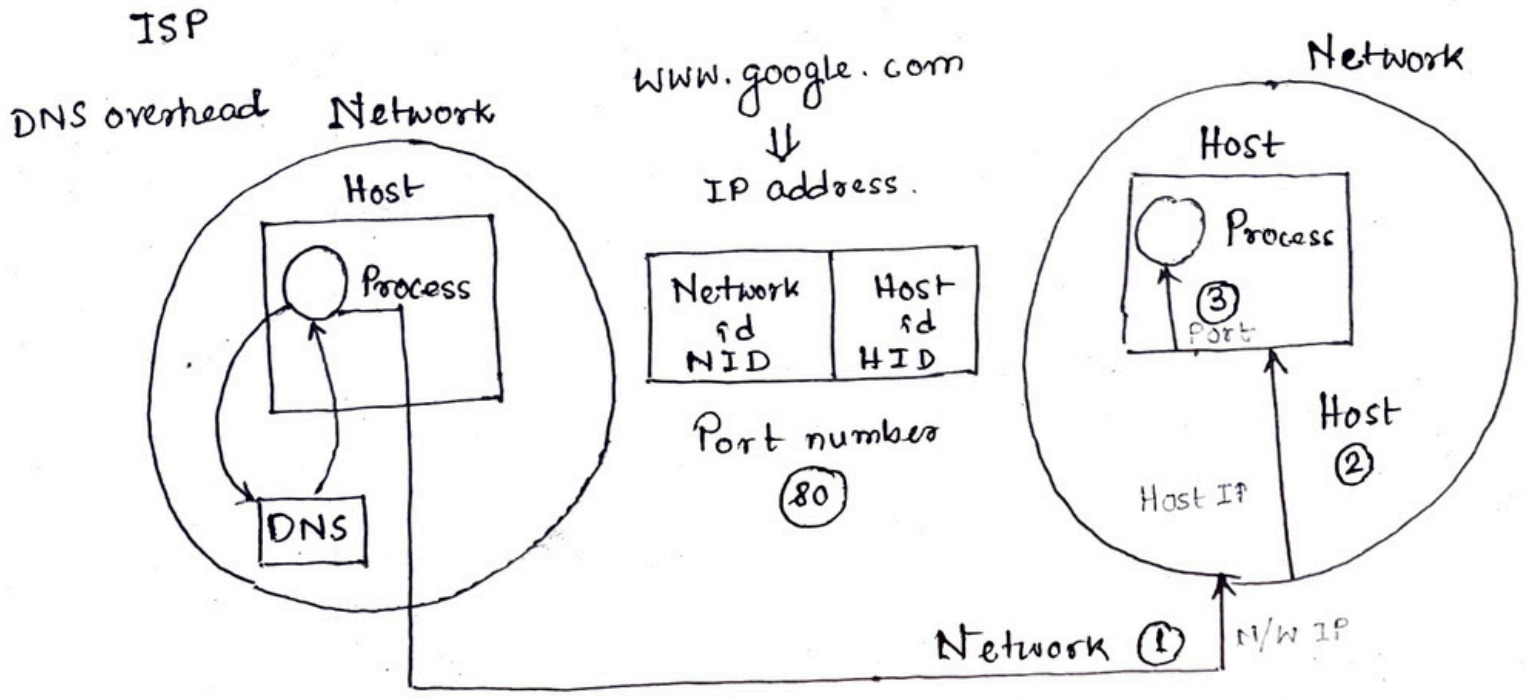
GATE CSE NOTES

by

UseMyNotes

IP address subnetting supernetting



→ Domain name service (DNS) provided by ISP to convert domain name to IP address.

→ Port number used to identify a particular process in the host. For well known services the port numbers are already predefined -

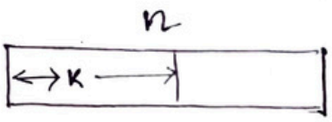
http : 80 smtp : 25 ssh : 22

ftp : 21, 20 https : 443 DHCP : 67, 68

→ ISP provides with DNS. Overhead for this conversion of domain name to IP address is called DNS overhead. To prevent this overhead, we have DNS cache which is a temporary storage of information about previous DNS lookups on a machine's OS or web browser. Keeping a local copy of a DNS lookup allows the OS or browser to quickly retrieve it and thus a website's URL can be resolved to its corresponding IP much more efficiently.

• Binary Number System.

If we choose k bits, the address space/number space will be divided into 2^k parts.



2^n combinations

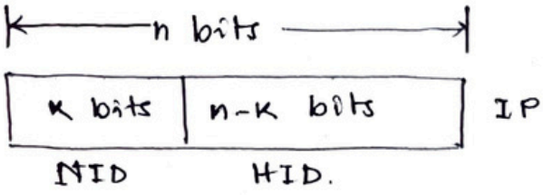
2^k parts

3 bits — Choosing 2 bits $= 2^2$ parts

000	Part 1 (00)
001	
010	Part 2 (01)
011	
100	Part 3 (10)
101	
110	Part 4 (11)
111	

2^k parts $= 2^n$ numbers.

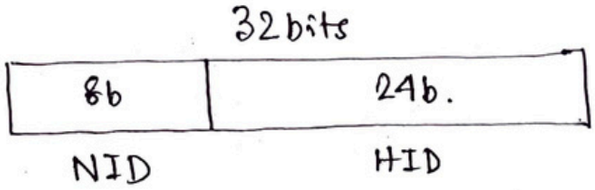
1 part $= 2^{n-k}$ numbers. $\Rightarrow$



$\Rightarrow$ Size of each N/W $= 2^{n-k}$

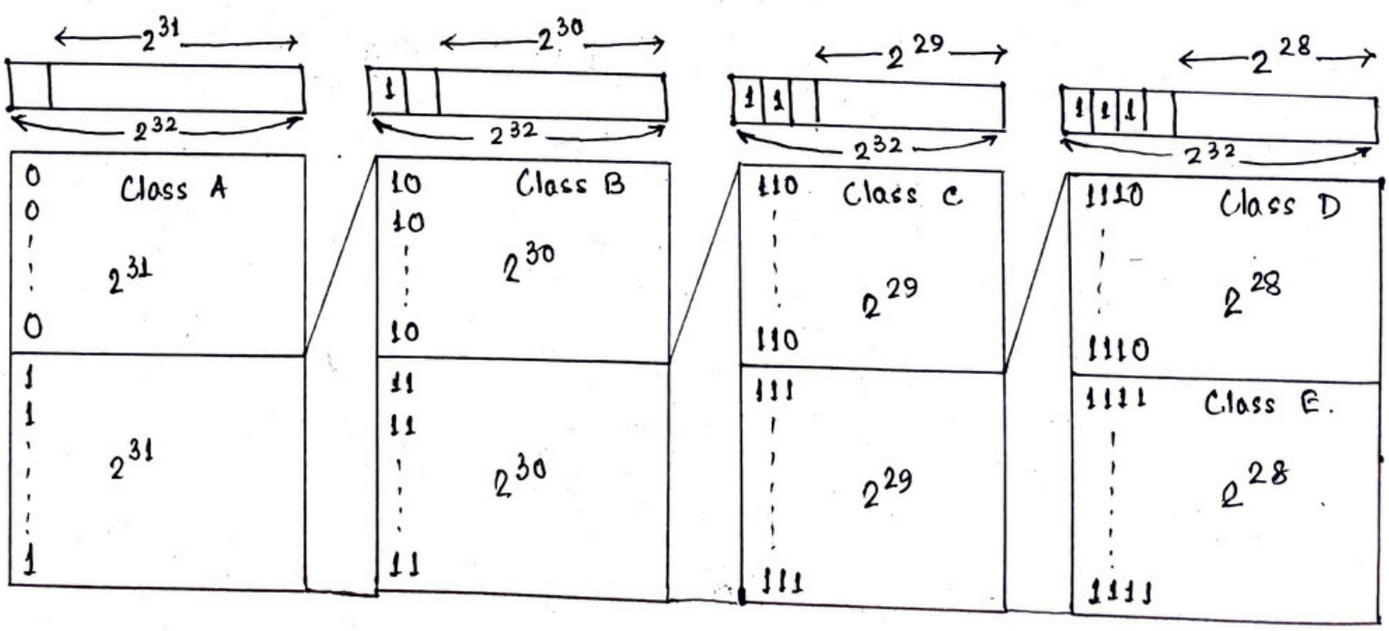
IP address size = 32 b

$\Rightarrow$ 2^{32} IP addresses possible.



$2^8 = 256$ Networks, each of size 2^{24} = 16 million hosts

* Classful IP address classification.



Dynamic host config protocol
Point-to-point protocol over Ethernet

* IP address. Internet Protocol Address.

Unique address assigned to each computing device on an network.

→ IP addresses types –

a) Static IP address. : Once assigned to a N/W element always remains the same. Configured manually. Some ISPs don't provide static IP addresses. More costly than dynamic IP addresses.

b) Dynamic IP address : Temporarily assigned IP address to a N/W element. Can be assigned to a different device if it is not in use. DHCP or PPPoE assigns dynamic IP addresses.

→ IP address format.: 32bit binary address written as 4 numbers (octets) separated by dots. Octets divided into Net ID and Host ID. Net ID represents the IP address of the N/W & is used to identify the N/W. Host ID represents the IP address of the host & used to identify the host within the N/W.

→ Classes of IP addressing –

i) Classful

ii) Classless (CIDR)

→ Classful addressing

1. Class A : If the 32 bit address starts with bit 0.
NID 8 bits ; HID 24 bits.

IP addresses = 2^{31}.

Networks = $2^7 - 2 = 126$

hosts = $2^{24} - 2$

Range [1, 126] | 0, 127 unused.

Min	0000 0000	0
Max	0111 1111	127

Class A is used by organisations requiring very large N/Ws.

2. Class B : 32 bit address starting with '10' bit

NID 16 bits ; HID 16 bits

IP address = 2^{30}

Networks = 2^{14}

hosts = $2^{16} - 2$

Range [128, 191]

Min	10 00 0000	128
Max	10 11 1111	191

Used by organizations requiring medium N/Ws like IRCTC, banks etc.

3. Class C : 32 bit address starting with 110.

NID 24 bits; HID 8 bits

IP addresses = 2^{29}

Networks = 2^{21}

hosts = $2^{8} - 2$

Range [192, 223]

Min	110 00000	192
Max	110 11111	223

Used by organisations requiring small to medium size N/Ws. (like colleges, small offices etc.)

4. Class D : 32 bit address starting with 1110.

IP addresses = 2^{28}

Range [224, 239]

Min	1110 0000	224
Max	1110 1111	239

Class D is reserved for multicasting.

In multicasting, there's no need to extract host address from IP address.

5. Class E : 32 bit address starting with 1111.

Not divided into NID, HID

IP addresses = 2^{28}

Range [240, 255]

Min	1111 0000	240
Max	1111 1111	255

Reserved for experimental purposes.

NB

1. All the hosts in a single N/W always have the same NID, but different HID.

2. 2 hosts in 2 different N/Ws can have same HID.

3. A single N/W interface can be associated with more than one IP addresses.

4. No relation between IP and MAC address of a host.

5. IP address of a N/W is obtained by setting all bits for HID to zero.

6. Class A N/Ws accounts for half of the total available IP addresses.

✓ 7. In class A, 0.0.0.0 is reserved for broadcasting requirements and 127.0.0.1 is reserved for loopback address used for S/W testing.

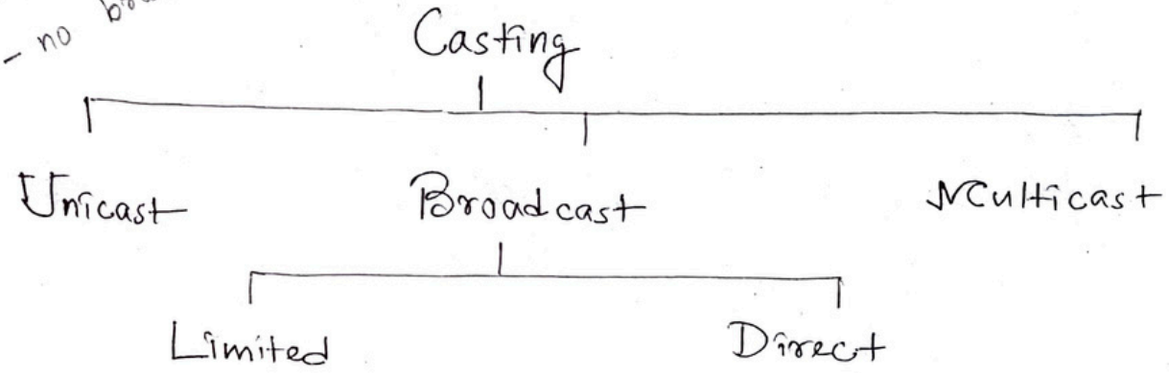
✓ 8. In all the classes, total number of hosts that can be configured are 2 less. When all HID bits are 0, it represents NID of the N/W, when all 1, it represents the DBA. (Direct Broadcast address)

9. Only those devices which have the network layer will have IP address.

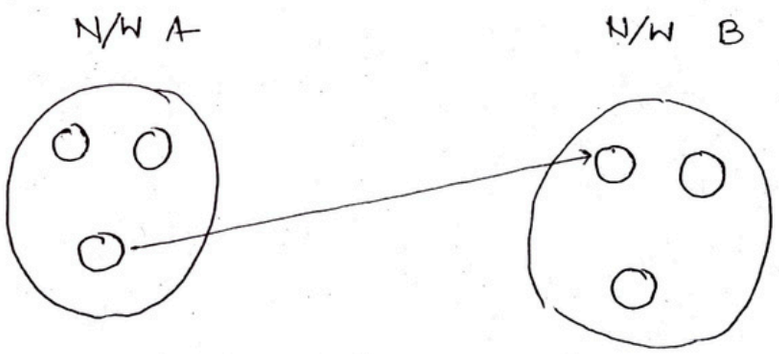
So, switches, hubs and repea-lers does not have any IP address.

* Casting Transmitting data (stream of packets) over the N/H.

(for IPv4 / IPv6 - no broadcasting)



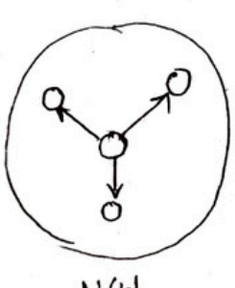
1. Unicast : Transmitting data from one source host to one destination host.
One-to-one transmission.



2. Broadcast : Transmitting data from one source host to all other hosts residing in the same or other N/W. One-to-all transmission.

Based on recipient's N/H,

a) Limited broadcast. Residing in same N/H.

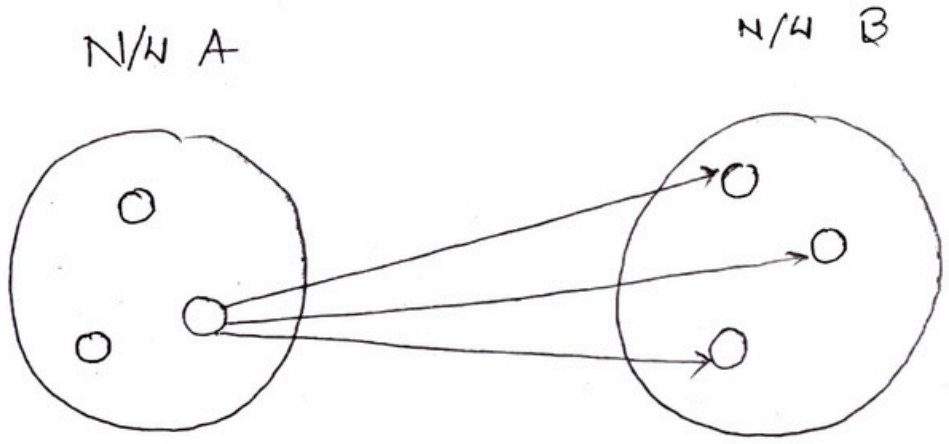


✓ LBA for any N/H = All 32 bits set to 1

Source address = IP address of host A

✓ Dest^{n} " = 255.255.255.255

b) Direct broadcast Residing in some other N/W.



DBA for any N/W is the IP address where N/W ID is the IP address of the N/W where all destination hosts are present, and Host ID bits are all set to 1.

eg. Host A (IP 11.1.2.3) sending data to all other hosts residing on the N/W having IP address 20.0.0.0.

Source address = 11.1.2.3

Dest^n address = 20.255.255.255.

3. Multicast : Transmitting data from one source host to a particular group of hosts having interest in receiving the data. One-to-many transmission.

eg. Sending a message to a particular group on WhatsApp, teleconference etc.

Multicast makes use of IGMP (Internet Group Management Protocol) to identify its group. Each group is assigned with an IP address from class D of IPv4.

* IP address vs. MAC Address.

12 digit HEX
6 byte Binary

Desc.	IP address 32b	MAC Address 48b
1. Acronym	Internet Protocol	Media Access Control.
2. Address type	Logical address. in N/W layer.	Physical address. in DLL.
3. Provided by	Assigned by user/admin, DHCP or ISP.	Hardware manufacturer (of NIC card)
4. Length	IPv4 uses 32 bit address (dotted notation), IPv6 uses 128 bit in Hex notation.	48 bit address that contains 6 group of 2 Hex digits, separated by hyphens, or colons.
5. Use of classes	IPv4 uses A, B, C, D, E classes for addressing.	No classes used.
6. Spoofing	IP address spoofing possible.	MAC address spoofing possible.
7. Type.	Software address.	H/W address
8. Work on	N/W layer of OSI model.	Data link layer of OSI model.
9. Used for	Numeric representation of a device that uses TCP/IP.	Numeric rep^{n} of a device that uses ethernet.
10. Subnetting	Used.	Not used.
11. Resolution	Address resolution protocol (ARP) used for resolving IP address into physical (MAC) address.	Reverse ARP (RARP) used for resolving physical (MAC) address into IP address.

4 segments
decimal.
192.14.32.10

6 segments
Hex 2 digits each segment
AA:BB:CC:DD:EE:11

$A \times 16^1 + A \times 16^0$
$= 10 \times 16 + 10$
$= 170_{10}$

NB

1.

Range of first octet	Class.
[1, 126]	A
[128, 191]	B.
[192, 223]	C
[224, 239]	D
[240, 254]	E.

NID. #bits

8	0000 0000 0
	1 — 0 — 128
16	11 — 0 — 192
	111 — 0 — 224
24	1111 0 240
	11111 0 248
	111111 00 252
	11111110 254
	11111111 255

2. For any given IP address, IP address of its N/W is obtained by setting all its host ID part bits to 0.

3. For any given IP address, DBA is obtained by setting all its host ID part bits to 1.

4. For any given IP address, LBA is obtained by setting all its bit to 1.

LBA = 255.255.255.255

5. Class D, E IP address are not divided into Net ID and host ID parts.

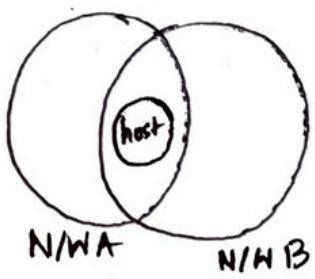
Q A device has to be having 2 or more IP addresses, the device is called -

1. Workstation
2. Router
3. Gateway
4. All.

→ All devices have a N/W layer. So, they will have at least one IP address. In TCP/IP suite, workstation and gateway have all the 5 layers. Router has only 3 layers last layer being network layer.

Workstation : A user may configure more than one IP addresses in his workstation. With more than one IP addresses, it remains present in more than one N/Ws. So, if one N/W goes down, it is always reachable from other N/Ws.

Note IP addresses are assigned to interfaces.



host present in 2 networks

When we buy a new laptop, we usually get 2-3 interfaces. Thus, a workstation can have more than one IP addresses.

Router : A router may be connected to various interfaces. Each interface has a unique IP address. Thus, a router may also have more than IP addresses.

Similare in the case with gateways because gateways are extension of routers.

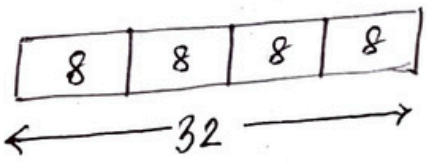
→ All 0 bits in HID → NID.

All 1 bits in HID → DBA
(Directed broadcast)

Number of IP addresses possible in a N/W of class A = 2^{31}, of class B = 2^{30}, of class C = 2^{29}, of class D, E = 2^{28}.

→ Dotted decimal representation of IP address.

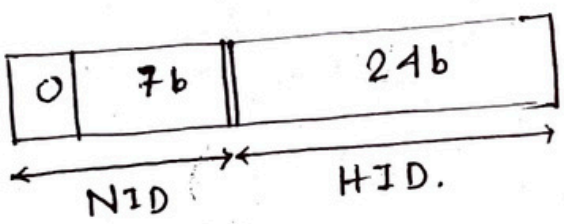
32 bits in 4 parts of 8 bits.



→ Class A starts with 0
" B " " 10
" C " " 110
" D " " 1110
" E " " 1111.

Any prefix of a class can't be a prefix of any of the other,
eg. 0 is not a valid prefix of any other class except class A.

→ Class A. (1-126)



1st octet

0 _ _ _ _ _ _ _
0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 1
1 1 1 1 1 1 1 1

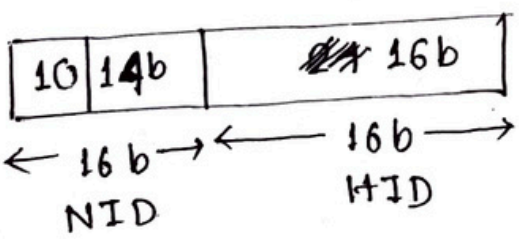
0
1
127

N/W = 2^7 = 128 (Theoretical)
Size of each N/W = 2^{24}
= 16 M (# host)

Big corporations will use class A.

0, 127 are not used.
So, practically # N/W = 126
Range in class A 1–126.

→ Class B (128-191)



N/W = 2^{14} = 16K Networks.
ip addresses / N/W = 2^{16}
Range in class B 128 – 191

10 _ _ _ _ _ _
0 0 0 0 0 0
0 0 0 0 0 1
1 1 1 1 1 1
8b

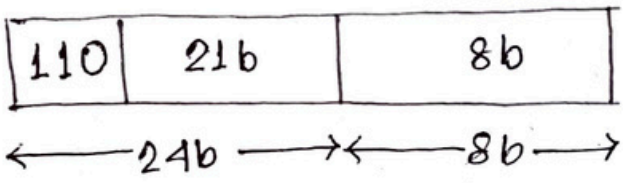
128
129
191

64 numbers × 2^8 = 2^{14} N/Ws
for 2nd octet of NID.

128.0
128.1
128.255
129.0
129.1
129.255
191.255

2^{14} N/Ws

→ Class C (192 - 223)



N/Ws = 2^{21}.

IP addresses / N/W = 2^8
= 256

Range of class C = 192 – 223

110 – – – – –

0 0 0 0 0 → 192
0 0 0 0 1 → 193
⋮
1 1 1 1 1 → 223

} 32×2^{16} = 2^{21} N/Ws

192.0.0
192.0.1
192.0.2
⋮
192.0.255
192.1.0
⋮
192.1.255
⋮
192.255.255.

→ For class D and E, entire is left as IP address.

Class D (224 - 239)

1110 – – – –

0 0 0 0 → 224
⋮
1 1 1 1 → 239

Class E (240 - 255)

1111 – – – –

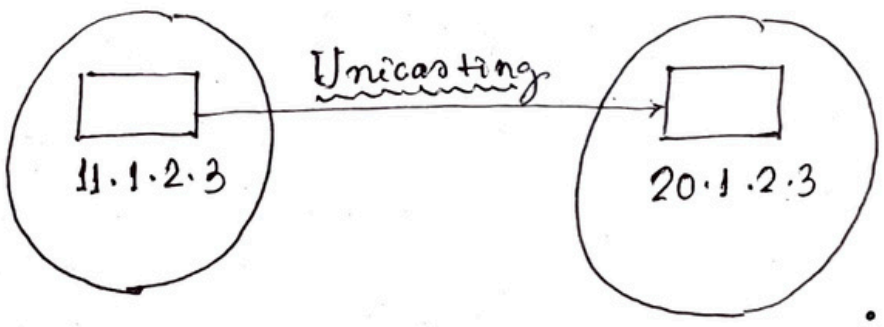
0 0 0 0 → 240
⋮
1 1 1 1 → 255

2^{28} IP addresses for class D, E.

→ #hosts will always be less by 2.

We don't use 2 IP addresses in every class (all 0s, all 1s).

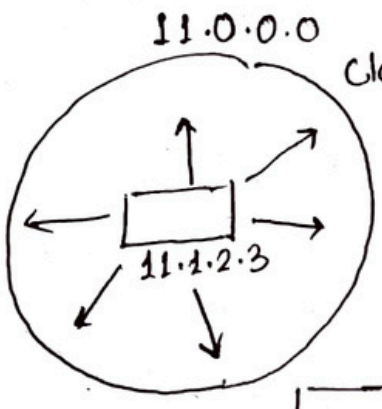
* Casting
  - → Unicast (One host to one host)
  - → Broadcast (One host to many hosts)
    - → Limited (same network broadcasting)
    - → Directed (different network broadcasting)



Data packet

Data	11.1.2.3	20.1.2.3
	Source address	Dest^n address

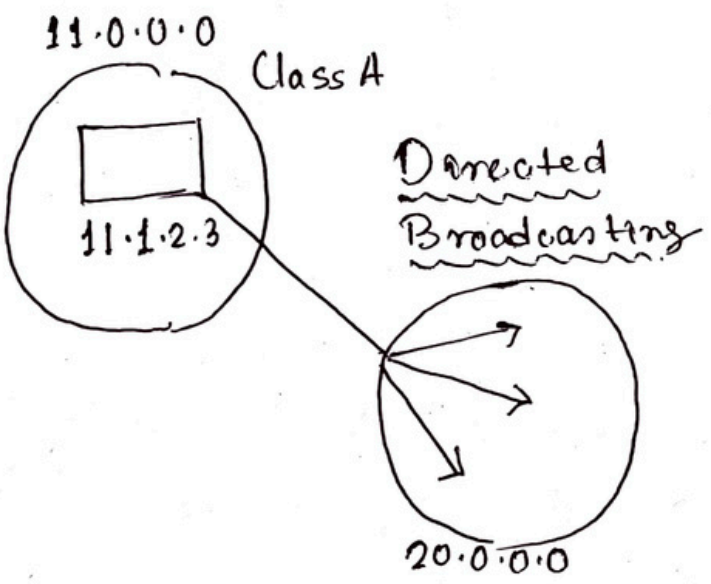
- In the host id, if there is all 0's, it designates the network This is why, we don't use the 1st IP addr.



Limited Broadcasting.

Data packet.

Data	11.1.2.3	255.255.255.255



Data	11.1.2.3	20.255.255.255

Data packet.

- When dest^n addr. is 255.255.255.255 then the packet is sent to all hosts in the N/W.

Limited broadcasting addr.

LBA = 255.255.255.255

- In the host id, if there is all 1's, it means it is used for directed broadcasting for different N/W. This is why, we don't use this IP address.

Direct broadcast address : NID, HID(all 1's)

• Example. C_A : 1 – 126 8.24 C_c – 192 – 223 24,8

C_B : 128 – 191 16.16

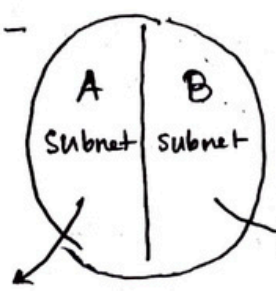
IP	NID	DBA	LBA.
1.2.3.4.	1.0.0.0	1.255.255.255	255.255.255.255
10.15.20.60	10.0.0.0	10.255.255.255	n
130.1.2.3	130.1.0.0	130.1.255.255	n
150.0.150.150	150.0.0.0	150.0.255.255	n
200.1.10.100	200.1.10.0	200.1.10.255	n
220.15.1.10	200.15.1.0	200.15.1.255	n
250.0.1.2	–	–	–
300.1.2.3	–	–	–

* Subnetting

Dividing a single N/N into multiple subnetworks. It improves security and also the maintenance, administration of subnets are easy.

Each subnet has its unique network address known as its subnet ID. The subnet ID is created by borrowing some bits from the host ID part of the IP address. No. of bits borrowed depends on the no. of subnets created.

eg. 2 subnets. class c



200.1.2.0 _____

Range 0 – 127 $2^{7}-1$

NID = 200.1.2.0

DBA = 200.1.2.127

200.1.2.1 _____

Range 128 – 255 $2^{8}-1$

NID = 200.1.2.128

Directed broadcast address (DBA)

= ~~200.1.2.127~~

200.1.2.255

200.1.2.x

SID	New HID

Ambiguity ~ NID of the main network and NID of the first subnet same. Also, DBA of the network and DBA of the last subnet are same [Which network or subnet to send packet, depends on situation. If packet is coming from outside, packet should be transmitted to all hosts of the network. If packet is coming from inside, packet should be transmitted to the subnet B's all hosts.

→ 200.1.2.69 S_A eg

Disadvantages of subnetting

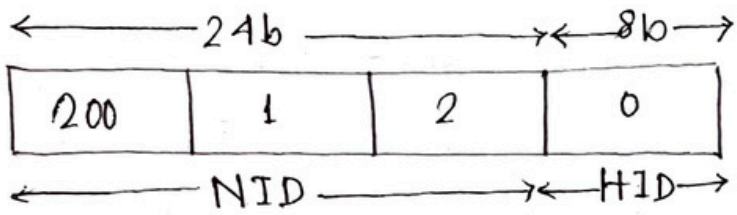
1. Subnetting leads to loss of IP addresses. 2 IP addresses are wasted for each subnet. One IP address is wasted for its network address (SID), another IP address is wasted for its direct broadcasting address (DBA).

2. Subnetting leads to complicated communication process. After subnetting, the communication process becomes complex involving the 4 steps —

1. Identifying the network
2. Identifying the subnet
3. Identifying the host
1. Identifying the process.

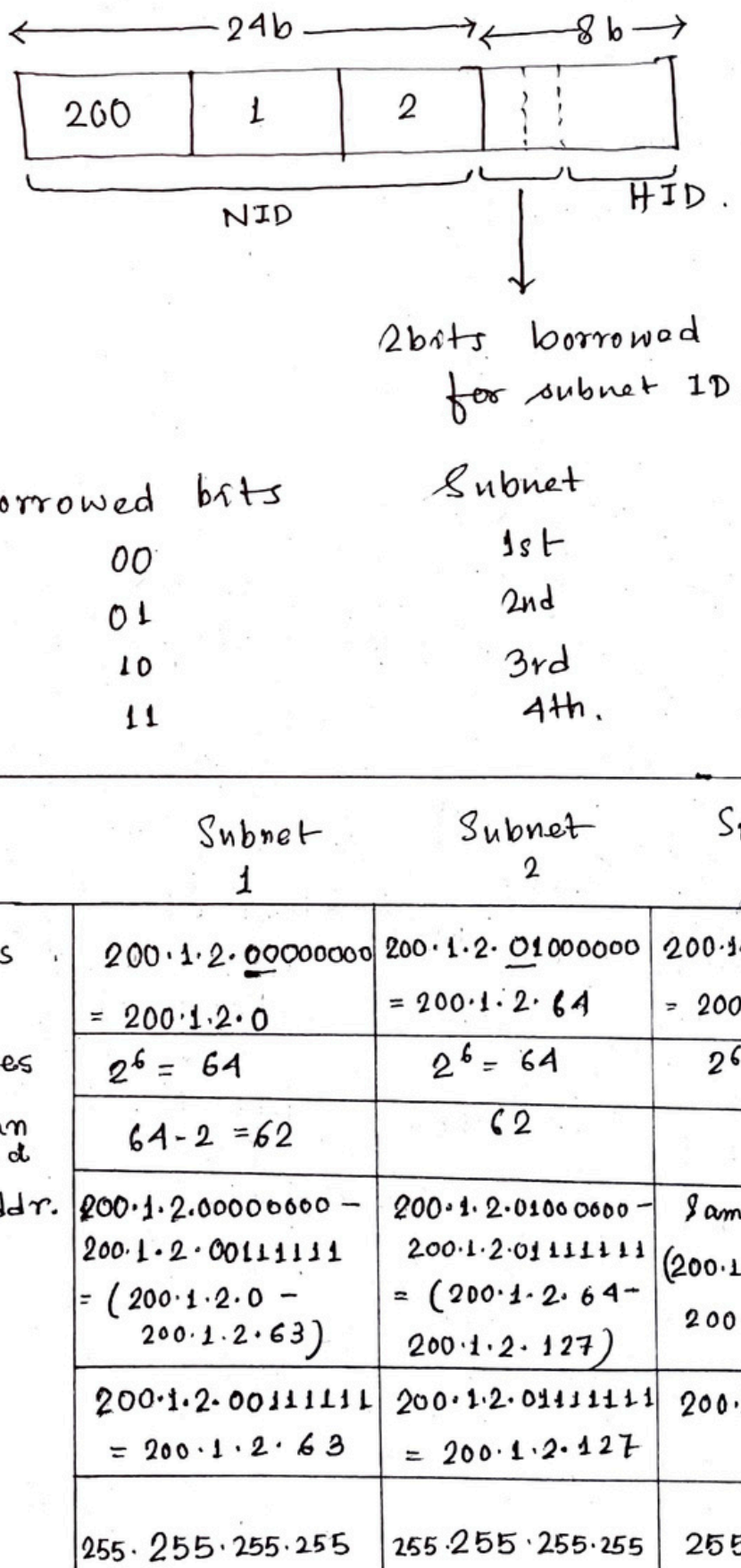
eg We have a big single network having IP address 200.1.2.0. We want to divide this N/W into 4 subnets.

N/W belongs to class C



For creating 4 subnets & to represent their subnet IDs, we require 2 bits.

So, we borrow 2 bits from the HID part.



Now,

Borrowed bits	Subnet	Subnet ID
00	1st	SNID /26
01	2nd	
10	3rd	
11	4th.	

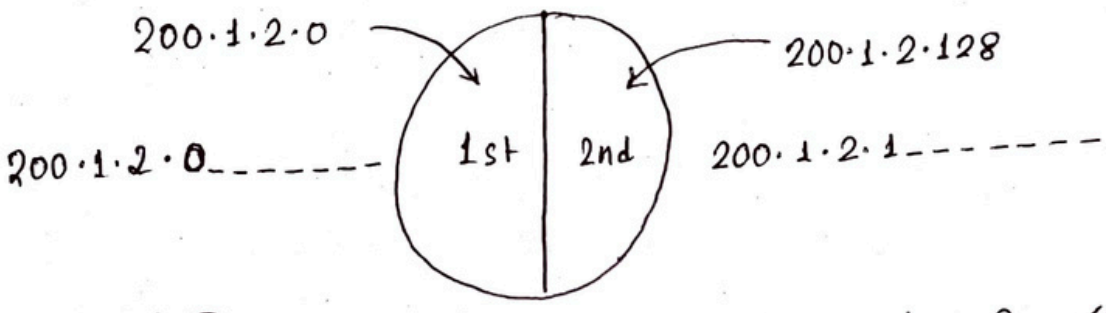
	Subnet 1	Subnet 2	Subnet 3	Subnet 4.
IP address	200.1.2.00000000 = 200.1.2.0	200.1.2.01000000 = 200.1.2.64	200.1.2.10000000 = 200.1.2.128	200.1.2.11000000 = 200.1.2.192
# of IP addresses	$2^6 = 64$	$2^6 = 64$	$2^6 = 64$	$2^6 = 64$
#hosts that can be configured	64-2 = 62	62	62	62
Range of IP addr.	200.1.2.00000000 – 200.1.2.00111111 = (200.1.2.0 – 200.1.2.63)	200.1.2.01000000 – 200.1.2.01111111 = (200.1.2.64 – 200.1.2.127)	Same way (200.1.2.128 – 200.1.2.191)	(200.1.2.192 – 200.1.2.255)
DBA	200.1.2.00111111 = 200.1.2.63	200.1.2.01111111 = 200.1.2.127	200.1.2.191	200.1.2.255
LBA	255.255.255.255	255.255.255.255	255.255.255.255	255.255.255.

Eg. Big single N/W having IP 200.1.2.0. Subnetting into 3 subnets.

Subnetting will be performed in 2 steps:

1. Dividing the given network into 2 subnets
2. Dividing one of the subnets (1 or 2) into 2 subnets.

Step 1: Dividing N/W into 2 subnets :-

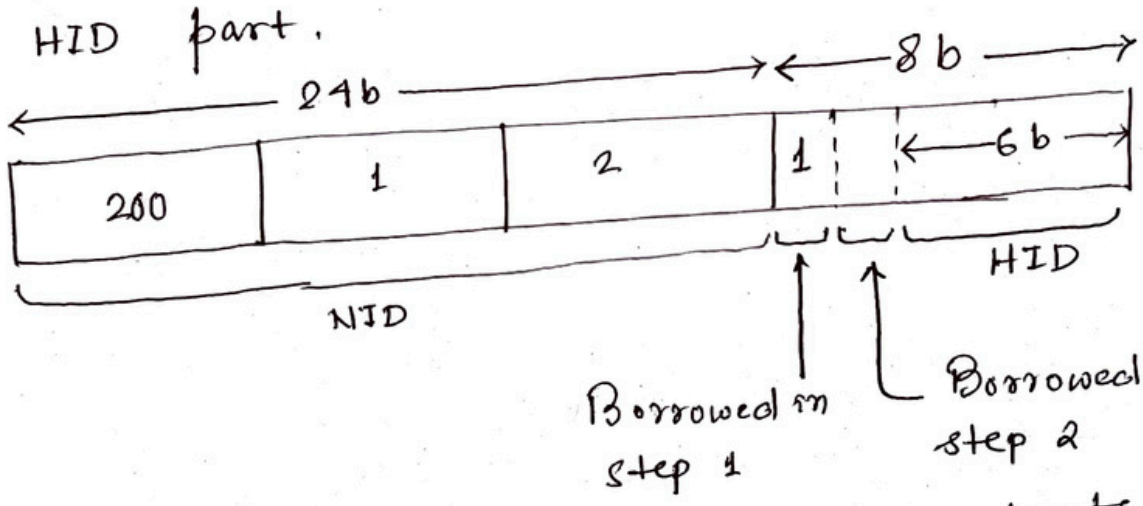


$2^x = 3$

Step 2: Dividing one subnet into 2 subnets :-

We do subnetting of the 2nd subnet (200.1.2.128)

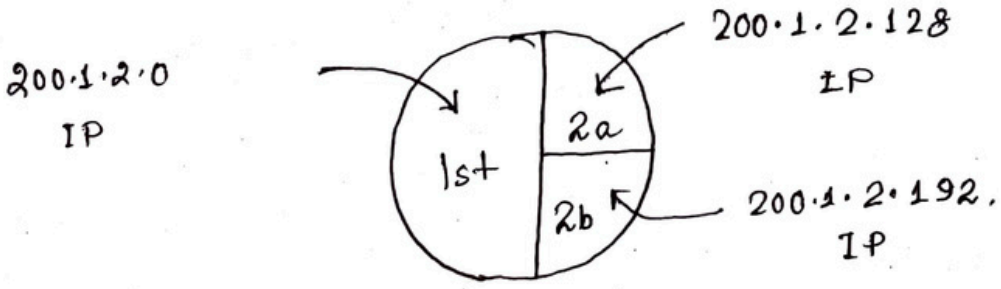
For creating 2 subnets & to represent their subnet IDs, we require 1 bit. So, we borrow 1 bit from HID part.



IP addresses of further divided subnets in the subnet 200.1.2.128 are

200.1.2.10 000000 = 200.1.2.128

200.1.2.11 000000 = 200.1.2.192.



	1	2a	2b
IP address	200.1.2.0	200.1.2.128	200.1.2.192
#IPaddress	$2^7 = 128$	$2^6 = 64$	$2^6 = 64$
#hosts that can be configured	128 - 2 = 126	64 - 2 = 62	64 - 2 = 62
Range of IP addr.	200.1.2.00000000 - 200.1.2.01111111 = (200.1.2.0 - 200.1.2.127)	200.1.2.10000000 - 200.1.2.10111111 = (200.1.2.128 - 200.1.2.191)	200.1.2.11000000 - 200.1.2.11111111 = (200.1.2.192 - 200.1.2.255)
DBA	200.1.2.127	200.1.2.191	200.1.2.255

- Subnet address = First IP address

  Broadcast address = Last IP address.

- **Subnet Mask** It is a 32 bit number which is a sequence of 1's followed by a sequence of 0's where -
  - 1's represent the global network ID part & the subnet ID part
  - 0's represent the host ID part.

Used to determine subnet

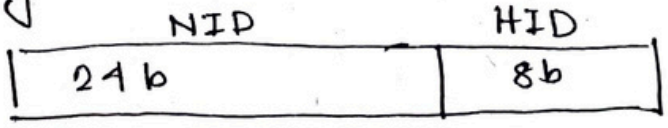
Calculating subnet mask -

For any given IP address, the subnet mask is calculated -

- by setting all the bits reserved for NID part & subnet ID part to 1.
- by setting all the bits reserved for HID part to 0.

eg. N/N having IP address 200.1.2.0

Class c IP.



Subnet mask -

11111111. 11111111. 11111111. 00000000

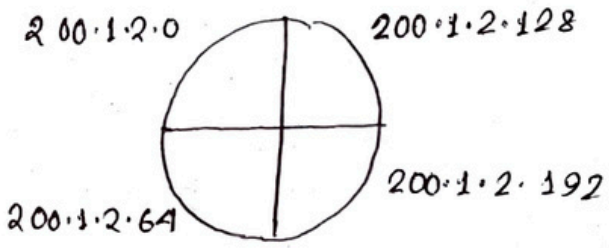
= 255. 255. 255. 0.

Use of subnet mask — ANDing with dest. IP

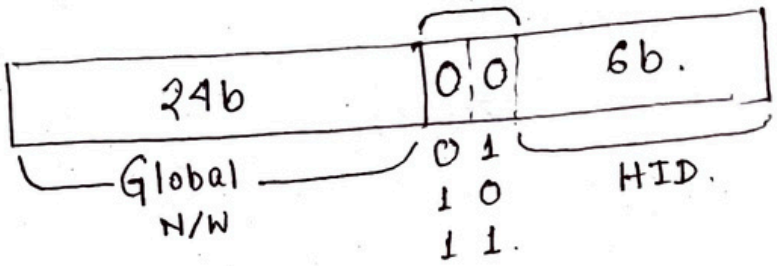
Subnet mask is used to determine to which subnet the given IP address belongs to.

eg. Single network 200.1.2.0 divided into 4 subnets.

Class C.



For each subnet



Subnet mask for each subnet in the global network 200.1.2.0 =

11111111 . 11111111 . 11111111 . 11 000000

= 255 . 255 . 255 . 192 .

Fixed length subnetting — all subnets have same subnet mask since the size of each subnet is same.

- Types of subnetting

1. Fixed length or classful subnetting

Divides the N/W into subnets where all the subnets are of same size, have equal no. of hosts, have same subnet mask.

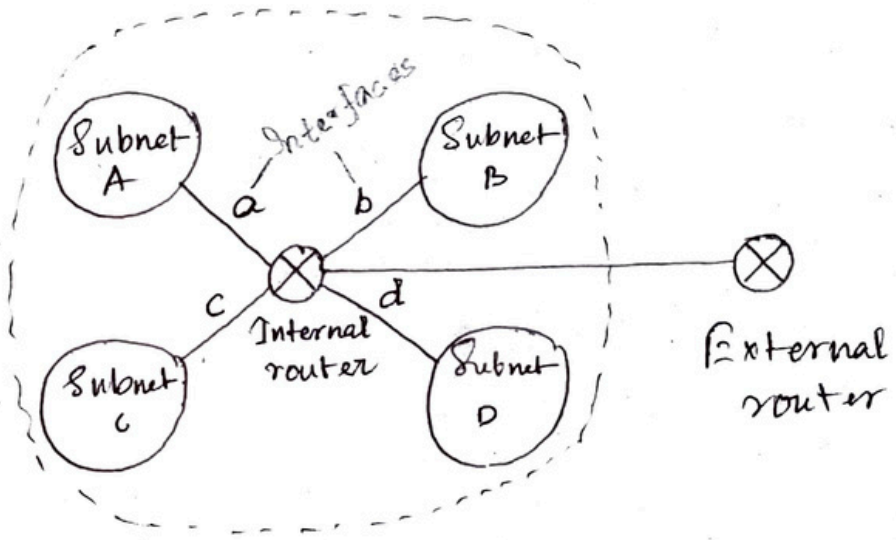
2. Variable length or classless subnetting.

Divides the N/W into subnets where all the subnets are not of same size, don't have equal no. of hosts, don't have same subnet mask.

0	A 1-126
10	B 128-191
110	C 192-223
1110	D 224-239
1111	E 240-254

Arrangement of subnets.

All the subnets are connected to an internal router. Internal router is connected to an external router. The link connecting the internal router with a subnet is an interface.



Physical view.

Working:

When a data packet arrives,

- External router forwards the data packet to the internal router.
- Internal router identifies the interface on which it should forward the incoming data packet.
- Internal router forwards the data packet on that interface.

* Routing Table.

A table is maintained by the internal router called routing table. It helps the internal router to decide on which interface the data packet should be forwarded.

Routing table consists of the following 3 fields —

1. IP address of the destination subnet
2. Subnet mask of the subnet
3. Interface.

eg. N/N subnetted into 4 subnets.

IP addresses –

1. 200.1.2.0 (S_A)
2. 200.1.2.64 (S_B)
3. 200.1.2.128 (S_C)
4. 200.1.2.192 (S_D).

Routing table –

Destination IP	Subnet mask (.11000000)	Interface.
200.1.2.0	255.255.255.192	a
200.1.2.64	255.255.255.192	b
200.1.2.128	255.255.255.192	c
200.1.2.192	255.255.255.192	d
Default	0.0.0.0	e (default interface)

Working of Routing Table

When a data packet arrives to the internal router. –

Step 1 – Router performs bitwise ANDing of destⁿ IP address (mentioned in the data packet) and all the subnet masks one by one.

Step 2 – Router compares each result with their corresponding IP address of the destination subnet in the routing table. Now 3 cases may arise –

a) If there occurs only one match, router forwards the data packet the the corresponding interface.

b) If there occurs more than one match, router forwards the data packet on the interface corresponding to the longest subnet mask (longest run of 1's).

c) If there occurs no match, router forwards the data packet on the interface corresponding to the default entry.

→ NB

✓(i) In fixed length subnetting, all the subnets have the same subnet mask. So, bitwise ANDing is performed only once. If the result matches to any of the destn subnet IP address, router forwards the data packet on its corresponding interface. Otherwise, it is forwarded on the default interface.

(ii) In variable length subnetting, all the subnets don't have same subnet mask. So, bitwise ANDing is performed once with each subnet mask.

✓(iii) A host may also be directly connected to the router. In that case, there exists a host specific route from the router to the host. Router saves the IP address of that host in the Destination network column. ✓Router saves 255.255.255.255 in the subnet mask column. ANDing of its destn address & subnet mask yields the IP address of the host. When a data packet arrives for that specific host, bitwise ANDing is performed. When the result of ANDing is the IP address of the host, packet is forwarded to its host specific route.

(iv) Subnet mask for default route = 0.0.0.0

Subnet mask for Host specific route = 255.255.255.255

eg.

Dest^n IP in packet: 11001000 . 00000001 . 00000010 . 10000010
200 1 2 130

24-2-6

AND

Subnet mask: 11111111 . 11111111 . 11111111 . 11000000
255 255 255 192.

11001000 . 00000001 . 00000010 . 10000000
200 . 1 . 2 . 128.

Dest^n subnet IP address.

Q. In a class B N/W on the internet has a subnet mask of 255.255.240.0. What is the max. no. of hosts per subnet?

→ Binary rep^n of subnet mask.

11111111 . 11111111 . 1111 0000 . 00000000
NID. 20 b HID 12b.

In class B, upper 16 bits form the N/W address & lower 16 bits form the host.

No. of hosts per subnet = $2^{12} - 2$ = 4094. (Ans)

[Also, # bits reserved for subnet ID = 20 - 16 b
= 4 b

No. of subnets possible = $2^4 = 16$]

→ NB

1. Defaut subnet masks.

Class	SM.
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

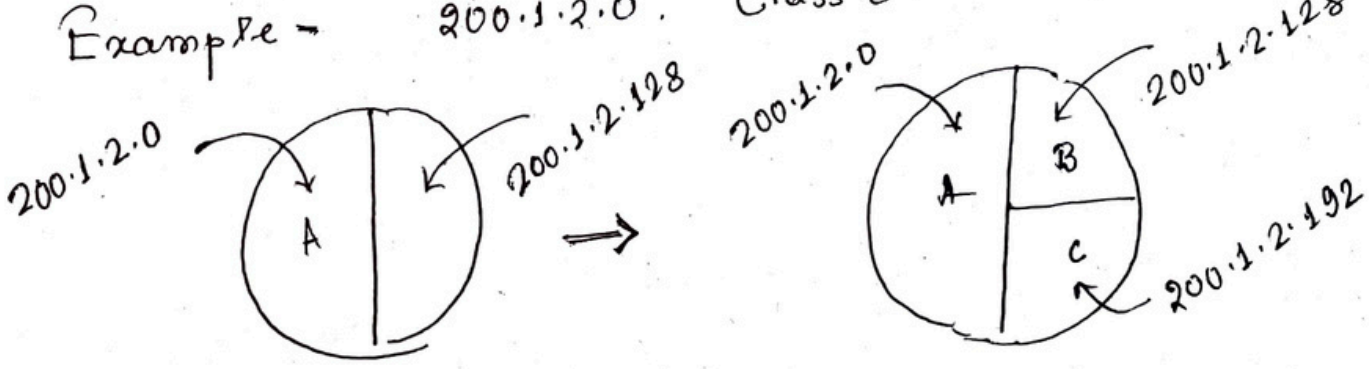
2. Network size is the total no. of hosts present in it. Networks of same size always have the same subnet mask. N/Ws of different size always have the different subnet mask.

3. For a N/W having larger size, its subnet mask will be smaller (no. of 1's less). For a N/W having smaller size, its subnet mask will be larger (no. of 1's more).

4. We should not use 255.255.255.15 like subnet masks. 15 ≡ 00001111. In this case, we can't divide the ranges in subnets properly.

- Variable length subnet masking (VLSM)

Example - 200.1.2.0. Class C.



For subnet A,

24+1 7
1's 0's

SM = 255.255.255.128

For subnet B and C,

24 + 2 bits 6 bits

1's 0's

SM = 255.255.255.192.

0000 0000	0
1000 0000	128
1100 0000	192
1110 0000	224
1111 0000	240
1111 1000	248
1111 1100	252
1111 1110	254
1111 1111	255

eg

	Subnet mask	# hosts	Subnets in class A	Subnets in class B	Subnets in class C
A	255.0.0.0	$2^{24}-2$	1	-	-
	255.128.0.0	$2^{23}-2$	2	-	-
	255.192.0.0	$2^{22}-2$	2^2	-	-
	255.240.0.0	$2^{20}-2$	2^4	-	-
B	255.255.0.0	$2^{16}-2$	2^8	1	-
	255.255.254.0	2^9-2	2^{15}	2^7	-
C	255.255.255.0	2^8-2	2^{16}	2^8	1
	255.255.255.224	2^5-2	2^{19}	2^{11}	2^3
	255.255.255.240	2^4-2	2^{20}	2^{12}	2^4
			2^{27-8}	2^{27-16}	2^{27-24}

as 8b NID ⇒ rem. 19b for subnets

Q. Routing table.

Dest^n IP	SM	Interface.
144.16.00	255.255.0.0	eth0
144.16.64.0	255.255.224.0	eth1
144.16.68.0	255.255.255.0	eth2 ✓
144.16.68.64	255.255.255.224	eth3.

Packet bearing destn addr. 144.16.68.117 will go to which interface ?

→ . 144.16.68.117 AND 255.255.0.0 = 144.16.0.0. (match)

144.16.68.117 AND 255.255.224.0 = 144.16.64.0 (match)

144.16.68.117 AND 255.255.255.0 = 144.16.68.0 (match)

144.16.68.117 AND 255.255.255.224 = 144.16.68.96

More than one match. 255.255.255.0 has longest run of 1's among the matches.

Router forwards the packet to the interface eth2.

Q. Default route can be described as —

i) Dest^n values of 0.0.0.0 in the routing table

ii) It can be used if N/W has only one next hop router.

iii) It's useful in keeping routing table small.

iv) All.

- When any host connects to the internet, ISP provides following 4 things to the host:

1. IP address – ISP assigns an IP address to the host so that it can be uniquely identified on the internet. (DHCP)

2. Default Gateway – Default router connected to the N/W in which the host is present, is the default gateway for the host.

3. Subnet mask – Used to determine to which N/W the given IP address belongs to.

4. Domain Name Service (DNS) – Used to translate the domain name into an IP address.

- Subnet mask use.

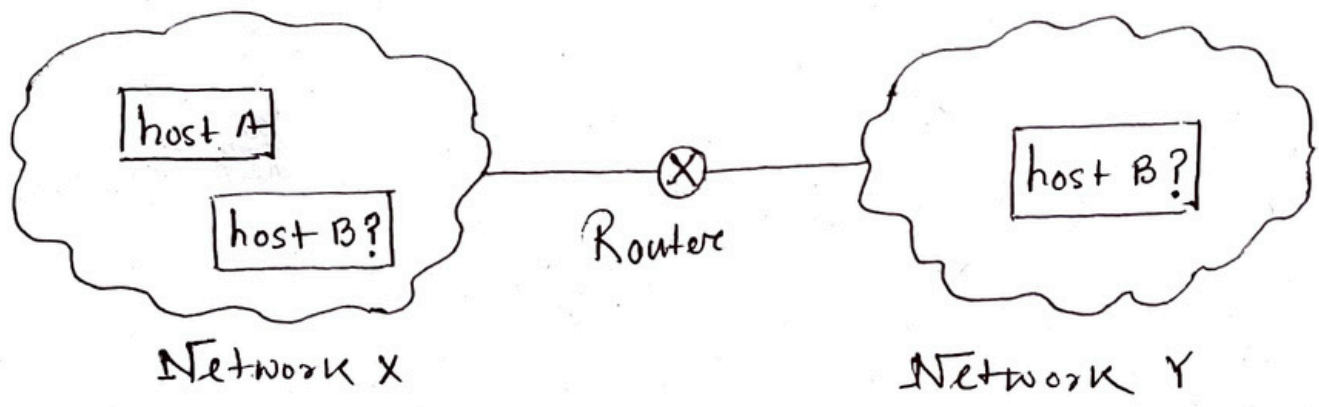
Host uses its subnet mask to determine whether the other host it wants to communicate with is present within the same N/W or not.

If the dest^n host is present within the same N/W, then source host sends the packet directly to the dest^n host.

If the destination host is present in some other N/W, then source host routes the packet to the default gateway. Router then sends the packet to the destⁿ host.

Example –

There's a host A present in some N/W X. There's a host B. Host A wants to send a packet to host B. Before transmitting the packet, host A determines whether host B is present within the same N/W or not



To determine whether destⁿ host is present within the same N/W or not, source host follows the following steps –

Source host A
Destⁿ host B.

Step 1 Source host computes its own N/W address using its own IP address & subnet mask. After this, source host obtains its N/W address wrt itself. (AND opⁿ)

Step 2 Source host computes the N/W address of destⁿ host using destⁿ IP address & its own subnet mask. After this, source host obtains the N/W address of destⁿ host wrt itself. (AND opⁿ)

Step 3 Source host compares the 2 results obtained –

cases : 1. If same, source host assumes that the destⁿ host is present in the same N/W. Source host sends the packet directly to the destⁿ host.
2. If different, source host assumes that the destⁿ host is present in some other N/H. Source host sends the packet via router to the destⁿ host.

NB

i) Each host knows only its own subnet mask. It does not know the subnet mask of any other host.

ii) The conclusion drawn by a host about the presence of other host within the same or other N/W might be wrong. (Subnetting can be different (NW-8 20:00)

Considering, host A draws some conclusion about host B. Then, same conclusion might not be drawn by host B about host A. Both the hosts have to perform the above procedure separately at their ends to conclude anything.

Q. 2 computers C1 and C2 are configured as follows –

	IP	net mask
C1	203.197.2.53	255.255.128.0
C2	203.197.75.201	255.255.192.0

Which is true?

1. C_1 & C_2 both assume they are on same N/W.
2. C_1 assumes C_2 is on same N/W, but C_2 assumes C_1 is on a different N/W.

→ At C1,

C1 computes its N/W address

I_1 S_1

203.197.2.53 AND 255.255.128.0

= 203.197.0.0. NID_{11}

C1 computes N/W address of C2

I_2 S_1

203.197.75.201 AND 255.255.128.0

I_{21}

= 203.197.0.0 = C1 N/W address

So, C1 assumes that C2 is on the same N/W.

At C2,

C2 computes its network address

203.197.75.201 AND 255.255.192.0

= 203.197.64.0

C2 computes N/W address of C1

203.197.2.53 AND 255.255.192.0

= 203.197.0.0

Since, results are different, C2 assumes C1 is one a different N/W.

- Unforeseen limitations to classful addressing.

1. During the early days of the internet, the seemingly unlimited address space allowed IP addresses to be allocated to an organisation based on its request rather than its actual need. As a result, addresses were freely assigned to those who asked for them without concerns about the eventual depletion of the IP address space.

2. The decision to standardize on a 32 bit address space meant that there were only ~~232~~ 2^{32} (4,294,967,296) IPv4 addresses available. A decision to support a slightly larger address space would have exponentially increased the number of addresses thus eliminating the current address shortage problem.

3. The classful A, B and C octet boundaries were easy to understand & implement, but they did not foster the efficient allocation of a finite address space. Problems resulted from the lack of a network class that was designed to support medium-sized organisations.

→ NAT used to deal with these problems.

Class C

For example, a /24, which supports 254 hosts, is too small while a /16, which supports 65534 hosts, is too large. In the past, sites with several hundred hosts were assigned a single /16 address instead of 2 /24 addresses. This resulted in a premature depletion of the /16 network address space. Now, the only readily available addresses for medium-sized organisations are /24s, which have the potentially negative impact of increasing the size of the global internet's routing table.

Class B

* Classless Addressing / Classless Inter-Domain Routing

Improved IP addressing system. (CIDR).
Makes the allocation of IP addresses more efficient.
It replaces the older classful addressing.

CIDR block - When a user asks for specific number of IP addresses, CIDR dynamically assigns a block of IP addresses based on certain rules. This block contains the certain required number of IP addresses as demanded by the user. This block of IP addresses is called CIDR block.

Rules for creating CIDR block

1. All the IP addresses in the CIDR block must be contiguous.
2. The size of the block must be power of 2. Size of the block is total no. of IP addresses contained in the block.
3. First IP address of the block must be divisible by the size of the block.

→ If any binary pattern consisting of (m+n) bits is divided by 2^n, then

- remainder is least significant n bits
- quotient is most significant m bits.

So, any binary pattern is divisible by 2^n, iff its least significant n bits are 0.

eg. 100.1.2.64.

⇓

01100100.00000001.00000010.01000000

6 zeros

Divisible by 2^5 or 2^6

Not divisible by 2^7.

CIDR Notation.

CIDR IP address looks like a.b.c.d/n

Ends with a number, called IP N/W prefix.

IP N/W prefix tells the number of bits used for the identification of N/W. Remaining bits are used for the identification of hosts in the N/W.

eg. 182.0.1.2/28 — 28 bits for NID, 4 bits for HID

→ for writing the CIDR representation, we can choose to mention any IP address from the CIDR block. The chosen IP address is followed by a slash & IP N/W prefix. We generally choose to mention the first IP address.

Q. CIDR representation 20.10.30.35/27. Find range of IP addresses in the block.

→ 27 bits Identification of N/W or block

(32-27) = 5 bits for HID.

Range = (00010100.00001010.00011110.001 00000 to
00010100.00001010.00011110.001 11111)

= (20.10.30.32 to 20.10.30.63)

Q. Consider a block of IP addresses ranging from 100.1.2.32 to 100.1.2.47.

1. Is it a CIDR block?
2. If yes, give CIDR representation.

→ i) All IP addresses are contiguous.

ii) No. of IP addresses = $47-32+1 = 16 = 2^4$

iii) 1st IP address 100.1.2.32

$32 \equiv 0010\,0000$

reduce only this much bits from right in the IP

100.1.2.32 is divisible by 2^4 since its least significant 4 bits are zero.

All rules satisfied.

So, given block is a CIDR block.

Now, size of block $= 2^4 \neq$ # IP addresses

To have 2^4 IP addresses, total 4 bits are required in the HID part.

No. of bits in the NID part = 32-4
= 28

CIDR representation –

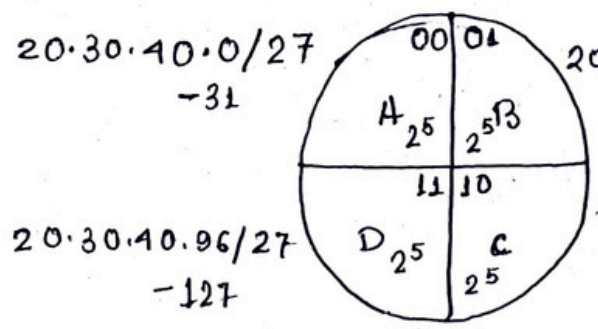
100.1.2.32/28.

* Subnetting in CIDR.

20.30.40.10/25

20.30.40.0 | 0001010

NID or BID | HID. → for 4 subnets



20.30.40.0/27 – 31

20.30.40.32/27 – 63

20.30.40.64/27 – 95

20.30.40.96/27 – 127

25+2 = 27 bits for NID in the subnets

(32-27) = 5 bits for HID. ⇒ # hosts = $2^5 - 2$ configurable

IP addresses = 2^5

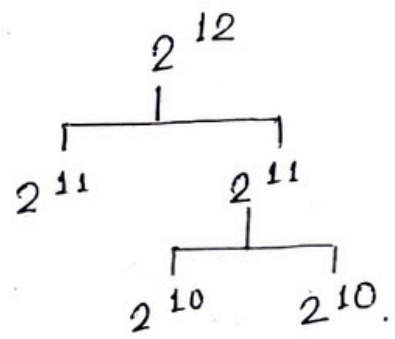
* VLSM & CIDR.

Variable Length SM

40.30.10.10/20

NID 20 bits

HID 12 bits.



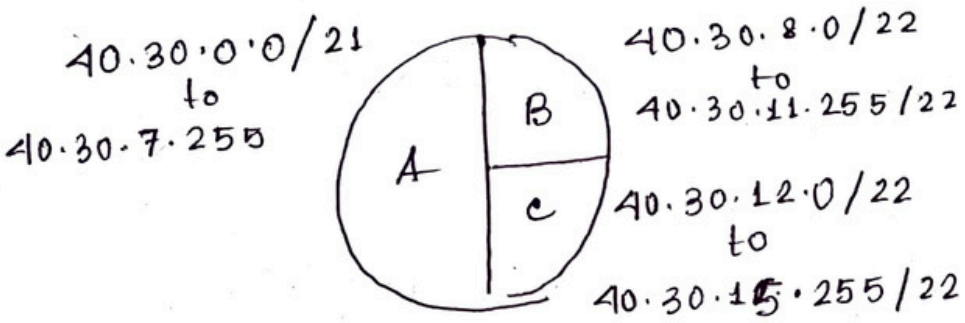
40.30.10.10.

⇓

$2^3 2^2$

40.30.0000 | 1010.00001010

BID HID.



1st subnetting:

A 40.30.0000 | 0 | 000.0000 0000 = 40.30.0.0/21

21 bits

40.30.0000 | 1 | 000.0000 0000 = 40.30.8.0/21

2nd subnetting (on 40.30.8.0/21):

B 40.30.0000 | 10 | 00.00000000 = 40.30.8.0/22

22 bits

C. 40.30.0000 | 11 | 00.00000000 = 40.30.12.0/22.

A range –

40.30.00000 | 111.11111111 = 40.30.7.255/~~22~~ 21

last IP.

B range –

40.30.0000 10 | 11.11111111 = 40.30.11.255/22

last IP

C range –

40.30.000011 | 11.11111111 = 40.30.15.255/22

last IP.

NB

1. Subnet mask 255.255.255.255

An address with subnet mask 255.255.255.255 means that the NID and IP address are same. [As SM AND IP = NID]. So, every device connected to the device will also get NID as its own IP address. If A wants to send packet to B, then it will send it to the gateway first & afterwards to B. [End to end connection].

It's not a network, but a standalone host. So, this N/W with SM as 255.255.255.255 puts each device inside its own subnet, forcing them to communicate with the router before communicating with any other device.

A

I_A 10.12.0.1

SM_A 255.255.255.255

AND 10.12.0.1 NID_{AA}

B

I_B 23.12.1.0

SM_A 255.255.255.255

23.12.1.0 NID_{BA}

Different

⇒ A sends packet via router to the host B

2. Given DBA, # subnets possible

For a DBA, host bits part is all 1's.

DBA is represented as valid N/W id + all hosts bits as 1's.

eg. 201.15.16.31 DBA

201.15.0001 0000.000|11111

5 bits → HID

000|1 1111
000 1|1 111
000 1 1|1 1
000 1 1 1|1

If it is a DBA, then at most last 5 bits can be host bits.

Possabilities.:

	N/W / Subnet ID	N/W / Subnet Mask	Hosts configured.
1.	201.15.16.0 (000 | 00000)	255.255.255.224 (NID part 27, HID part 5)	$2^5 - 2 = 30$
2.	201.15.16.16 (0001 | 0000)	255.255.255.240 (NID 28 | HID 4)	$2^4 - 2 = 14$
3.	201.15.16.24 (00011 | 000)	255.255.255.248 (NID 29 | HID 3)	$2^3 - 2 = 6$
4.	201.15.16.28 (000111 | 00)	255.255.255.252 (NID 30 | HID 2)	$2^2 - 2 = 2$
5.	201.15.16.30 (0001111 | 0)	255.255.255.254 (NID 31 | HID 1)	$2^1 - 2 = 0$

* Supernetting

Opposite of subnetting. In supernetting, multiple networks are combined into a bigger network termed as a supernetwork or supernet.

Supernetting is mainly used in Route Summarization, where routes to multiple networks with similar network prefixes are combined into a single routing entry, with the routing entry pointing to a super network, encompassing all the networks. This in turn significantly reduces the size of routing tables & also the size of routing updates exchanged by routing protocols.

So, supernetting is used in route aggregation to reduce the size of routing tables and routing table updates.

→ While performing supernetting on networks, we have to keep on mind –

1. All the IP addresses should be contiguous.
2. Size of all the small networks should be equal & must be in form of 2^n.
3. First IP address should be exactly divisible by whole size of supernet.

Eg 4 small networks of class C: /24

200.1.0.0
200.1.1.0
200.1.2.0
200.1.3.0

Build a bigger network that have a single network ID.

Before supernetting, routing table

NID	Subnet mask	Interface.
200.1.0.0	255.255.255.0	A
200.1.1.0	255.255.255.0	B
200.1.2.0	255.255.255.0	C
200.1.3.0	255.255.255.0	D.

Condition checking:

1. Contiguous: Range of 1st Network is from 200.1.0.0 to 200.1.0.255. If we add 1 in last IP address of first N/W that is 200.1.0.255 + 0.0.0.1, we get the next N/W ID that is 200.1.1.0.

All N/Ws are contagious having size 256 hosts.

2. Equal size of all N/W: As all N/Ws are of class C, so all of them have a size of 256 which in turn equals to 2^8.

3. First IP address exactly divisible by total size:

First IP address 200.1.0.0.

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

10 bits 0 ⇒ / by 2^{10}

200.1. 0000 0000 . 0000 0000

First IP address is divisible by total supernet size.

- add $\log_2 4$ bits to HID part.

So, we can join all of them and make a supernet.

NID	HID
22	10

New supernet ID 200.1.0.0 / 22.

- Finding supernet ID using supernet mask:

4 networks' IP addresses

- Changing / variable part 0's
- Constant part 1's

← constant	variable →
200.1 . 0000 0000 .	0000 0000
200.1 . 0000 0001 .	0000 0000
200.1 . 0000 0010 .	0000 0000
200.1 . 0000 0011 .	0000 0000

Supernet mask 255. 255. 252 . 0

Supernet ID = (Any IP address among the 4) AND (Supernet mask)

= 200.1.0.0

→ Advantages of supernetting :

1. Control & reduce N/W traffic.

2. Helpful to solve the problem of lacking IP addresses.

3. Minimises the routing table

→ Disadvantages of supernetting :

1. It cannot cover different area of N/W when combined.

2. All the N/Ws should be in same class & all IP should be contiguous.

Eg. 100.1.2.0/25 (1)

100.1.2.128/26 (2)

100.1.2.192/26 (3)

We can apply supernetting on (2) and (3) first that yields supernet 100.1.2.128/25

Now 100.1.2.128/25 and 100.1.2.0/25 are supernetted.

We get supernet 100.1.2.0/24.

* If we do supernetting on 2^n subnets, the Supernet ID part decreases by n bits.

Supernetting four /24 subnets

⇓

Supernet is /22 (24 - 2)

* Private IP addresses.

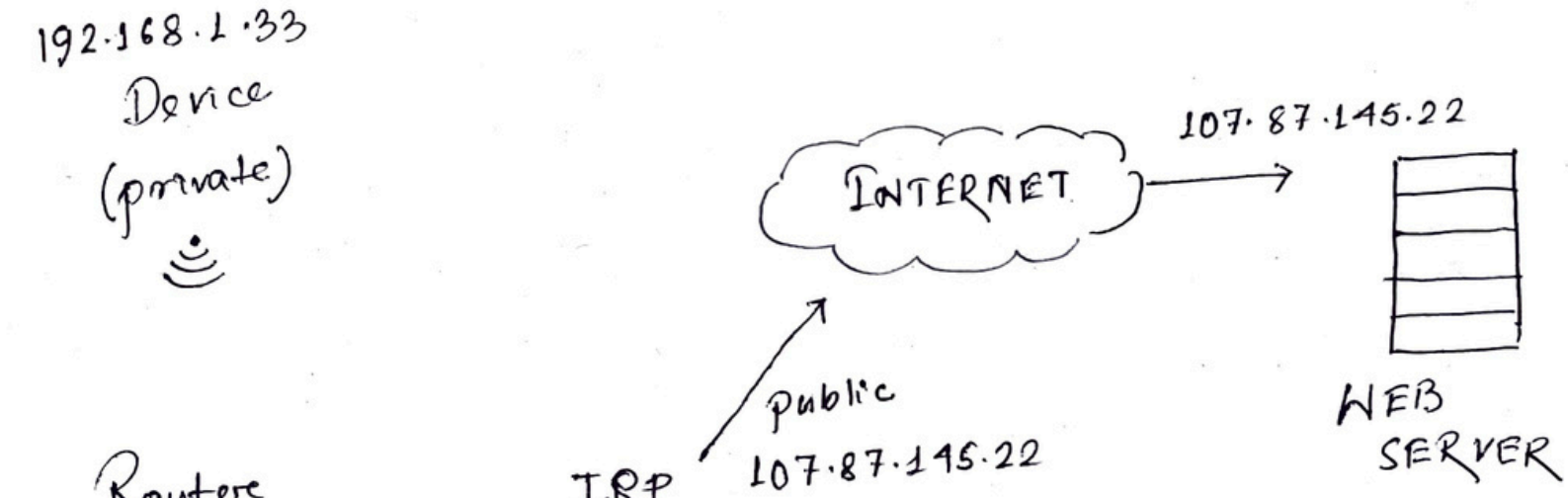
IANA - Internet Assigned Numbers Authority

- 192.168.0.0 – 192.168.255.255 (class C 256×2^8, 65536 IP addresses)
- 172.16.0.0 - 172.31.255.255 (Class B, $16 \times 2^{16} = 1,048,576$)
- 10.0.0.0 – 10.255.255.255 (class A, 2^{24} (16,777,216))

IANA reserves these IP address blocks for use as private IP addresses.

→ Another range of private IP addresses is 169.254.0.0 to 169.254.255.255, but those addresses are for automatic private IP addressing (APIPA) use only.

→ Instead of having devices inside a home or business network each use a public IP address, of which there's a limited supply, private IP addresses provide an entirely separate set of addresses that allow access on a N/W but without taking up a public IP address space. All the devices that are contained within private networks around the world can use a private IP address with virtually no limitation, which can't be said for public IP addresses.



Q. G'12 An ISP has the following chunk of CIDR-based IP addresses available with it: 245.248.128.0 /20. The ISP wants to give half of this chunk of addresses to organisation A, and a quarter to organisation B, while retaining the remaining with itself. Which of the following is a valid allocation of addresses to A and B.

a) 245.248.136.0/21 & 245.248.128.0/22

b) 245.248.128.0/21 & 245.248.128.0/22

c) 245.248.132.0/22 & 245.248.132.0/21

d) 245.248.136.0/24 & 245.248.132.0/21

→ 245.248.128.0

⇓

245.248.1000|0000.0000 0000

Different subnet splittings

245.248.1000 [1] [000.0]

↓

245.248.136.0/21

or

245.248.1000 [0] [000.0]

↓

245.248.128.0/21

245.248.1000 [00] [00.0]

245.248.128.0/22

245.248.1000 [01] [00.0]

245.248.132.0/22

245.248.1000 [10] [00.0]

245.248.136.0/22

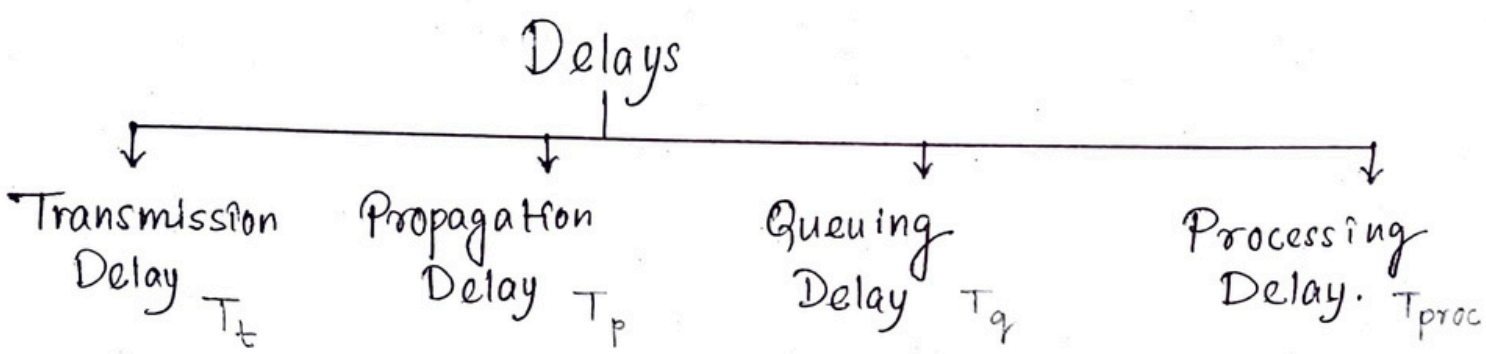
245.248.1000 [11] [00.0]

245.248.140.0/22

Flow Control Methods.

* Delays in CN.

Consider two hosts A and B are connected over a transmission link / transmission media. A data packet is sent by the host A to host B.



1. Transmission Delay. T_t

Time taken to put the data packet on the transmission link.

$$T_t \propto \text{Length or Size of data packet}$$

$$T_t \propto \frac{1}{\text{Bandwidth}}$$

BW → transmission rate

or

$$T_t = \frac{\text{Length / Size of data packet}}{\text{Bandwidth of N/W}}$$

$$T_t = \frac{L}{B}$$

2. Propagation Delay T_p

Time taken for one bit to travel from sender to receiver end of the link.

$$T_p \propto \text{Distance between sender \& receiver}$$

$$T_p \propto \frac{1}{\text{transmission speed}}$$

$$T_p = \frac{\text{Distance b/w sender \& receiver}}{\text{Transmission speed.}}$$

$$T_p = \frac{d}{v}$$

3. Queuing delay T_q

Time spent by the data packet waiting in the queue before it is taken for exec^n.

It depends on the congestion in the N/W.

4. Processing delay T_{proc}

Time taken by the processor to process the data packet.

It depends on the speed of the processor. Processing of the data packet helps in detecting bit level errors that occur during transmissi

NB.

1. Total delay in sending one data packet

or

✓ End to End time =

$$T_t + T_p + T_q + T_{proc}$$

2. In optical fibre, transmission speed of data packet = 2.1×10^8 m/sec.

(70% of speed of light)

3. Both queuing delay & processing delay are dependent on the state of the system.

This is because -

- If dest^n host is busy doing some heavy processing, then these delays increase.
- If dest^n host is free, then data packets will be processed immediately & these delays will decrease.

4. For any particular transmission link, bandwidth and transmission speed are always constant. This is because they are properties of the transmission medium.

*5. Bandwidth is always expressed in powers of 10 and data is always expressed in powers of 2.

1 kilo bytes = 2^{10} bytes

1 kilo bytes per second = 10^3 bytes per second

* Q. G'15. Since it is a N/W that uses switch, every packet goes through two links, one from source to switch and other from switch to destination. Since there are 10000 bits and packet size is 5000, two packets are sent. Transmission time for each packet is $5000/10^7$ sec. Each link has a propagation delay of 20 μs. The switch begins forwarding a packet 35 μs after it receives the same. If 10000 bits of data are to be transmitted between the 2 hosts using a packet size of 5000 bits, the time elapsed between transmission of 1st bit of data and the reception of last bit of data in microseconds is —

Sender host transmits first packet to switch, the transmission time is $5000/10^7$ that is 500 μs. After 500 μs, the 2nd packet is