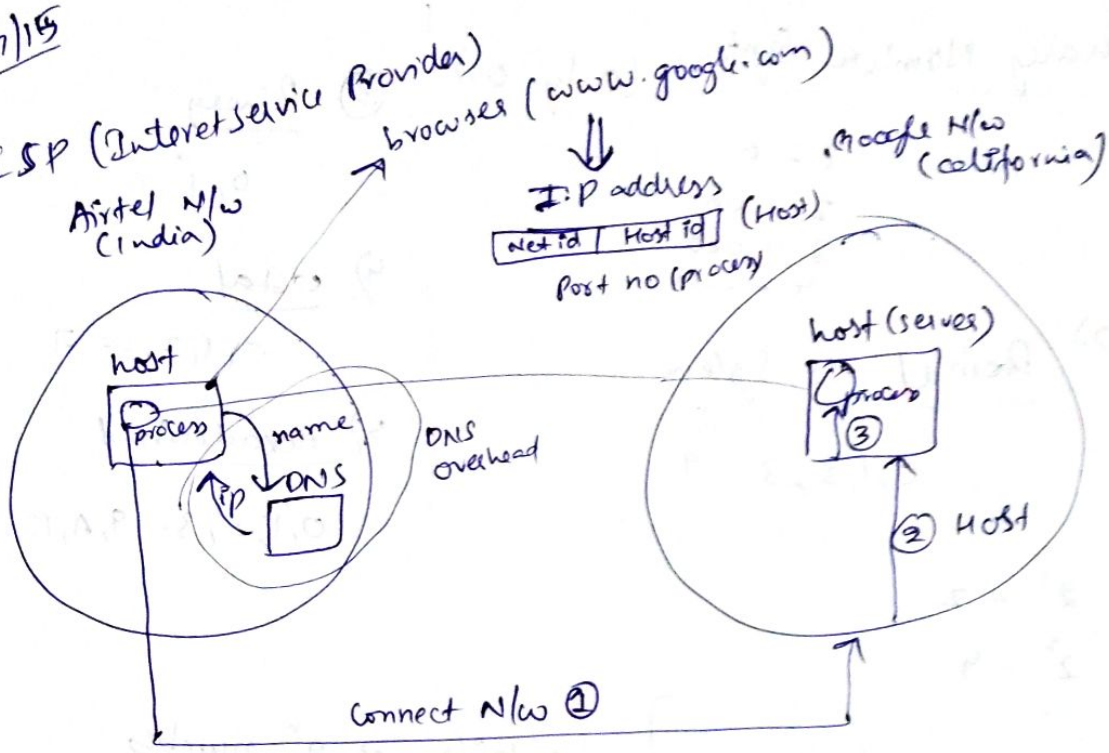
శ్రీరామరక్ష　　　　　　　　　　　　ఓం గం గణపతయే నమః

INDEX

NAME: ____________ STD.: ______ SEC.: ______ ROLL NO.: ______ SUB.: Computer Networks

S. No.	Date	Title	Page No.	Teacher's Sign / Remarks

25/7/15



www.google.com (domain Name)

↓

I.P address

| Net id | Host id | (To reach host)

↓

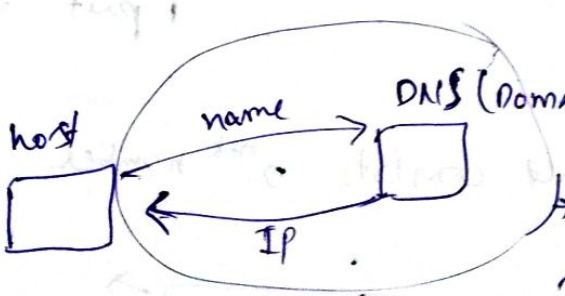
Port no (To reach process)

Port no

http – 80

FTP – 21

SMTP – 25



DNS overhead

⇓

It occurs only first time when we contact a server for first time

next stores in log & removes DNS overhead

log expires

⇓

again overhead

① Unary Number System (only 0's)

1 - 0
2 - 00
3 - 000
4 - 0000

② Decimal No System

0, 1, 2, 3 .. 9

③ Binary

0, 1

④ Octal

0, 1, 2, ... 7

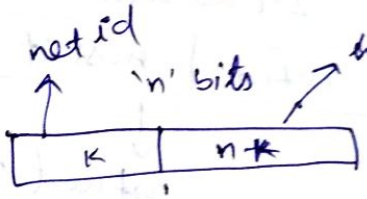
⑤ Hexadecimal

0, 1, 2, 3 .. 9, A, B, ...

$2^1 - 2$
$2^2 - 4$
.
.
$2^{10} = 1024 \ (K)$
$2^{20} - M$
$2^{30} - G$
$2^{40} - T$

n bits ⇒ 2^n numbers

ex:-
10 bits - 2^{10} numbers ...

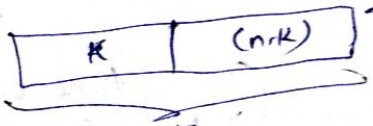


n bits ⇒ 2^n ⇒ 2^K parts - 2^n numbers

K bits = 2^K

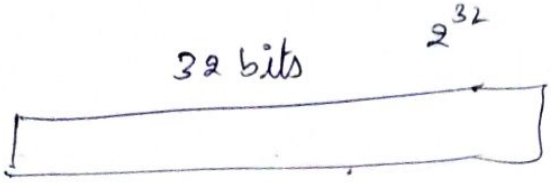
1 part = $\frac{2^n}{2^K} = 2^{n-K}$

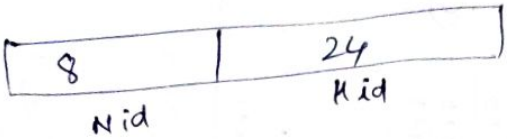
⇒ 1 part consists 2^{n-K} number



n bits - address
K bits - page offset

n bits - address
K - tag
n-K - block bits





$2^8 = 256$ $2^{24} = 16$ million

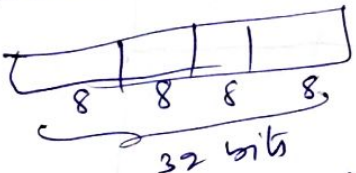
Bug 1-network ⇒ 16 million hosts

×

⇓ next

Classful Addressing

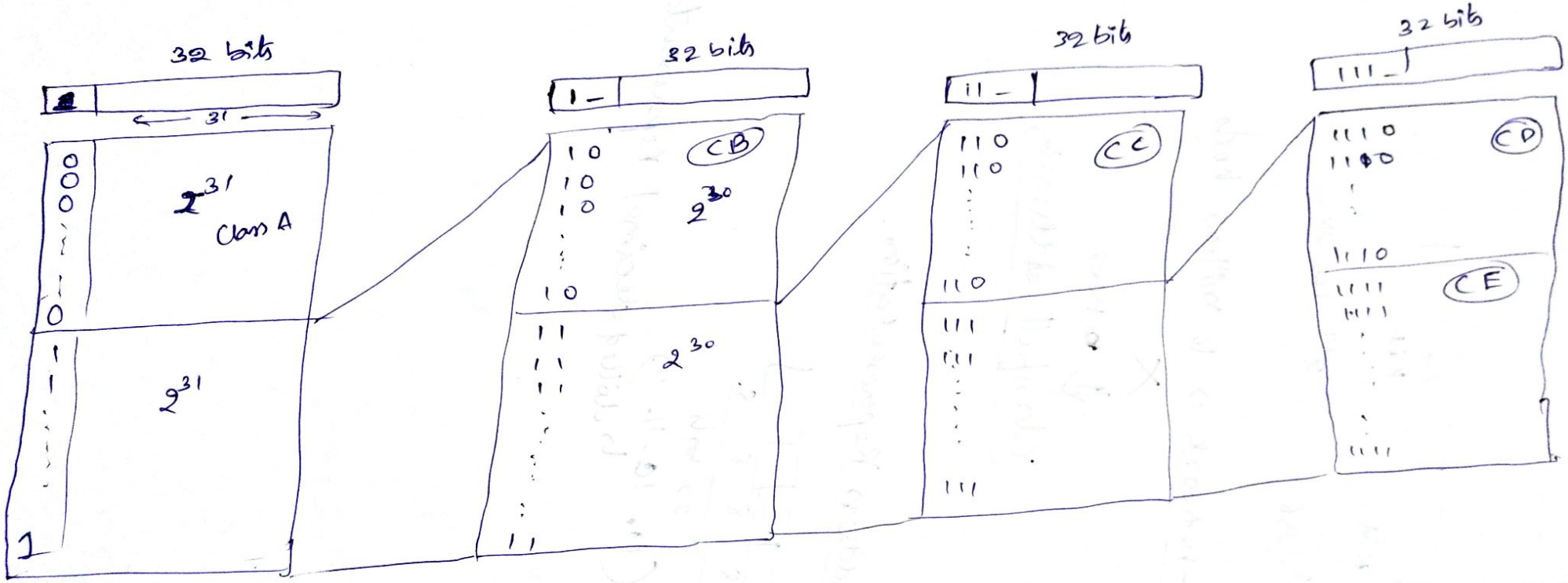
IP Address Representation:



(10.10.11.11)

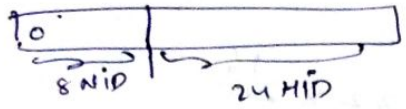
↳ dotted decimal Representation

Classfull Addressing



Class A:

1. No. of IP address = 2^{31}

2. 

$2^7 = 128$ N/w of CA

2^{24} ≈ 16 mil IP add

Range: (1-126)*

3) 0 - - - - - - -

0 0 0 0 0 0 0 - 0 *

0 0 0 0 0 0 1 - 1

0 0 0 0 0 1 0 - 2

- 126

Range

1 1 1 1 1 1 1 → 127 (seven one's ⇒ 127)*

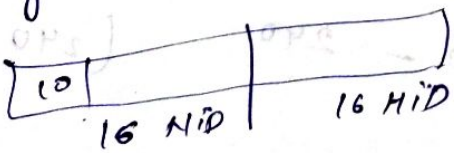
⇒ 128 n/w − 2 (0, 127) ⇒ 126 n/w

⇒ large n/w ⇒ Ex:- NASA, Pentagon etc

Class B:

1. no. of IP addrs = 2^{30}

Range .. 128-191



2^{14} = 16 K n/w of CB

2^{16} IP addrs = 64 K

10 0 0 0 0 0 0 - 128

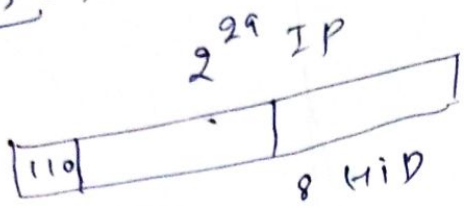
0 0 1 0 0 1 1 - 129

1 1 1 1 1 1 - 191

64 ⇒ 64×2^8 = 2^{14}

Ex:- IRCTC, SBI Bank

class C :-



2^{21} = 2mi. N/w $\equiv 32 \times 2^{16}$

2^8 = IIp add = 256 ipadd

Ex:- Engg Colleges etc

```
110 - - - - -
    0 0 0 0 0   - 192
    0 0 0 0 0   - 193      } 32
    0 0 0 0 0
    :
    1 1 1 1 1   - 223
```

192.0.0.1
192.0.1.1
192.1.0.1
:
192.255.1

class D:-

```
1110 - - - -   (224)    (224-239)  } multicast
    0 0 0 0
    :
    1 1 1 1    (239)
```

Route

class E:

```
1111 - - - -
    0 0 0 0  - 240      (240-255)  } Reserved
    :                              Ex:- military appln
    1 1 1 1  - 255
```

* we cannot configure all IP addresses in a network

Ex:- In 'A' we have 2^{24} host i/p add but we can configure only $2^{24}-2$ i/p address

Questions

class 'A'

total no. of i/p addresses possible = 2^{31}

no. of i/p add possible = 2^{24}

no. of hosts possible = $2^{24}-2$

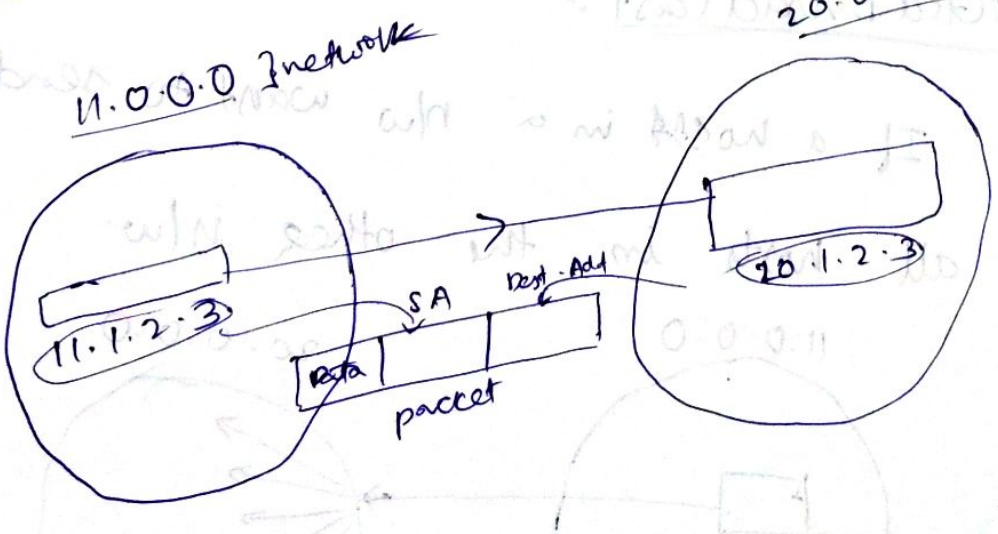
no. of n/w possible = 126

CASTING

Sending packet

Uni Cast :- sending packet from one host to another host

BroadCast :- one host to many hosts



8

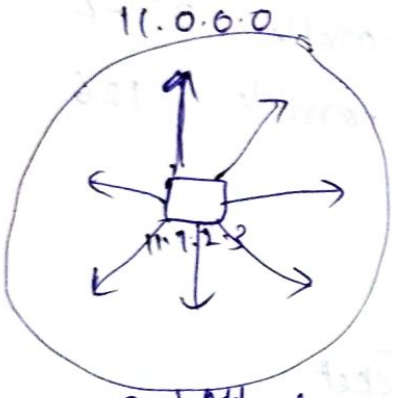
Broadcasting

Limited Broadcasting

Directed BC

Limited BC:

* If you want to send the packet to every in your network, then we use limited



	SA	DA
msg	11.1.2.3	255.255.255.255

* In Dest Add we fill 255.255.255.255 ⇒ limited B.C. Add

11111111.(1...1).(1...1).(1...1)

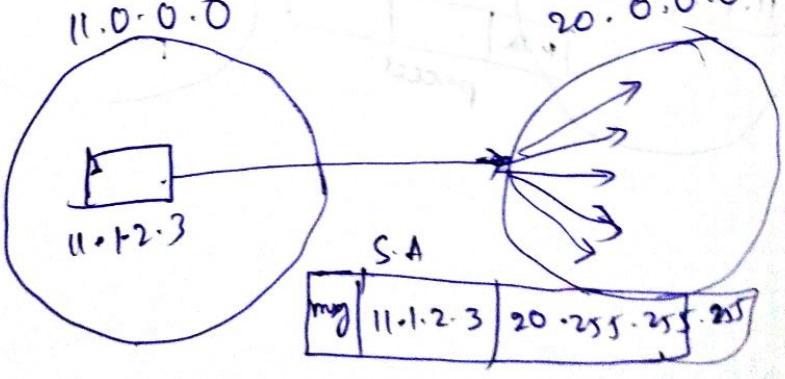
⇓

all 32 bits

Limited Broadcast add: 255.255.255.255

Directed Broadcast:-

If a host in a n/w want to send msg to all hosts in the other n/w



	S.A	
msg	11.1.2.3	20.255.255.255

Directed B.A : (Nid) . (Hid - all 1's)

Ex: (20 . 255 . 255 . 255)

Nid : (Nid) . (Hid - all 0's)

2^n ⇒ i/p adds possible

$2^n - 2$ ⇒ hosts possible

⇒ 2 (Directed B.A , net-id)

CA :- $2^{24} - 2$ hosts

CB : $(2^{16} - 2)$

CC : $(2^8 - 2)$

CA-(1-126) ; CB - (128-191) ; CC (192-223)
CD (224-240)

I-P	class	Net-id	Directed B.A	Limited B.A
1.2.3.4	'A'	1.0.0.0	1.255.255.255	255.255.255.255
10.15.20.60	A	10.0.0.0	10.255.255.255	255.255.255.255
130.1.2.3	B	130.1.0.0	130.1.255.255	255.255.255.255
150.0.150.150	B	150.0.0.0	150.0.255.255	255.255.255.255
200.1.10.100	C	200.0.10.0	200.0.10.255	255.255.255.255
220.15.1.10	C	220.15.1.0	220.15.1.255	255.255.255.255
250.0.1.2	E	250.0.0.0	250.255.255.255	255.255.255.255
300.1.2.3	X	X	X	X

Subnet-

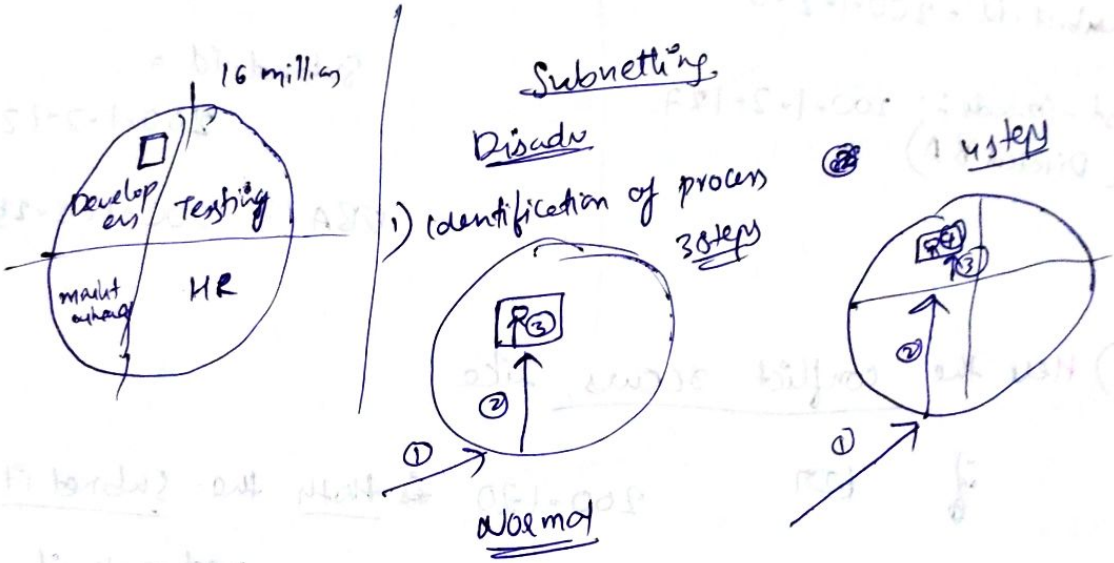
Sub-Nets, Sub-Net Mask, Routing

→ A very big n/w like → C'A' - 16 million hosts in a n/w

disadv:

1. maintainance
2. security

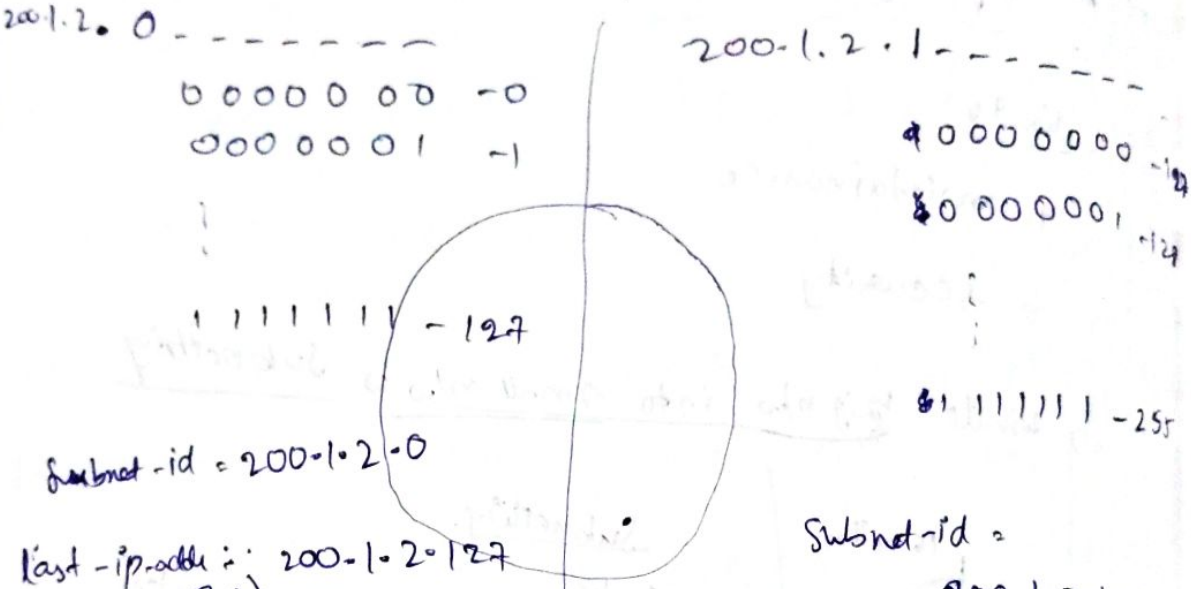
⇒ Divide big n/w into small n/w ⇒ Subnetting



Ex:

200.1.2.0

Divide into subnets



Subnet-id = 200.1.2.0

last-ip-addr : 200.1.2.127
(Directed BA)

Subnet-id = 200.1.2.127

DBA = 200.1.2.255

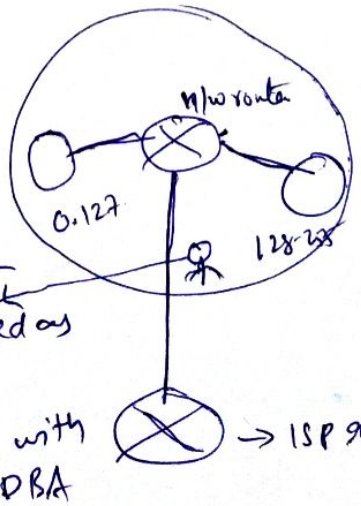
1) Here the conflict occurs, like

200.1.2.0 is both the subnet id & network id

and

200.1.2.255 → is both D.B.A of subnet & network

To resolve issue, it depends on perspective like



If you are inside n/w
200.1.2.0 is treated as
subnet-id & same with DBA

Q → if you are outside
200.1.2.0 is treated
as network-id
and same with
DBA

2)

at first ; 256 - 2 = 254

after subnets ; 128 - 2 = 126 × 2 = 252

Now Divide into four subnets

200.1.2.0

200.1.2.[00]------

00 (0-63)

200.1.2.00------

000000-0

000000-1

:

111111-63

200.1.2.0

200.1.2.63

(128-191)

200.1.2.00------

01------

10------

11------

10

200.1.2.[10]------

000000-128

:

111111-191

200.1.2.128

200.1.2.191

01

200.1.2.01------

000000-64

:

111111-127

(64-127)

200.1.2.64

200.1.2.127

11

200.1.2.11------

000000-192

:

111111-255

(192-255)

200.1.2.192

200.1.2.255

S_1 S_3 S_2 S_4

Subnet-Mask

? which subnet should pass packet

(0-63) (128-191) (64-127) (192-255)

Packet

Subnet-mask / Network Mask

1) It is a 32 bit address

2) 1's → Nid & Sid

   0's → Hid

Ex:

200.1.2.0 ⇒ four subnets ⇒ two bits are used for Subnetting

(200.1.2.0 — nid)

255 . 255 . 255 . 192

11111111 . 11111111 . 11111111 . 11000000

Subnet-mask ↳ Host-id part

Use of Sub-net Mask:

1) If we take subnet mask and bit wise "AND" with IP address, we get Sub-net id of the particular IP address

Ex:

200.1.2.130 (packet to be sent to)

11111111 . 11111111 . 11111111 . 11000000

(200.1.2.130) 11001000 . 00000001 . 00000010 . 10000010

11001000 . 00000001 . 00000010 . 10000000

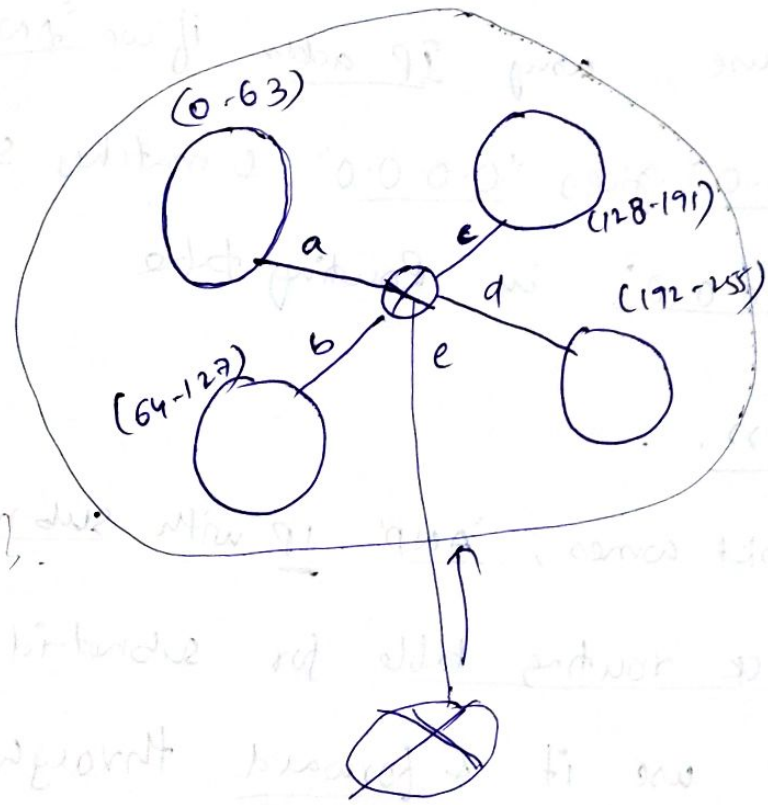
200 . 1 . 2 . 128

⇓

Sub net-id of IP-address

1. By using sub-net mask router forwards packet to appropriate sub-net

Router maintains routing table to send pkt to appropriate host interface



Routing table

Nid	Subnet-mask	Interface
200.1.2.0	255.255.255.192	a
200.1.2.64	"	b
200.1.2.128	"	c
200.1.2.192	"	d
0.0.0.0	0.0.0.0	e

default entry ← 0.0.0.0

→ If the packet does not match with any of the n/w interfaces connected to sub-nets, then it will be sent-out (default entry)
(e)

→ We use sub-net mask 0.0.0.0 for default entry because any IP addr if we 'AND' with 0.0.0.0 gives '0.0.0.0' & matches sub-net id of '0.0.0.0' in Routing-table

x) Process:

1) If pkt comes, 'AND' IP with sub-net mask and check routing table for subnet-id if found use it & forward through interface

2) If more than one match found, choose the sub-net mask of longest length, i.e, more no of 1's

3) If doesn't match → default Entry

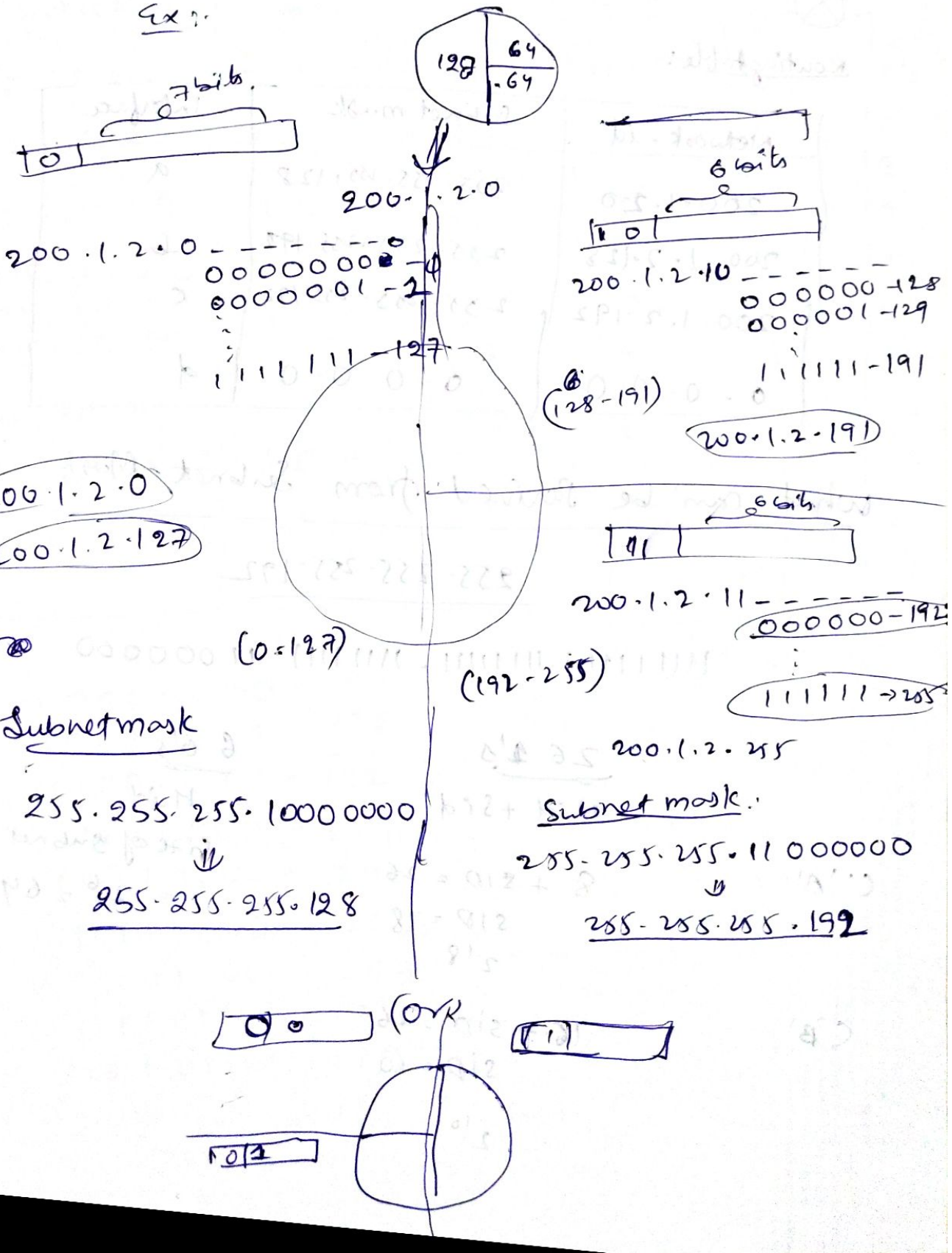
Fixed Length Subnet Masking :: (FLSM)

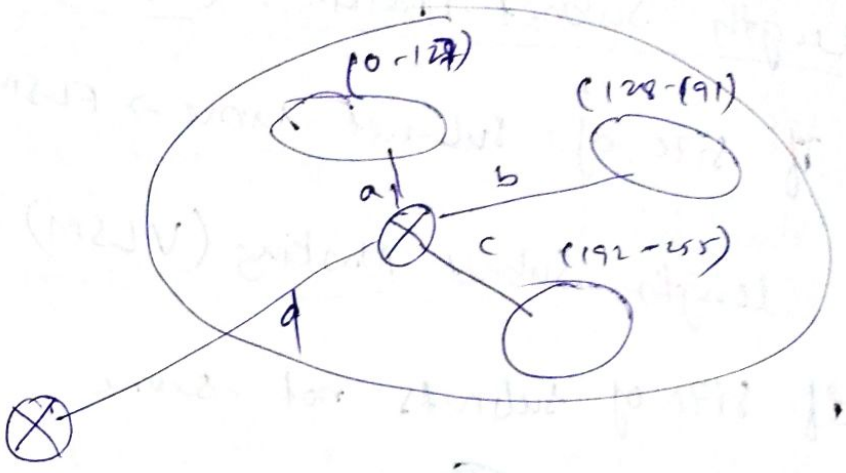
If size of sub-net same ⇒ FLSM

Variable length Subnet Masking (VLSM)

If size of subnets not same

Ex :-





Routing table:

Network-id	Subnet mask	Interface
200.1.2.0	255.255.255.128	a
200.1.2.128	255.255.255.192	b
200.1.2.192	255.255.255.192	c
0.0.0.0	0.0.0.0	d

What can be Derived from Subnet-Mask

255.255.255.192

11111111.11111111.11111111.11000000

26 1's — Nid + Sid

6 0's — Hid

Size of subnet = $2^6 = 64$

C 'A'

8 + SID = 26

SID = 18

2^{18}

C 'B'

16 + SID = 26

SID = 10

2^{10}

8 8 8 4
255.255.255.15 → subnet-mask (theoretical practically not possible)

c'c

.0001111

Nid + Sid = 28 1's

24 + Sid = 28

Sid = 4

Subnet mask	no of hosts	Subnets in class 'A'	Subnets in class 'B'	Subnets in class 'C'	10 bits (because we have only 8's)
255.0.0.0	$2^{24}-2$	1	(not possible)	–	–
255.128.0.0	$2^{23}-2$	2^1	–	–	1
255.192.0.0	$2^{22}-2$	2^2	–	–	2^2
255.240.0.0	$2^{20}-2$	2^4	–	–	2^6
255.255.0.0	$2^{16}-2$	2^8	1	–	2^{13}
255.255.254.0	2^9-2	2^{15}	2^7	–	2^{14}
255.255.255.0	2^8-2	2^{16}	2^8	1	2^{17}
255.255.255.224	2^5-2	2^{19}	2^{11}	2^3	2^{18}
255.255.255.240	2^4-2	2^{20}	2^{12}	2^4	–

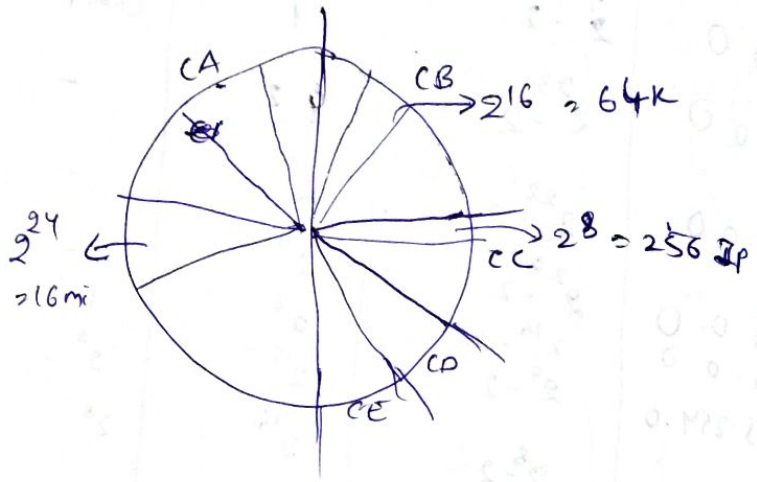
00000000 - 0
10000000 - 128
11000000 - 192
11100000 - 224
11110000 - 240
11111000 - 248
11111100 - 252
11111110 - 254
11111111 - 255

CIDR Blocks

if we use "/10" bits as network id, then no. of subnets = ?

∴

Classless Inter Domain Routing



IANA :-

Internet Assigned Number Authority

↳ we buy a network from IANA

Disadvantage :-

1. Smallest n/w has 256 IP's ⇒ if 'u' want '100' IP's can't buy

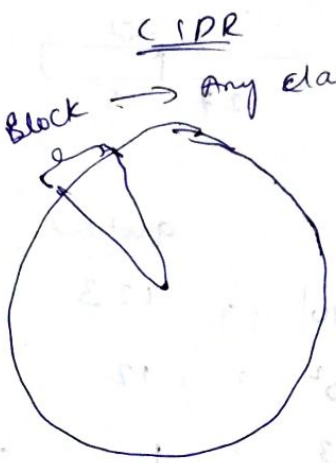
→ Till 1990's classFull Addressing is followed

then, ⟹ class less Addressing

CIDR

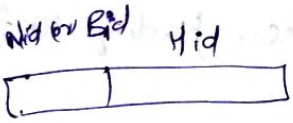
⇒ No classes

⇒ How many you require, that o many alone you can take



Disadv:

→ we cannot know Nid & Hid, so we use slash notation



a.b.c.d/n

20.10.50.100/20 ⇒ Nid = 20 bits
Hid = 12 bits $= 2^{12}$ ip

↓

CIDR Notation (Currently we are using)

Rules for forming CIDR Blocks

1. All Ip add should be continuous

Ex: (.10, .11, .12, .13)

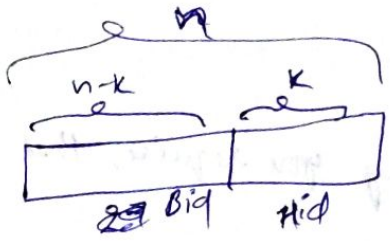
2. Block size should be power of '2'

Ex: 10 1 1 — (11)

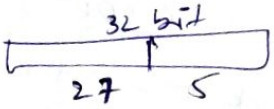
if divided by 2^1 = 101 (quotient) | 1
2^2 = 10 | 11
2^3 = 1 | 011
2^4 = 0 | 1011

Similarly if you divide 'n' bit binary no with

then,



$\Rightarrow 2^5$



Similarly decimal no:

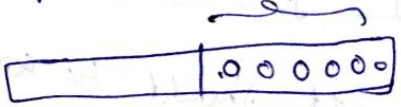
1234	quotient	Remainder
$/10^1$	123	4
$/10^2$	12	34
$/10^3$	1	234
$/10^4$	0	1234

So, if block size is power of 2, then finding host is very easy

(3) First IP add in the block should be evenly divisible by size of the block.

Ex:

2^n



000000

:

111111

if it divisible by size, then 'Hid' will be

⇒ So, we can use first IP address as "Block id (or) Host id : Subnet"

Ex:-

① 100.1.2.32 → Block-id

100.1.2.33

⋮

100.1.2.47 → BBA

16 = 2^4

1) contiguous
2) size
3)

100.1.2.00010000 (4)

100.1.2.32/28 ⇒ CIDR

/24 ⇒ Remainder

② 20.10.30.32

20.10.30.33

⋮

20.10.30.63

32 = 2^5

1)
2)
3)

20.10.30.32/27

20.10.30.001 (5 bits) 00000 /2^5

⇒ CIDR

③ 150.10.20.64

150.10.20.65

⋮

150.10.20.127

64 = 2^6

1)
2)
3)

150.10.20.01000000

150.10.20.64/26

⇒ CIDR

④ 20.10.30.35/27

Nid | Hid

20.10.30.001 00011

00000 - 32

00001 - 33

⋮

11111 - 63

Ex:-

100.1.2.35/20

Bid | Hid

100.1.0000 0010.00 0100011

100.1.0.0 — 0000.00 000000 - 0

:

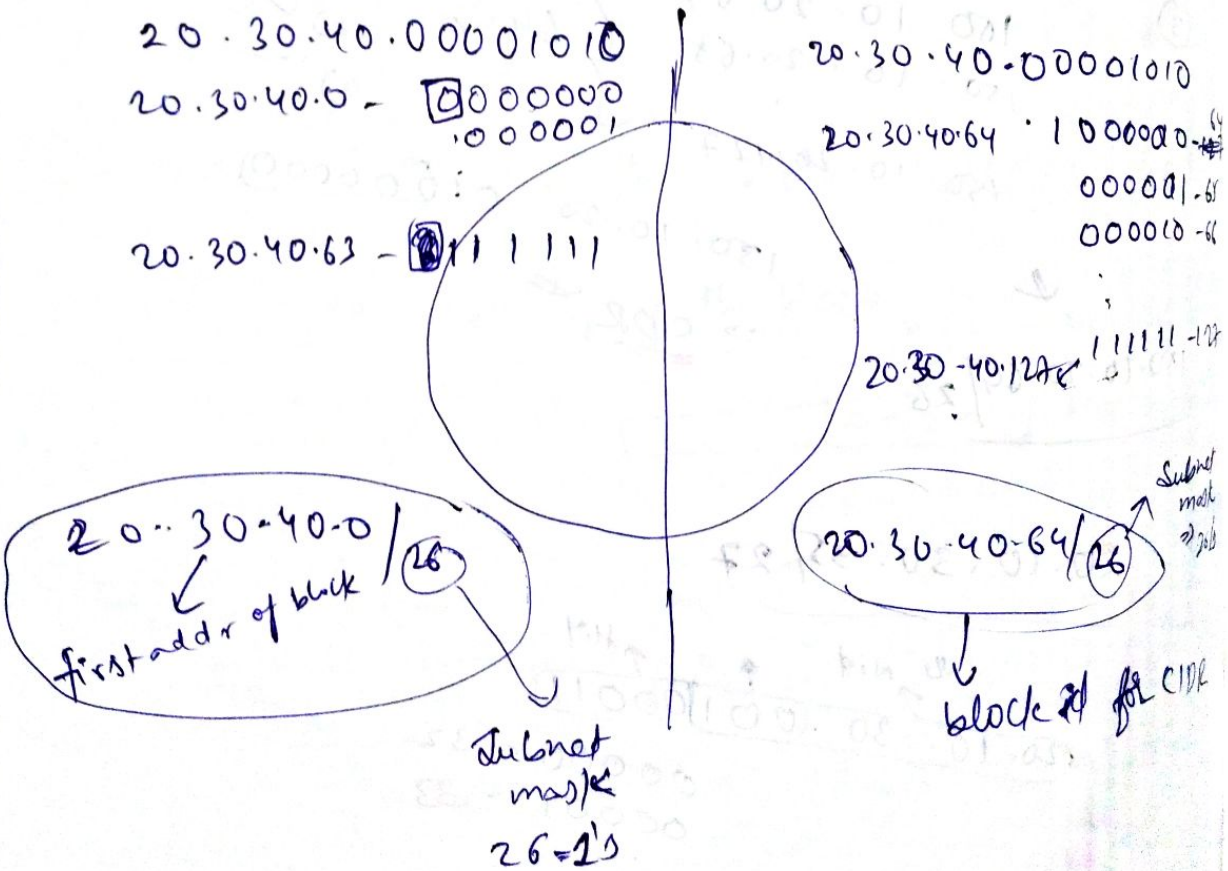
100.1.15.255 — 1111.11 11 1111 -

Subnetting in CIDR

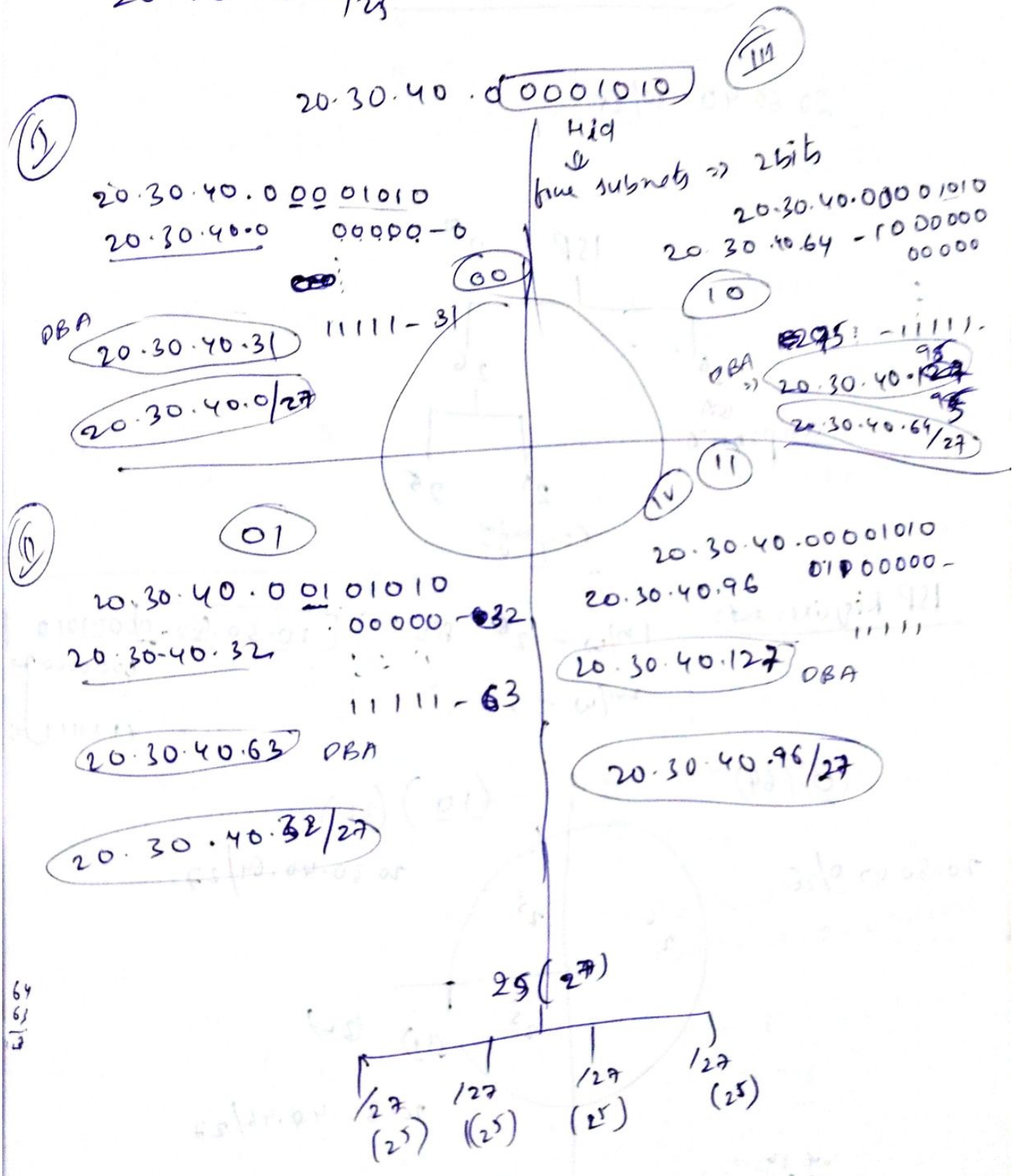
20.30.40.10/25

20.30.40.00001010

Hid

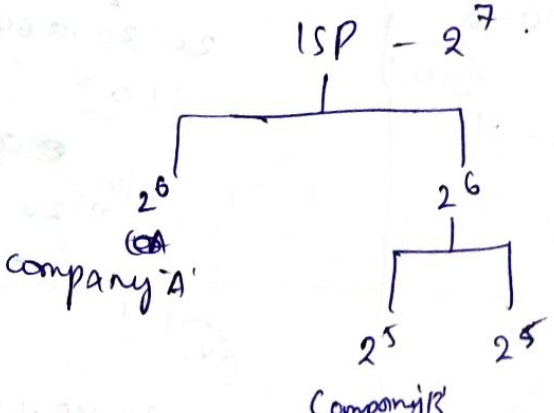


20.30.40.10/25 ⇒ four subnets



VLSM in CIDR

20.30.40.10/25



ISP Requirements:

1 n/w - 2^6 size

2 n/w - 2^5

20.30.40.0

Ex 2:

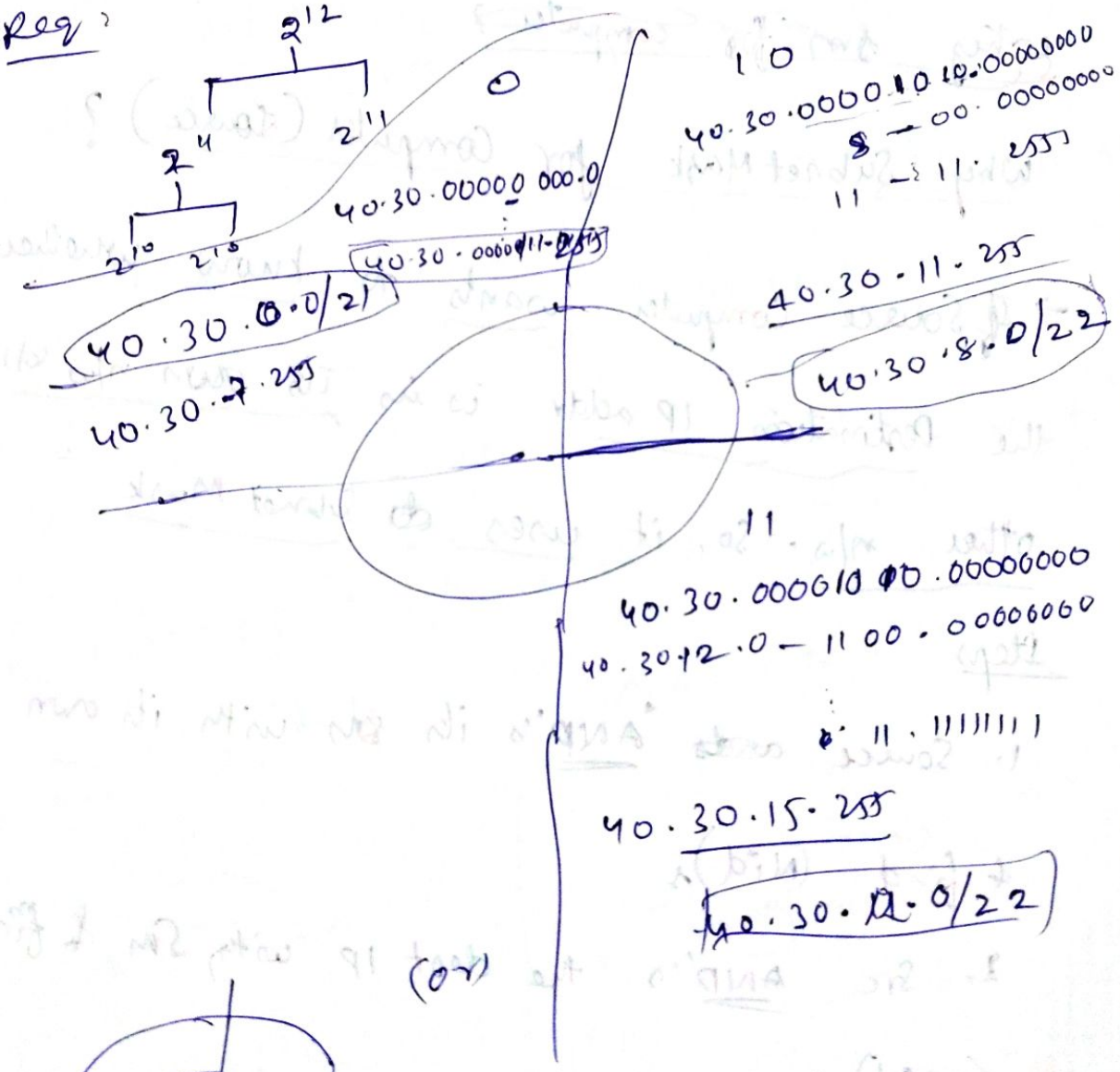
40.30.10.10/20

Bid	HH
40.30.0000	1010.00001010

40.30.0.0 - 0000.00000000

40.30.15.255 - 1111.1111 1111

Req:



Problems on Subnet Mask

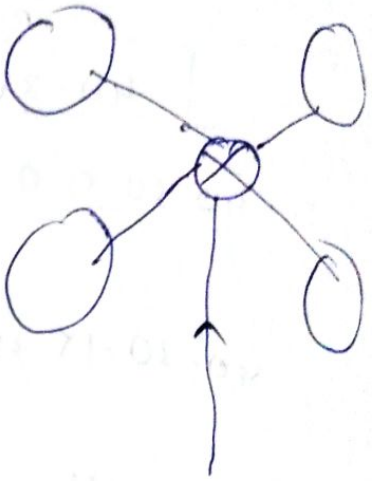
> IPCONFIG

IPV4 - IIP

DGW (default gate way)

SM (Subnet mask)

DNS (Domain Name Server)



~~why SM for computer?~~

Why Subnet Mask for Computer (Source)?

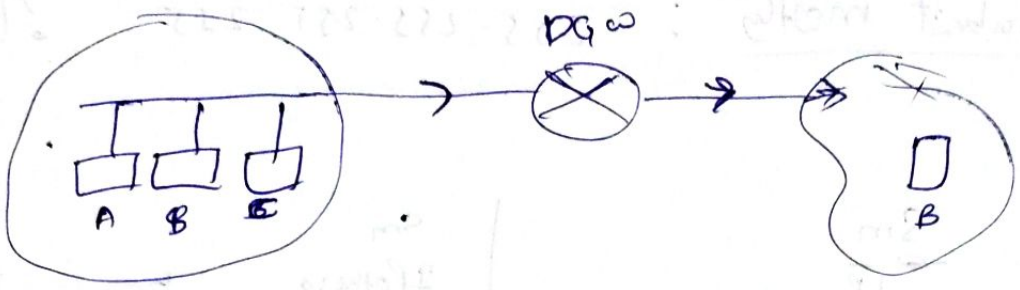
→ If Source Computer wants to know whether the Destination IP addr is in its own n/w or other n/w. So, it uses Subnet Mask.

Steps

1. Source "AND"s its SM with its own IP & find $(Nid)_s$
2. Src AND's the dest IP with SM & finds $(Nid)_d$

if $(Nid)_s == (Nid)_d \Rightarrow$ same n/w

$(Nid)_s \neq (Nid)_d \Rightarrow$ diff n/w



Tricky Question:

I_A : 200.1.2.10

S_A : 255.255.255.128

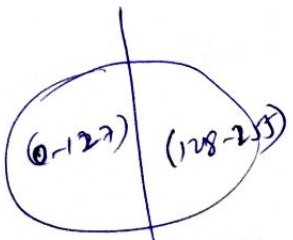
I_B = 200.1.2.69

S_B = 255.255.255.192

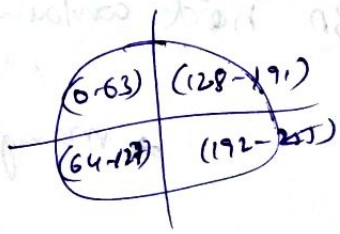
I_A / S_A (Nid_{AA} = 200.1.2.0) ≡ I_B / S_A (Nid_{BA} = 200.1.2.0) } According to 'A'

I_A / S_B (Nid_{AB} = 200.1.2.0) ≠ I_B / S_B (Nid_{BB} = 200.1.2.64) } according to 'B'

According to 'A'



According to 'B'



SubNet ⇒ PERCEPTION

→ Subnet mostly : 255.255.255.255

Sm / IP(ours)	Sm / IPothers
(Nid)ours = (IP)ours	Nid(others) = IPothers

(Nid)ours ≠ (Nid)others

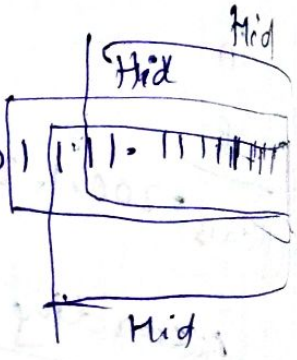
⇒ because if you connect using modem, ours should connect through Router

so, Sm is 255.255.255.255

Q Given DBA ; netid ? ; subnetmask ?

DBA : 200.1.15.255

11001000.00000001.0000111.11111111



DBA hid contains all 1's

⇒ many possibilities

⇒ /20

/21

/22

Supernetting (or) Aggregation

→ combining various n/w's to form a big n/w

why?

1. if pkt from US → India ; US routing table need not to have all n/w of India. just send to India Router then forward to states → cities → towns ↓ Dest

2. Mainly Decreases Routing table length

So, combine smaller n/w → Bigger n/w

Rules for Aggregation

i) n/w's should be contiguous (i.e n/w ids)

ii) size of n/w should be same & power of 2

iii) first n/w id divisible by size of total super net

Ex:-

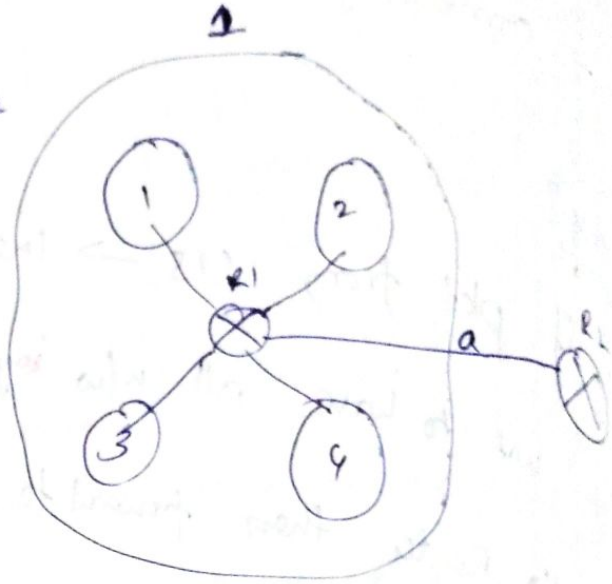
① 200.1.0.0/24
② 200.1.1.0/24
③ 200.1.2.0/24
④ 200.1.3.0/24

i) contiguous ✓
ii) size ✓
iii) first n/w id / 2^3 (total size of super net) ✓

Size of supernet : $4 \times 2^8 = 2^{10}$

R1 routing table

Nid	subnet SMask	Interface
200.1.0.0	255.255.255.0	a
200.1.1.0	255.255.255.0	a
200.1.2.0	255.255.255.0	a
200.1.3.0	255.255.255.0	a



for all 4 n/w ⇒ Supernet-id

Supernet Mask : 32 bit

0's → variable part

1's → fixed part

Subnet mask

Subnet-id & n-id ≠ no 1's

H-id = 0's

① 200. 1. 00000000. 00000000 ← Super-net-id

200. 1. 00000001. 00000000

200. 1. 00000010. 00000000

200. 1. 00000011. 00000000

fixed part | variable part

size of n/w

255. 255. 11111100. 00000000

255. 255. 252. 0 ⇒ Supernet mask

IP
n/w Mask
net id

i.e.,

n/w id
Supernet Mask
supernet id
↳ first n/w-id

→ always first net-id is supernet-id

N.id	supernet mask	Interface
200.1.0.0	255.255.252.0	a

Ex:

200.1.32.0/24
200.1.33.0/24
⋮
200.1.47.0/24

Size of n/w:
$2^7 \times 2^5 = 2^{12}$
⇒ 12 bits H-id
⇒ 20 bits n-id

Supernet mask:
255.255.240.0

Supernet -id
200.1.32.0/20

Subnet (ex) supernet consists 20 bits

Ex:-

100.1.2.0/25
100.1.2.128/26
100.1.2.192/26

supernet 100.1.2.128/25
$2^6+2 = 2^7$ → 7 bits host
25 bits net-id

⇒

100.1.2.0/25
100.1.2.128/25
⇒ $2^7 \times 2$ = 28 size

100.1.2.0/24 → net-id

→ Recent devel.

proponents vs free agents

↓

states

↓

measuring what causes what

↓

determinism

→

"Wallace" → land → Eastern Indo

↳ myths - lies - Tim

↓

settlement on Island. ↑ Timor

↳ Israel

↓

Timor

island

→

biography

↓

Nalcomale (-ve)

↓ ↳ not exception

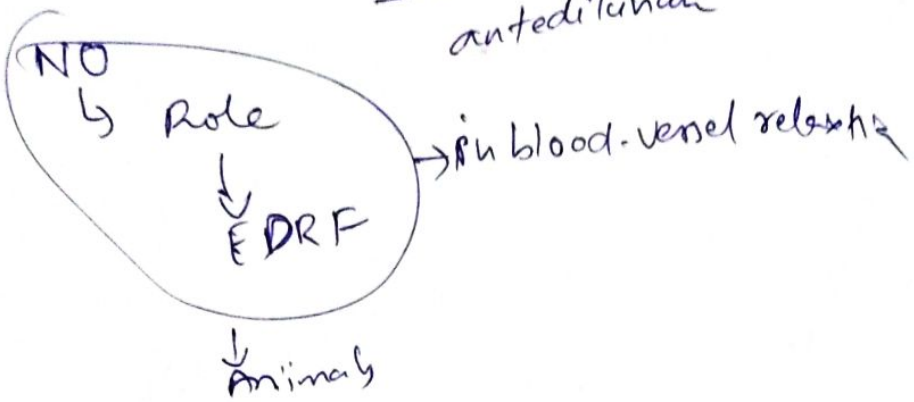
opp to chiefs

↓

exercise his power

antedilurian

antediluvian



Plants

C.: exp

D. dilemma

Story - formation

fmass + ple

→ C.O.9. → retroactivity

X

↓

counts.

↓ X

→ electron - breaki

⇒ ⊙ "Constituent"
↓
C.E →

flow : C.R, M, P

⊙ → photon - p- com Interaction

→

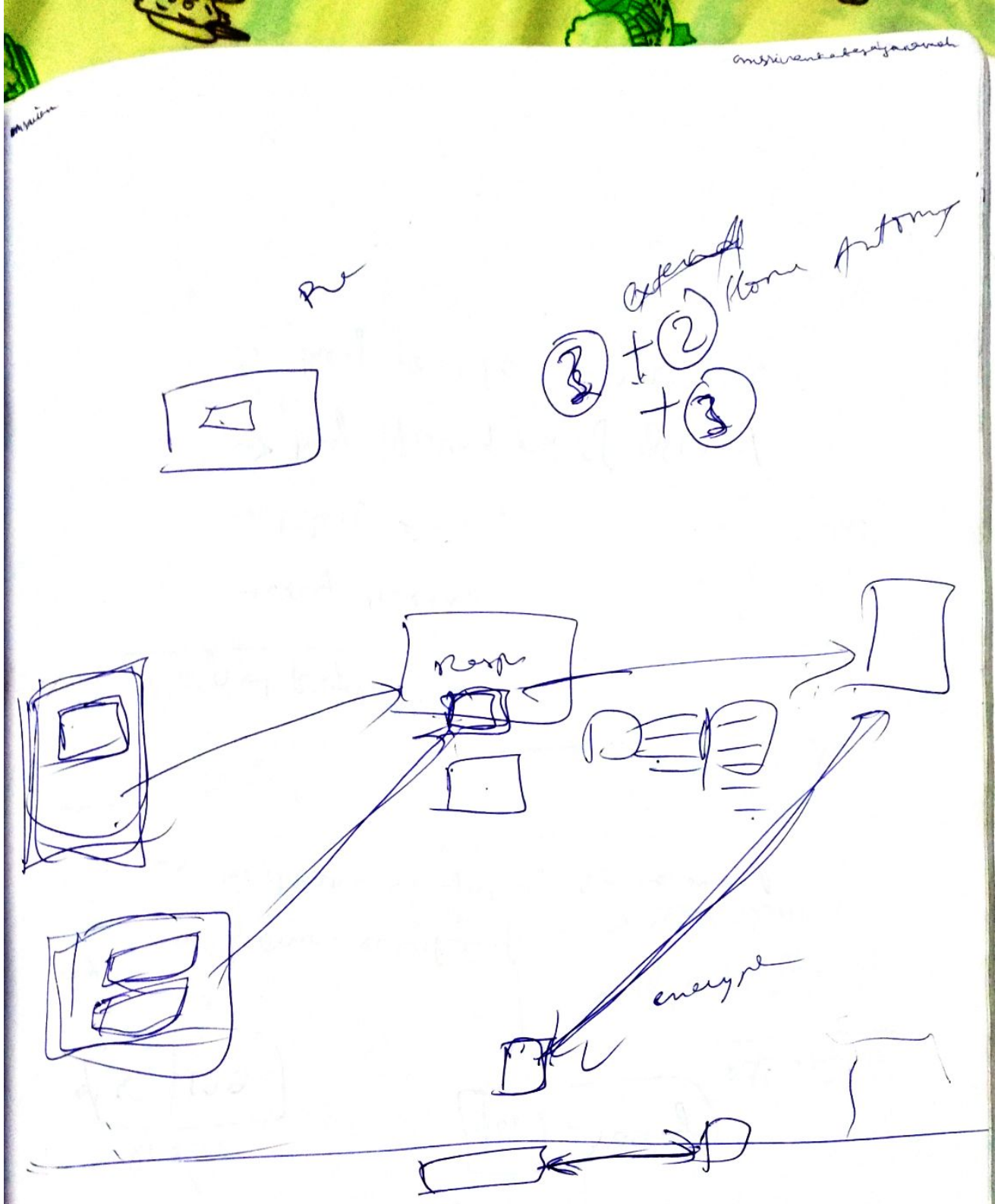
→ Cobies → fisesh tropical, temperate

→ healthy

Critical - thirsty
↓
gradient area
→

→ wright → newel
↓ no sep co

→


Home Automy
repo
energy
Arduino
connect
Tube.
FAN
TV
Res

mass spectrometry –
→ effects

→ Tech → microbiology labs → automation

→ apply
→ potential appln

→ limitations
↳ grow it
↳ directly not identify

→ TEM, identification & diagnostic of disorder.

Floral symmetry,

→ botany ↳ Rosen

→ Asymmetry → Mono

→ N-1 - rocks → age + comp:
origin → history

→ B & C - T. comp.

↓

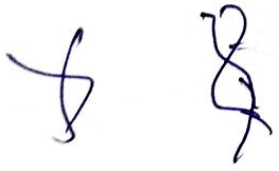
I - G. activity → ~~X~~

↓

S - Terr - sequ

→

→ N. anem → accident · DNA (..



* modbus TCP/IP

2) BMS (Building management system)

- BACnet
- DALI
- Open webnet

$y < z$

$AC < BC$

$x + y = 13$

$x + z = 22$

$y - z = -9$

$z - y = 9$

$\frac{1}{3} \times 13 + \frac{1}{5} \times 18 + \frac{1}{5} \times 22 + \frac{1}{5} \times 17 + 2$

$18 + 4.9$

$= \frac{223}{80}$

$\frac{1}{3}$

TYPE E

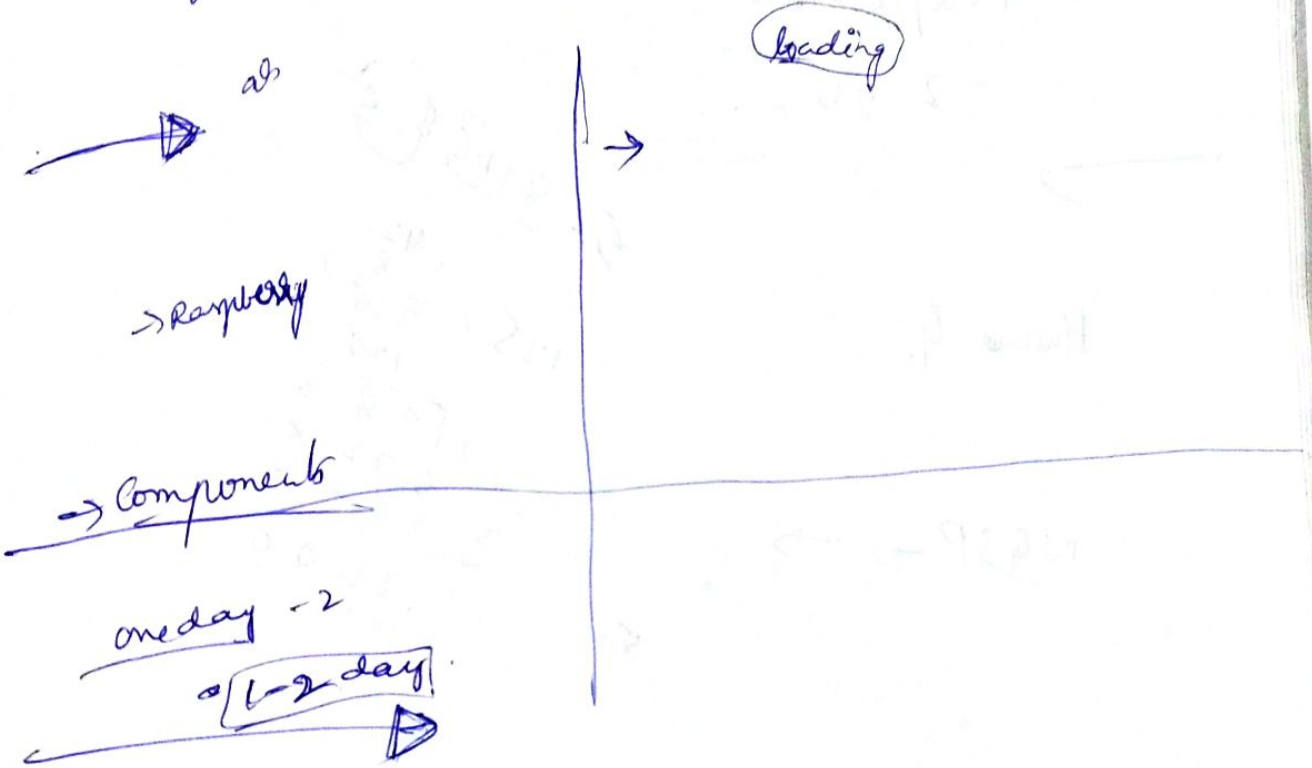
$$\frac{63 \times 0.36 \times 0.15}{0 + 0.27}$$

$= 30 \times 0.15$

4.5

Raspberry pi

→ It is an mini computer with arm processor, memory and graphic capabilities



Raspberry

→ OS installation
→ commands
→ wifi's
→ O.S

Omsairam Om malaiyappathayanamaha. Omsriventateshayanamaha

X — music

→ Europe - tour

- 2 - yrs - .

→

Hallow - G.

NIGSP → →

5 . 8 7.6 $ - 5

125 | 42 | 8 | 3 | 336 | 600 | 125

2 | 98 | 72 | 36 | 4.2200

$

$\frac{20}{20} + \frac{30}{30}$

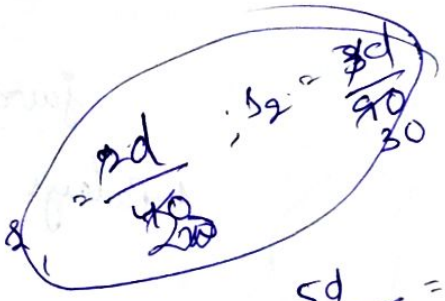
$\frac{20}{10}$ $\frac{30}{3}$

Raspberry pi -

ipaddress :

port_no :

Client



1. $^{9}C_3$ → $\frac{9 \times 8 \times 7}{3 \times 2}$ = 84

$\frac{10 \times 9 \times 8 \times 7}{4 \times 3 \times 2}$ = 210

$\frac{8 \times 7}{2 \times 1}$ = 28

$\frac{8 \times 7 \times 6}{3 \times 2}$ = 56

10×56 = 560

$^{5}P_2 = 5!$

$^{5}P_3 = \frac{5 \times 4 \times 3}{3 \times 2}$

$\frac{10 \times 9 \times 8 \times 7}{4 \times 3 \times 2}$

$\frac{85}{40}$ / 00 → 340 × → 0.3400

$P(A \cup B) = P(A) + P(B) = 0.63$

$P(B \cap C) = P(B) \cdot P(C) = 0.34$

$P(B) + P(C)$ $P(B \cap C) = P(A) \cdot P(B)$

$P = \frac{3 \times \frac{1}{7}}{5 \times \frac{1}{7} + \frac{2}{7}}$ =

$3P(1) +$

$3P + 4P = 1$

$P(7) = P = 1/7 \times 2$ $P(6) = 2/7$

$P(\text{odd number}) = P(1^{st}\text{ odd}) + P(2^{nd}\text{ odd}) + P(3^{rd}\text{ odd})$

$^{10}P_3$

$^{10}C_3 = \frac{10!}{7! \cdot 3!}$ $\frac{10!}{3! \cdot 7!}$ / $3!$

$\frac{4}{10C_1}$ $\frac{5}{9C_1}$

For

$\frac{4}{10} \cdot \frac{5}{9} \rightarrow \frac{2}{9}$

① $b \neq 0$

$\frac{ab+3}{b}$; $\frac{a(b+1)}{b}$

②

$x^2 y$

$x^2 y = 72$

$\frac{1}{4} + \frac{1}{36} + \frac{1}{32} \quad \frac{1}{44}$

③

25, 50, 75, 100, 1000

$\frac{10250}{2}$ × 40

④

$3y = \frac{6x+9}{3}$

$y = \frac{2x+3}{1} - y = 0$

⑧

$\frac{20}{3} = 6$

$\frac{6}{3} = 2$

$\frac{2}{3} = \frac{}{8}$

$\frac{20}{5}$ (4)

⑩

24

20

1200

50 × 7 = 350

450

2700

1500

500

700

$24/(35) = 5/7$

	11	12	13	16
A				
B				
C				Y
D				x
E				

Int.

Opinion -

an

7·6

720

24
×5
120
×6
720
×7
5040

240
×7
1680

240·4
720×8
3×2

120
720×7
3×2

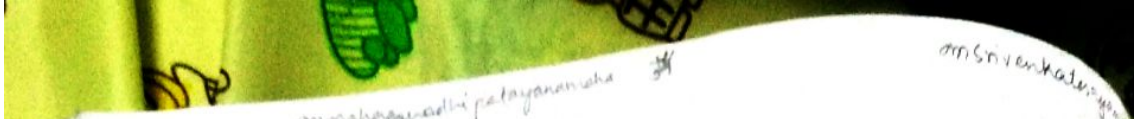
ecnc.

MC VMc

conflict

AV

A			
B			
C			
D			
E			



om sri venkateswaraya namaha

om mahaganadhipathayenamaha

om sri ram

Wasting sections

10:00pm

10:00

Relationships are founded on trust which goes hand-in-hand with

fourth

2:30 pm

①

etc

T. :

C. :

P&E :

Speaking 1. note taking 1 less than
group / 2 team work 1 leadership skills
or 3. develop an article
for example:

Conclusion:

Passage

Public meeting

building renovation

- 100

only electrical

destroy's

lecture

→ heavy down

→ [illegible]

→ brick bed

→ ruined [illegible]

→ cost less

→ communication

college

[illegible]

VLAN

LAN:-

A local Area Network (LAN) is a computer network that inter connects computers in a limited area such as home, school etc

VLAN:-

It is a group of hosts with a common set of requirements that communicates as if they were attached to the same broadcast domain regardless of their physical location

Java.math.BigInteger Class

Constructor

BigInteger(string val);

Methods

(b1, b2) → BigIntegers

b3 = b1.add(b2);

b3 = b1.divide(b2);

b3 = b1.multiply(b2);

~~b3 = b1.divide(b2);~~

b3 = b1.subtract(b2);

~~b3 =~~ b1.mod(b2);

Compare:

int c = b1.compareTo(b2)

b3 = b1.modPow(b2, b4)

((b1^b2) % b4)

b3 = b1.pow(int m)

(b1^m)

b3 = b1.max(b2);

b3 = b1.min(b2);

Logical

b3 = b1.and(b2) → b1 & b2

b3 = b1.or(b2)

b3 = b1.xor(b2)

b3 = b1.andNot(b2)

→ (b1 & ~b2)

b2 = b.abs();

b3 = b1.shiftLeft(int n);

b1 << n;

b3 = b1.shiftRight(int n);

b1 >> n;

```
b3 = b1.gcd(b2);

int a = b1.intValue();

Long a = b1.longValue();

String s = b1.toString();
```

BigDecimal

Constructors :-

```
BigDecimal(int val);
BigDecimal(char[] in);
BigDecimal(float val);
BigDecimal(long val);
BigDecimal(String val);
BigDecimal(BigInteger b);
```

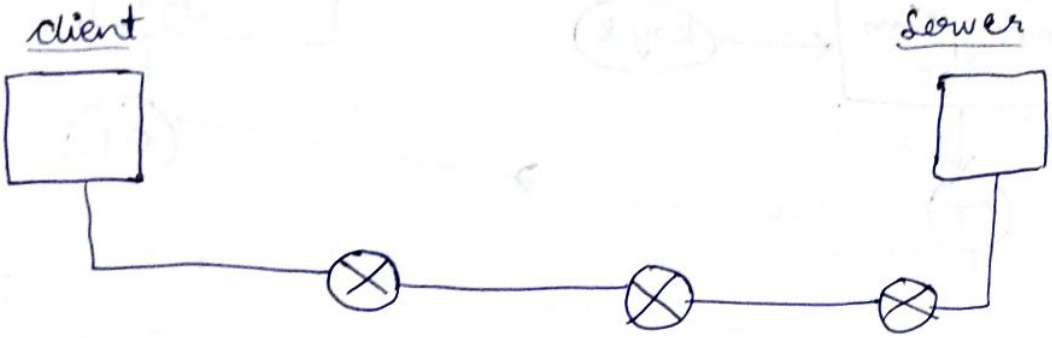
Methods:

```
b1 = b2.abs();
b3 = b1.add(b2);
b3 = b1.divide(b2);
b3 = b1.multiply(b3);
b3 = b1.remainder(b2);
b3 = b1.subtract(b2);
int b3 = b3.compareTo(b2);
b3 = b1.min(b2);
b3 = b1.max(b2);

String s = b1.toString();
int i = b1.toIntValue();
```

Network Security

Introduction to Cryptography:



tapping:- by selling our frequency to sender freq we can tap the signals

Cryptography: Plain text (PT) → (Encryption) → Cipher text (CT) → (decryption) → PT

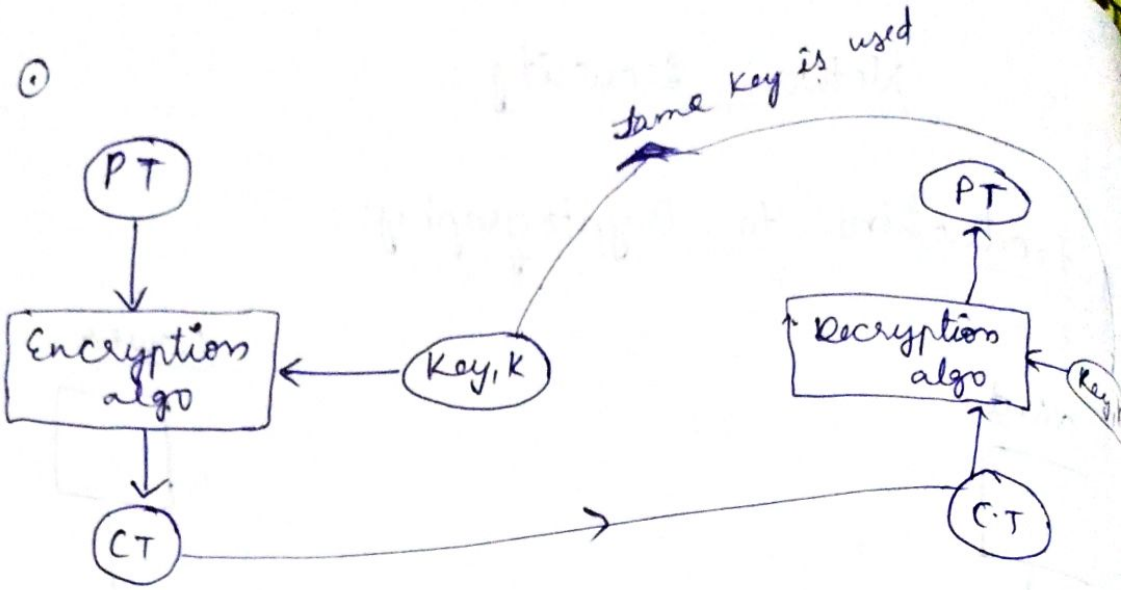
Cryptography

- Symmetric Key (or) Shared Key
- Assymmetric Key (or) Public Key - private Key

Symmetric Key (or) Shared Key:

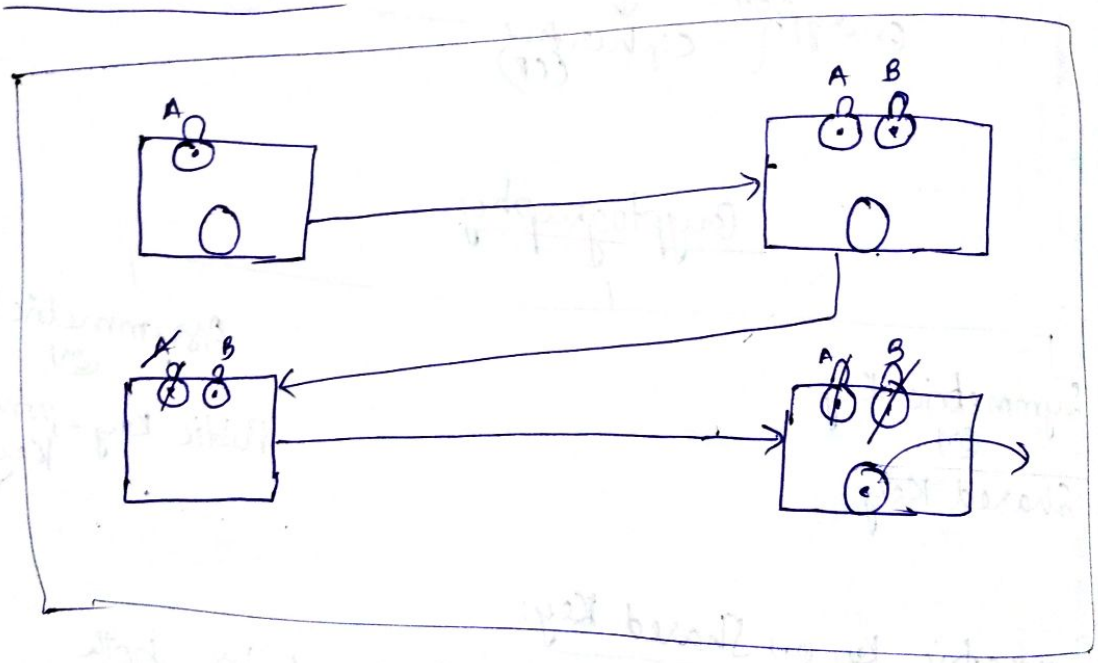
Ex:- Same (or) Shared Key is used for both encryption & decryption, which results in the Key-Exchange problem

①



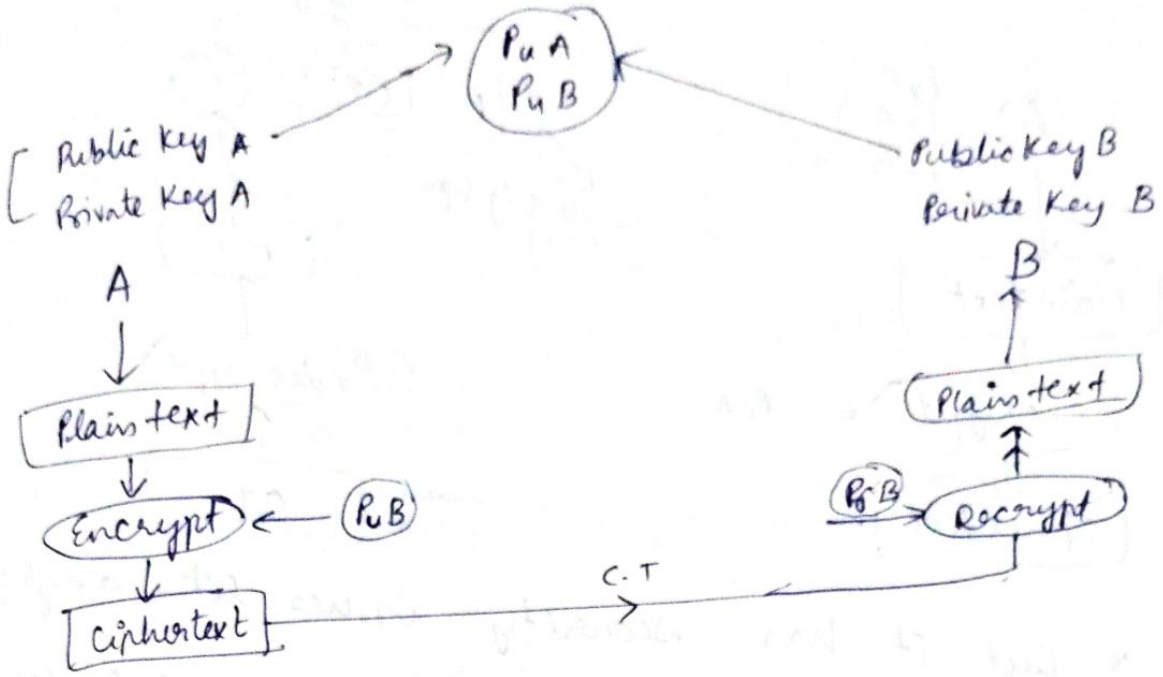
②

③ Alternate method



Public Key Private Key Cryptography :-

→ Assymetric encryption, ⇒ different keys are used for encryption & decryption.



Pu → Public keys of both the sender & Receiver are shared to all

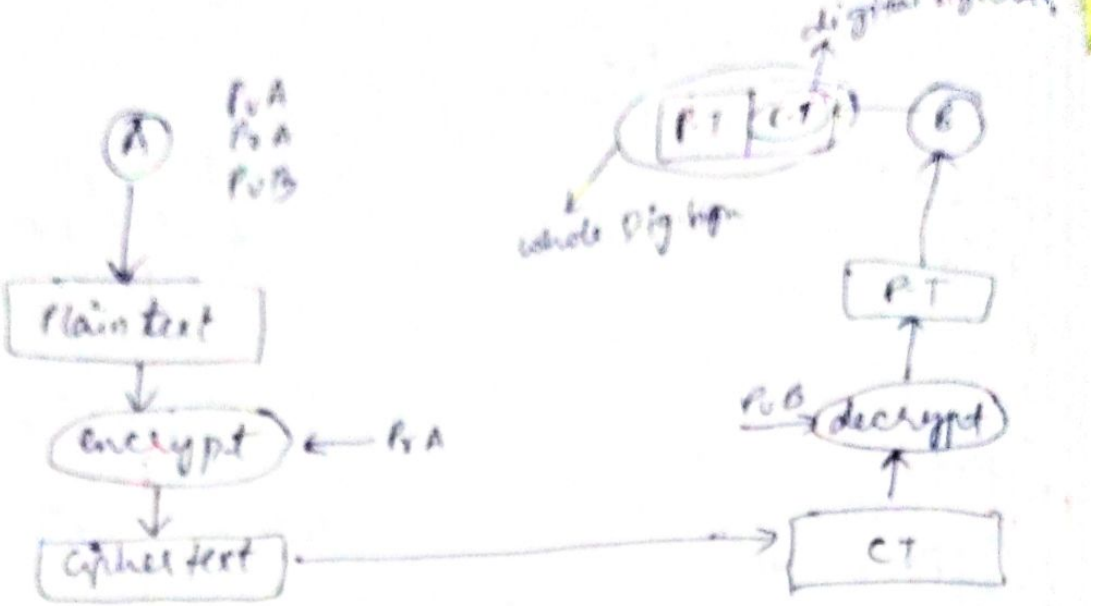
→ If we encrypt with Private Key of 'A', we can decrypt only with Public Key of 'A' vice versa

→ So, we encrypt with public key of 'B', which can be decrypted only with the private key of 'B'.

Digital Signature:- & Authentication

* "Signatures" are to identify a person (or sender,

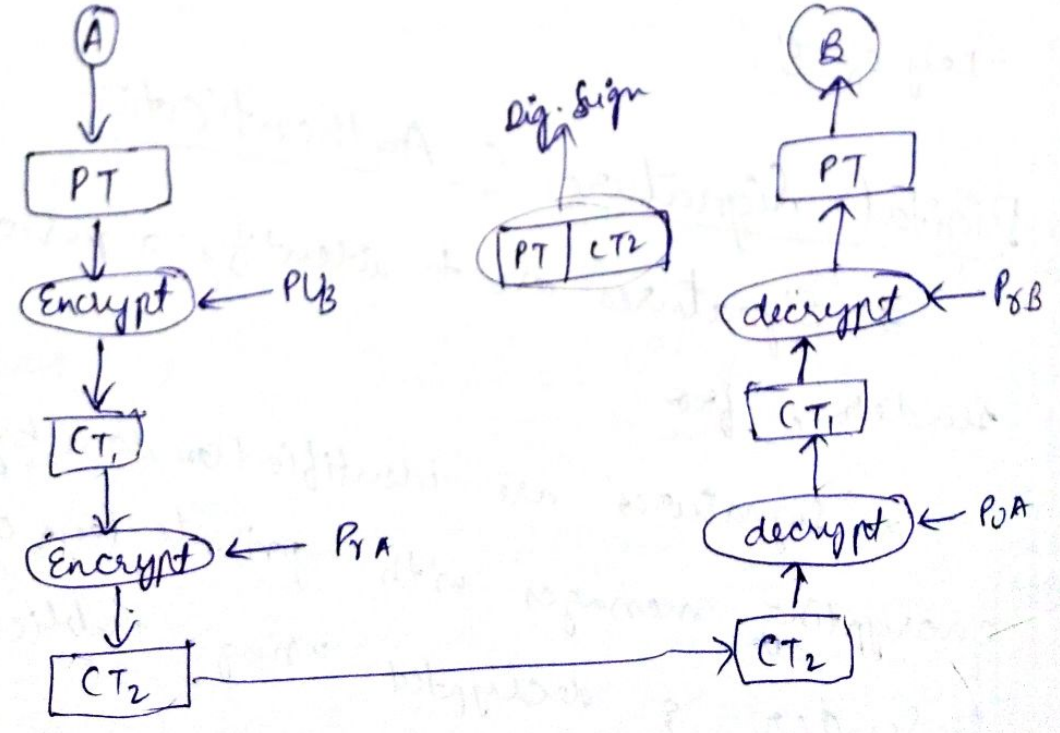
x "Signatures" are identified or done by encrypting messages with private keys of Sender & decrypted using public key of Sender



* But it has security issues like any can decrypt using Public Key of A, which is available for all.

Ex: For bank txn from client, which is to be authenticated by bank using digital signature

Encryption & Authentication together:-



Fermat's (Little) Theorem :-

p - prime number ; a - +ve integer ("p" should not divide "a")

$$a^{p-1} \equiv 1 \pmod{p}$$

⇒ If "a^{p-1}" divided by 'p' it gives '1' as remainder

⇒ $$a^{p+1} \equiv a \pmod{p}$$

Ex:- $a = 2 ; p = 7$

$a^{p-1} = 64 \Rightarrow \frac{64}{7} = 1$ (Remainder)

* Mainly used in Primality Testing (checking whether it is prime (or) not)

Ex:- 'p'

1) ——→ (p

↓

take b/w numbers & perform check using formula

Euler's totient function :-

$\phi(n) \equiv$ {k} $1 \le k \le n$

relatively prime to 'n'

gcd(k, n) = 1

① Ex: n = 9

1, 2, 3, 4, 5, 6, 7, 8, 9

$\Rightarrow \phi(9) = 6$

② n = 5

1, 2, 3, 4, 5

$\Rightarrow \phi(5) = 4$

* If 'p' is prime, then

$$\phi(p) = (p-1)$$

$\phi(10) = 4$

1 ~~2~~ 3 ~~4~~ ~~5~~ ~~6~~ 7 ~~8~~ 9 ~~10~~

$\phi(n)$ is multiplicative.

$n = m \times l \Rightarrow \phi(n) = \phi(m) \times \phi(l)$

$10 = 5 \times 2 \Rightarrow \phi(10) = \phi(2) \times \phi(5)$

$= 1 \times 4$

$= 4$

$\phi(35) = \phi(5) \times \phi(7)$

$= 4 \times 6$

$= 24$,

$\phi(p \times q) = \phi(p) \times \phi(q)$

$= (p-1) \times (q-1)$,

Chinese Remainder Theorem :-

$n_1, n_2, n_3 \cdots n_k$ → positive integers

→ relatively prime pair wise

$x \equiv a_1 \bmod (n_1)$

$\vdots$

$x \equiv a_k \bmod (n_k)$

→ '⊗' $1 < x < (n_1 n_2 n_3 \cdots n_k)$

↓

unique integer in the given range

→ A Integer 'x' can be uniquely represented in terms of remainders in btw the range '1' and $(n_1 n_2 n_3 \cdots n_k)$

Ex:- (2,5) → relatively primes

numbers b/w '1' and (2×5) can be uniquely represented like

(2×5) = 10

1 ---- 10
1 ---- 10

x	2	5
1	1	1
2	0	2
3	1	3
4	0	4
5	1	0
6	0	1
7	1	2
8	0	3
9	1	4
10	0	0

Ex:2 $x = 2 \pmod 3$ [∵ remainder is '2' when 'x' divided by '3']

$x = 3 \pmod 4$

$x = 1 \pmod 5$

⇒ $x = 3t + 2$

$x = 4s + 3$

$x = 5u + 1$

Primitive Root

If 'a' & 'n' are relatively prime ($\gcd(a,n)=1$) then there exists atleast one 'm' such that,

$$a^m \equiv 1 \bmod n$$

* i.e, when a^m divided by 'n' it should give '1' as remainder

Ex: If $a = 7$; $n = 19$; $m = ?$ (smallest)

$$7^m \equiv 1 \mod 19$$

substitute & find answer (is multiple

Let $m = 3$ $\quad = \frac{7^3}{19} = 1$

(2)

$a = 3$; $n = 7$; $m = ?$

$$3^m \equiv 1 \mod 7$$

$$m = 6$$

Ex:

$3 \mod 7$

$3^1 \mod 7 = 3$
$3^2 \mod 7 = 2$
$3^3 \mod 7 = 6$
$3^4 \mod 7 = 4$
$3^5 \mod 7 = 5$
$3^6 \mod 7 = 1$

} period = 6

⇒ If in $(a \mod b)$, if period $= \phi(b)$

then 'a' is primitive root of 'b'

RSA Algorithm

→ famous algo for generating public key private key (Linux based) pair

R S A
- R → Rivest
- S → Shamir
- A → Adleman (3 scientists)

→ proposed in 1977

→ (P_u, P_r) pair

Steps

1. choose two distinct prime numbers 'p' & 'q'
2. compute "$n = p * q$"
3. $\phi(n) = \phi(p) * \phi(q) = (p-1)(q-1)$
   $= pq - (p+q-1) = n - (p+q-1)$
4. choose an integer 'e' $1 < e < \phi(n)$
   $gcd(e, \phi(n)) = 1$
   (e is prime)
   $(e, n) \rightarrow$ public key
5. Determine d as $d \equiv e^{-1} \pmod{\phi(n)}$
   $\Rightarrow ed \equiv 1 \pmod{\phi(n)}$
   $(d, n) \rightarrow$ private key

(A) $(e, n) \rightarrow PU_A \rightarrow PU_A$.
$(d, n) \rightarrow PR_A$

Ex:- 1) $p = 61$; $q = 53$

2. $n = 61 \times 53 = 3233$

3. $\phi(3233) = (61-1)(53-1)$

$= 3120$

4. $1 < e < 3120$

$\downarrow$

$17 = e$

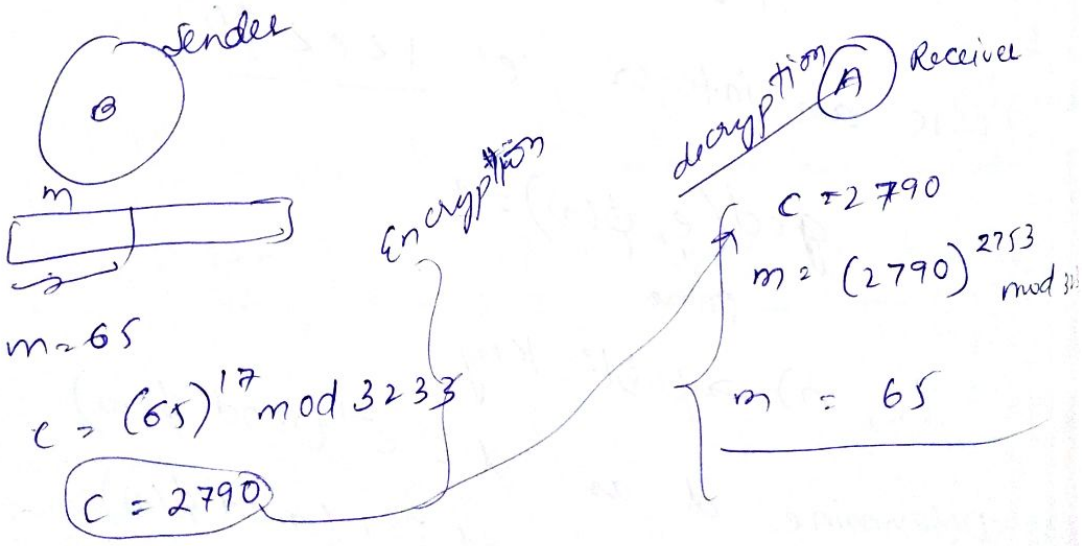
5. $(e * d) \% \phi(n) = 1$

$(2753 \times 17) \% 3120 = 1$

(d)

$\underbrace{PU(17, 3233)}_{e, n}$; $\underbrace{P_r(2753, 3233)}_{d, n}$

$P, q, \phi(n)$ → should be secret



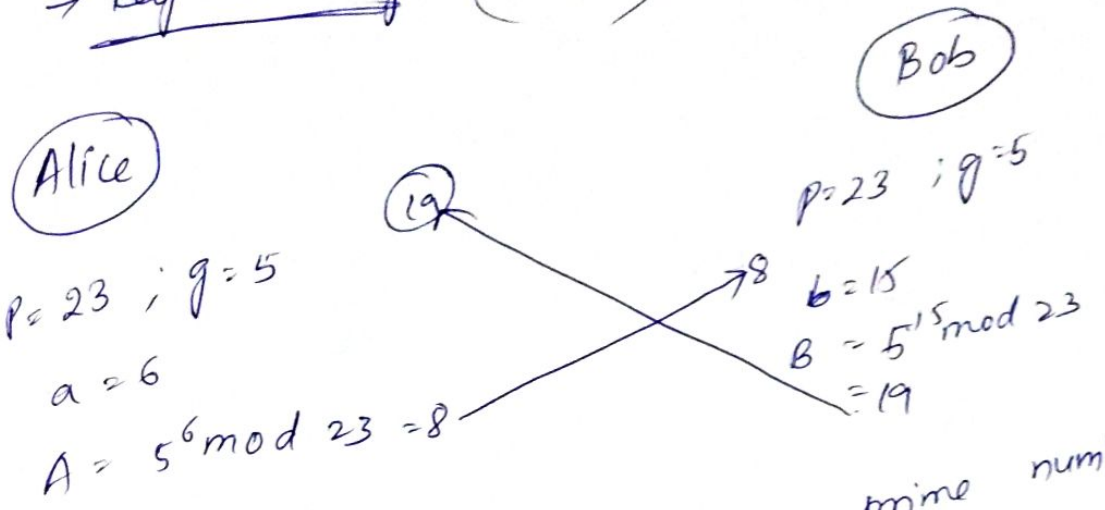
Disadv:-

* Requires large computations

Diffie - Hellman Algorithm

→ Primitive root concept is used

→ Key exchange → (only for key)



1. Alice and Bob agree to use a prime number, 'p' and a base 'g'
2. Alice chooses a secure integer a, then sends $A = g^a \bmod p$ to Bob
3. Bob chooses a secure integer b, then sends $B = g^b \bmod p$ to Alice

4. Alice computes $S = B^a \bmod p$

$19^6 \bmod 23 = 2$

5. Bob computes $S = A^b \bmod p$

$= 8^{15} \bmod 23$

2

⇓

Key used for exchange of msgs

Reading Comprehension Tips:

1) Focus on opening and closing Paragraphs and read the body paragraphs, while answering questions

2) Use Context to help you:

If a question asks about a particular line, don't go back in to the passage & read just that line. Read atleast 2 line before & after that line

3. Save Unfamiliar passage for last:

4. Really, Understand what the question is asking.

Don't skim through qstn & read the answer choices. Understand qstn & answer

5. Underline and Take Notes as you Read.

→ "+ve", "-ve" → author

→ some one (or) two key words

Components of a Passage:

1. The Point: "important piece of info, the author is trying to convey in the passage". By the end of your first read through you should be able to identify the main point

2. BACKGROUND: Info you need, in order to understand the point. Don't confuse between, "Back ground Info (or) supporting evidence"

Support: Additional Info given by the author in the form of evidence or examples to support Point. Keep an eye out for various evidence & supporting examples that the author provides

Implications: effects of the main point, End Results.

→

Trap Answers Types

1) Answer choices that use extreme or Categorical words such as "only, all, always, every, never and exclusively"

2) choices that make use of information that doesn't appear in the text

3) choices in which "Facts are Distorted"

4) choices that ask you to make judgements

5) choices that include "outrageous, illogical, unscientific, or politically incorrect" statements

6) choice that "Assume something that is not mentioned in passage"

7) choice, that cannot be backed by solid proof, from within the passage

STeps to Answer R.C

1. Read the first & last paragraphs and first and last lines of other paragraphs.
   : You should be able make out point & structure at one go"
2. Makes notes as you read.
3. Identify key and signal words :-
   Ex:- first, Second, In contrast, Claims
4. Recap with a Visual Movie:
   (10-15 secs)
5. Start Answering

Tips - 4g feel which are useful :-

1) Paraphrasing :
   → Paraphrase extensively, Replace that one particular term with some familiar (or) easy word that you can understand

1. minutiae - small, precise, (or) trivial details of something

2. ecclesiastical - spiritual

3. canonical - standard, accepted, orthodox

4 assay - evaluation, assessment, probe, scrutiny

5 vis-à-vis - in relation to, ~~with~~ with regard to

- women's need vis-à-vis employment

6. Retroactive - pay increase (or) augment (or) enhance (enact) of something that existed before.