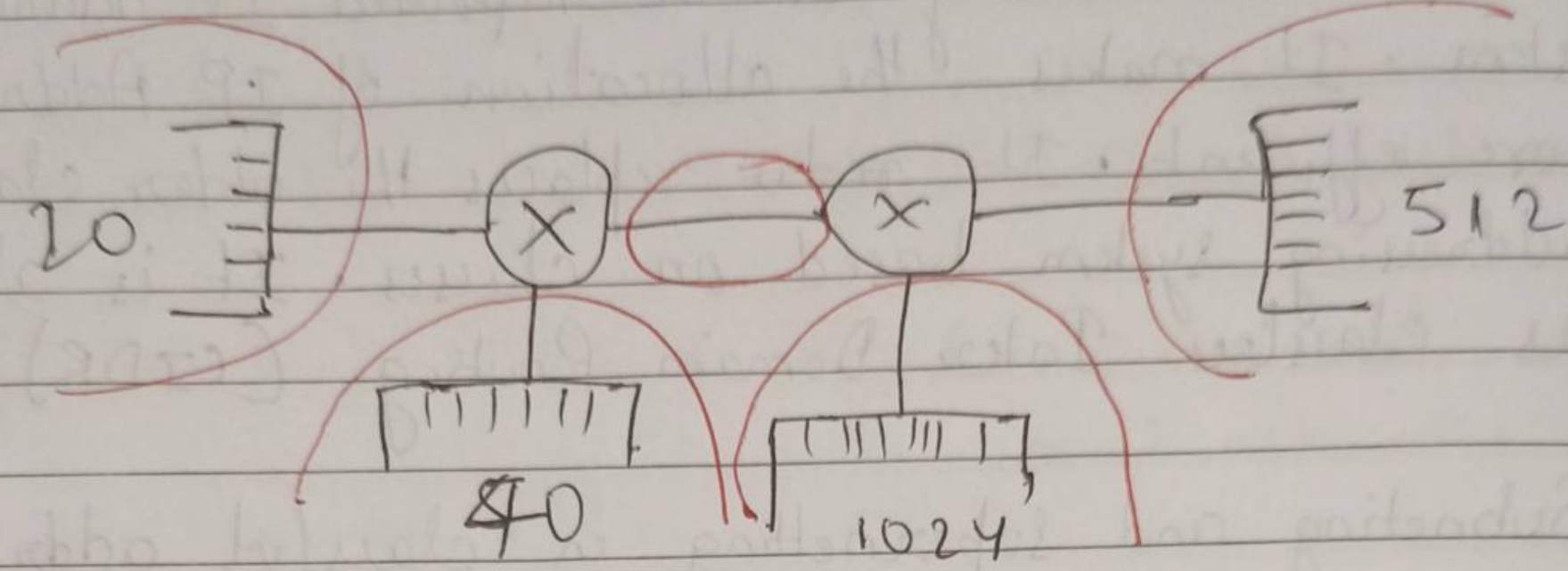
Example → 200.10.20.32 /28 → No. of host bit = 32 - 28 = 4

divisible by 16

So, Valid

No. of host ⇒ $2^4 = 16$

Now, lete see how we do subnetting in classless addressing with an example :-



Given ID = 12.0.0.0

Q1) How many subnet is required ?
⇒ 5 → See red color mark.

Q2) Now, do subnetting :-

Sol → Step 1 :-
Writ Given ID
⇒ 12.0.0.0

Step 2 :- Writ that in binary.
12.00000000.00000000.00000000

Step 3 :- check Condition to find n.

$2^n - 2 \geq 1024$

It is a major mistake point. Remember that it is $2^n - 2$. Dont made mistake with 2^n

$2^n - 2 \geq 1024$
$2^{11} - 2 \geq 1024$
⇒ n = 11

Step 4 :-

12.00000000.00000000.00000000

11 place ←

12.11111111.11111000.00000000

make 0 till this after that make all 1. [from right to left]

Step 5 :- 12.255.248.0 /21

Step 6 :- 12.255.248.0

Subnet mask = 255.0.0.0

1st Subnet ID = 12.255.248.0

AND operation = 225.0.0.0

12.0.0.0

12.11111111.11111000.00000000

255.00000000.00000000.00000000

12.00000000.00000000.00000000

⇒ 1st Subnet ID = 12.0.0.0

2nd Subnet ID :- 12.0.0.0

+ 8.0

12.0.8.0

[Remember: we add with the octate where 1 starts 2nd in this case]

3rd Subnet ID = 12.0.16.0

4th Subnet ID = 12.0.24.0

5th Subnet ID = 12.0.32.0

1st subnet Broadcast Id = 12.0.7.255
2nd subnet Broadcast ID = 12.0.15.255
3rd subnet Broadcast ID = 12.0.23.255

so on

Subnet Mask = 255.0.0.0

SuperNetting :-

↳ Also known as Prefix Aggregation & Route Aggregation.

Supernetting is about aggregating networks to form a ~~larger~~ larger network.

* The main purpose of supernetting is reducing the size of the routing table on routers. For example, instead of a router having 8 individual routes, it can have an aggrigated route of all these 8 individual routes.
* It saves memory and processing resources on routing devices. Basically they need less space to store their routing table and less processing power to search through the routing table.
* It provides stability on network because fluctuation in one part of network are not propagated to all part of network. i.e. fluctuations can be isolated.

Rules :-

1) IP's should be contigous in nature.
   i.e. 10.0.0.1, 10.0.0.2, 10.0.0.3, - - -
2) The size of all network ID should be same.
   ⇓
   i.e. class should be same.
3) The net ID should be divisible by number of host bits.

Lets see how we solve Supernetting Questions :-

Q1. Do Supernetting on
198.10.20.0/24
198.10.21.0/24.

Sol→ Step 1 :- Convert all into Binary.

198 → 11000110
10 → 00001010
20 → 00010100
21 → 00010101

I98.10.20.0 → 11000110.00001010.00010100.00000000
198.10.21.0 → 11000110.00001010.00010101.00000000

AND of these two → 11000110.00001010.00010100.00000000

← Net-ID → ← Host Id →

जहाँ से change हो रहा है, Whatever line h
↳ right to left

⇒ 198.10.20.0/23. Ans

Q.2 198.10.98.0 /24
198.10.99.0 /24
198.10.100.0 /24
198.10.101.0 /24
198.10.102.0 /24
198.10.103.0 /24.

Sol → 198 → 11000110
10 → 00001010
98 → 01100010
99 → 01100011
100 → 01100100
101 → 01100101
102 → 01100110
103 → 01100111

198.10.98.0 → 11000110.00001010.01100010.00000000
198.10.99.0 → 11000110.00001010.01100011.00000000
198.10.100.0 → 11000110.00001010.01100100.00000000
198.10.101.0 → 11000110.00001010.01100101.00000000
198.10.102.0 → 11000110.00001010.01100110.00000000
198.10.103.0 → 11000110.00001010.01100111.00000000

11000110.00001010.01100000.00000000
xxx xxxxxxxx

Yaha se change hua

⇒ 11000110.00001010.01100000.00000000
⇒ 198.10.96.0 /21

Ans

Q. Can 500 host be possible for
198.10.20.0 /24
198.10.21.0 /24.

Ans → No (without supernetting)

↓

2^8 possible host = 256 < 500

Yes (with supernetting)

↓

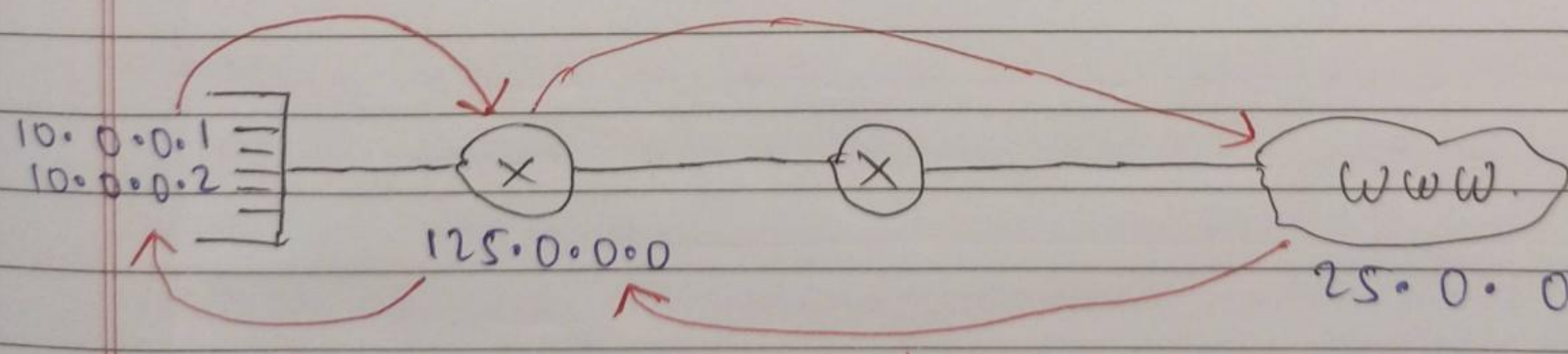
With supernetting as solved in Q.1, we get
198.10.20.0/23.

↓

2^9 host = 512 possible host > 500

Network Address Translation (NAT) :-

* It basically translates public addresses to private network and private network to public network.



During Sending	During Receiving
Source → 10.0.0.1	Source → 25.0.0.0
Destination → 25.0.0.0	Destination → 125.0.0.0
⇒ Though it will reach R_2. Still destination will be 25.0.0.0	⇒ After this Router will send to private net address of 10.0.0.1

Network Address Translation (NAT):-

To access the Internet, one public IP 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 private IP address to a public IP address is required. **Network Address Translation (NAT) is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts**. Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table. NAT generally operates on router or firewall.

Network Address Translation (NAT) Types –

There are 3 ways to configure NAT:

1. **Static NAT** – In this, a single unregistered (Private) IP address is mapped with a legally registered (Public) IP address i.e. one-to-one mapping between local and global address. This is generally used for Web hosting. These are not used in organizations as there are many devices who will need Internet access and to provide Internet access, the public IP address is needed.

Suppose, if there are 3000 devices who need access to the Internet, the organization have to buy 3000 public addresses that will be very costly.

2. **Dynamic NAT** – In this type of NAT, an unregistered IP address is translated into a registered (Public) IP address from a pool of public IP address. If the IP address of pool is not free, then the packet will be dropped as an only a fixed number of private IP address can be translated to public addresses.

Suppose, if there is a pool of 2 public IP addresses then only 2 private IP addresses can be translated at a given time. If 3rd private IP address wants to access Internet then the packet will be dropped therefore many private IP addresses are mapped to a pool of public IP addresses. NAT is used when the number of users who wants to access the Internet is fixed. This is also very costly as the organization have to buy many global IP addresses to make a pool.

3. **Port Address Translation (PAT)** – This is also known as NAT overload. In this, many local (private) IP addresses can be translated to a single registered IP address. Port numbers are used to distinguish the traffic i.e., which traffic belongs to which IP address. This is most frequently used as it is cost-effective as thousands of users can be connected to the Internet by using only one real global (public) IP address.

Advantages of NAT –

- NAT conserves legally registered IP addresses.
- It provides privacy as the device IP address, sending and receiving the traffic, will be hidden.
- Eliminates address renumbering when a network evolves.

Disadvantage of NAT –

- Translation results in switching path delays.
- Certain applications will not function while NAT is enabled.
- Complicates tunneling protocols such as IPsec.
- Also, router being a network layer device, should not tamper with port numbers (transport layer) but it has to do so because of NAT.

Hub, Repeaters, Switch and Bridge Structure of Router:-

1. Repeater – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.

2. Hub – A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, collision domain of all hosts connected through Hub remains one. Also, they do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.

Types of Hub

- **Active Hub:-** These are the hubs which have their own power supply and can clean, boost and relay the signal along with the network. It serves both as a repeater as well as wiring centre. These are used to extend the maximum distance between nodes.
- **Passive Hub :-** These are the hubs which collect wiring from nodes and power supply from active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend the distance between nodes.

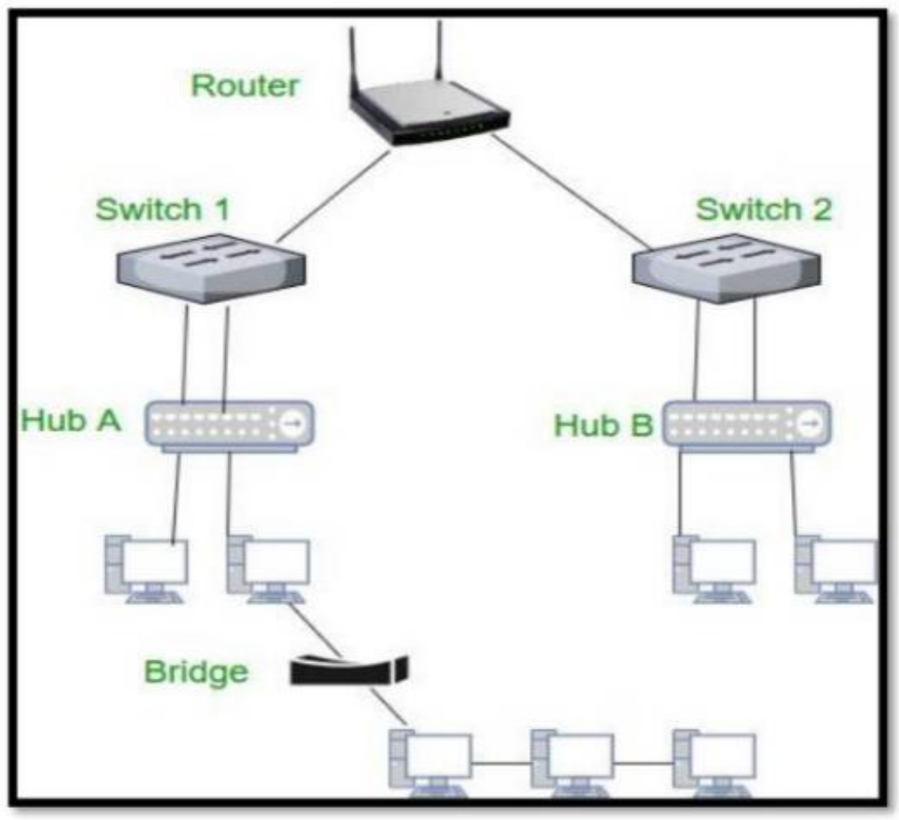
3. Bridge – A bridge operates at data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

Types of Bridges

- **Transparent Bridges:-** These are the bridge in which the stations are completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.
- **Source Routing Bridges:-** In these bridges, routing operation is performed by source station and the frame specifies which route to follow. The hot can discover frame by sending a special frame called discovery frame, which spreads through the entire network using all possible paths to destination.

4. Switch – A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only. In other words, switch divides collision domain of hosts, but broadcast domain remains same.

5. Routers – A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.



Differences between Hub and Switch:-

S.NO	HUB	SWITCH
1.	Hub is operated on **Physical layer**.	While switch is operated on **Data link layer**.
2.	Hub is a broadcast type transmission.	While switch is a Unicast, multicast and broadcast type transmission.
3.	Hub have maximum 4 ports.	While switch can have 24 to 28 ports.
4.	In hub, there is only one collision domain.	While in switch, different ports have own collision domain.
5.	Hub is a half duplex transmission mode.	While switch is a full duplex transmission mode.
6.	In hub, Packet filtering is not provided.	While in switch, Packet filtering is provided.
7.	Hub cannot be used as a repeater.	While switch can be used as a repeater.
8.	Hub is not an intelligent device hence it is comparatively inexpensive.	While switch is an intelligent device so it is expensive.
9.	Hub is simply old type of device and is not generally used.	While switch is very sophisticated device and widely used.

Differences between router and switch:

S.NO	ROUTER	SWITCH
1.	The main objective of router is to connect various networks simultaneously.	While the main objective of switch is to connect various devices simultaneously.
2.	It works in network layer.	While it works in data link later.
3.	Router is used by LAN as well as MAN.	While switch is used by only LAN.
4.	Through router data is sent in the form of packet.	While through switch data is sent in the form of packet and frame.
5.	It is a full duplex mode transmission.	It is also a full duplex mode transmission.
6.	There is less collision take place in router.	While there is no collision take place in full duplex switch.
7.	Router is compatible with NAT.	While it is not compatible with NAT.
8.	The types of routing are: Adaptive and Non-adaptive routing.	The types of switching are: Circuit, Packet and Message Switching.