20/9/19

⇒ Aloha access control.

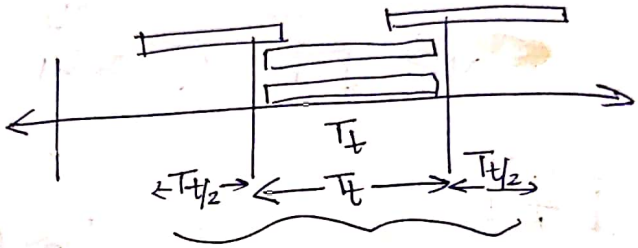
i) no channel sensing (any system can send data at any time)

ii) collision will occur in this, supports acknowledgement

iii) random backoff time on retransmission.

Aloha — pure aloha
       — slotted aloha.

* vulnerable time



$\eta = G.e^{-2G}$

G = no. of host wanted to transmit data for a time period T_t

$\frac{d\eta}{dG} = 0$, on solving, we get $G = \frac{1}{2}$

$\eta = \frac{1}{2} . e^{-1}$

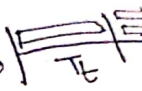
$\eta = 0.184$ i.e. 18.4%.

So, this is not an efficient way.

eg. Lets say that the communication media is using pure aloha access control with a BW of 4Mbps, then what is the effective BW.

Ans = 18.4% × 4 Mbps

→ Slotted Al.

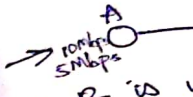


vulner

$\eta_{max} = e^{-}$

$\eta_{max} =$

* Differen



if B is
the
sends a
reduce

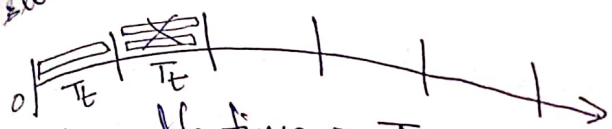
η

Go ba
selec

sta

10/10/19

→ Slotted Aloha.



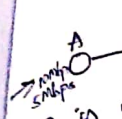
vulnerable time = T_t

$\eta_{max} = e^{-1}$

$\eta_{max} = \frac{0.368}{i.e.\ 36.8\%}$

* Difference between access control and flow control.

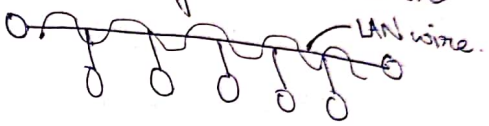
Flow control



If B is not able to cope with the speed of A, then it sends a message to A to reduce speed

Access control

for controlling shared media



$\eta = \frac{1}{1+a}$

Go back selective repeat $= \eta = \frac{N}{1+a}$

stop and repeat $= \eta = \frac{1}{1+2a}$

01/01/19

⟹ Networking layer

- logical addressing
- routing
- checksum (error detection)

* DHCP server. — dynamic / static.

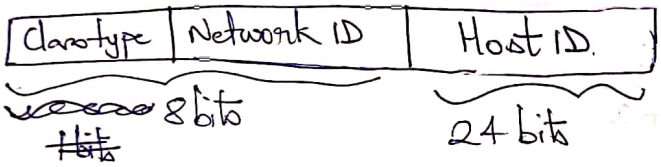
→ logical addressing

classful addressing → IPV4 → 32 bit address

	Decimal notation	Binary notation
class A	10.1.2.3	starts with 0
class B	129.1.2.3	starts with 10
class C	194.1.2.3	starts with 110
class D	230.1.2.3	starts with 1110
class E	242.1.2.3	starts with 1111

* Ranges
class A → 0–127
class B → 128–191
class C → 192–223
class D → 224–239
class E → 240–255

IP address – 32 bit



class A → 1, 7, 24 2^{24} → host
class B → 2, 14, 16 2^{16} → host
class C → 3, 21, 8 2^{8} → host
class D → reserved for multicasting
class E → reserved for future use.

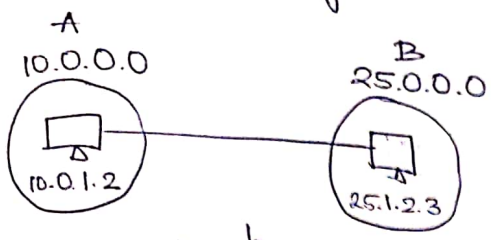
eg: When asked for no. of hosts

class A → $2^{24} - 2$
(1 for broadcast, 1 for network id.)

class B → $2^{16} - 2$
class C → $2^{8} - 2$

→ Casting
uni
bro
A
10.0.0.0
10.0.1.2
data
→ Broad
Limited
the broa
Directed
(Networ
eg. IP
10.1.
230.0
230.
192.
138.
129.
195
11
2
1.

→ Casting
- unicasting
- broadcasting.



unicasting

data	source IP	destination IP

→ Broadcasting — limited broadcasting
\ directed broadcasting.

Limited broadcasting. (for sending to same network).
The broadcasting IP address is 255.255.255.255

Directed broadcast

(Network ID). 255.255.255 → IP add. for directed broadcast
↓ for class A

eg. IP	Class type	LBC	DBC	No. of host	no. of networks
10.1.2.3 230.0.0.0	A	255.255.255.255		$2^{24}-2$	2^7
230.1.10.5 192.0.0.0	D	255.255.255.255			
138.1.2.10 129.0.0.0	B	255.255.255.255		$2^{16}-2$	2^{14}
195.1.20.10 11.0.0.0	C	255.255.255.255		2^8-2	2^{21}
241.1.2.3 130.0.0.0	E	255.255.255.255			

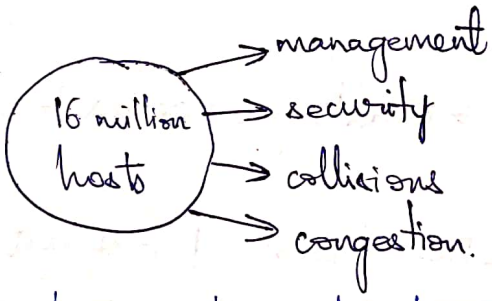
eg: IP	classtype
01011001.2.3.10	A
10111001.4.5.12	B
11011011.6.7.8	C
11101111.7.8.9	D
11111001.9.10.11	E

14/10/19

→ Classful addressing
- subnet → segmentation of the network
- subnet mask
- routing.

→ Class A

2^{24} — 16 million.



→ Disadvantage of big network.

→ Subnetting – IP addresses

VLAN → IP addressing and physical addressing.

VLAN is restricted to some of the switches only, not all routers/switches can provide VLAN capability).

(managable switches).

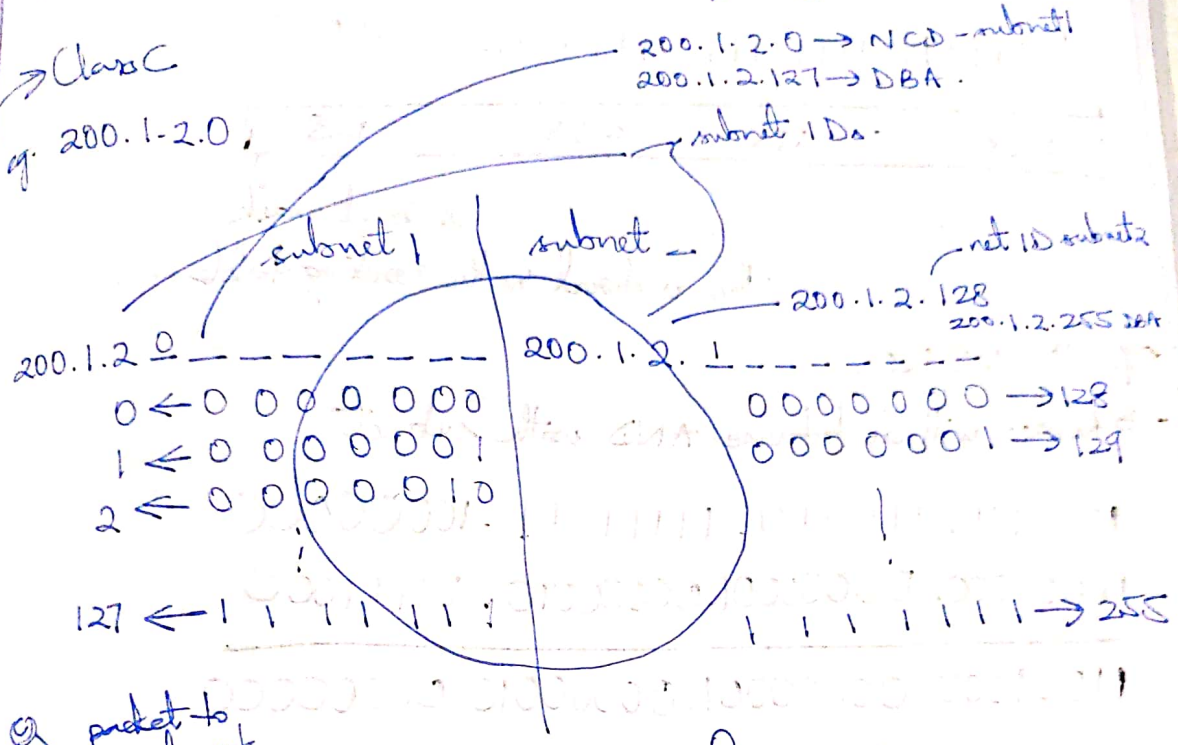
→ In each IP address, assign subnet ID.

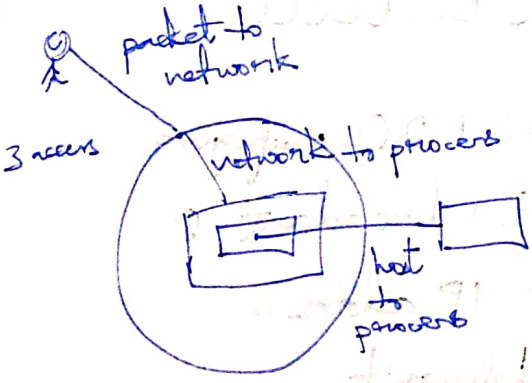
Division of four types

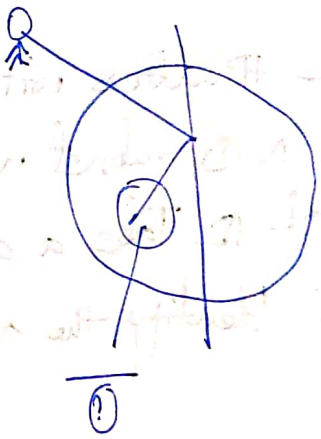
class type	NET ID	sub net ID	Host ID	

→ Class C

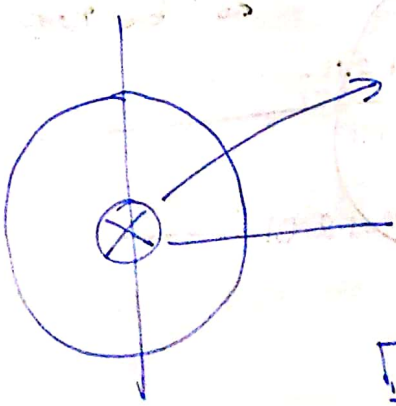
eg. 200.1.2.0,







(1)



NID.	SID	Interface
200.1.2.0		
200.1.2.128		

Data	SCIP	DSIP	Control block

32 bit size subnet mask

1's → NETID & subnet mask

0's → host

11111111.11111111.11111111.10000000

255	255	255	128

subnet mask

this is stored in the routing table.

eg. 200.1.2.120

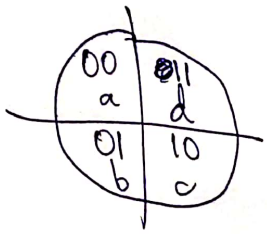
→ Router will do bitwise AND with subnet

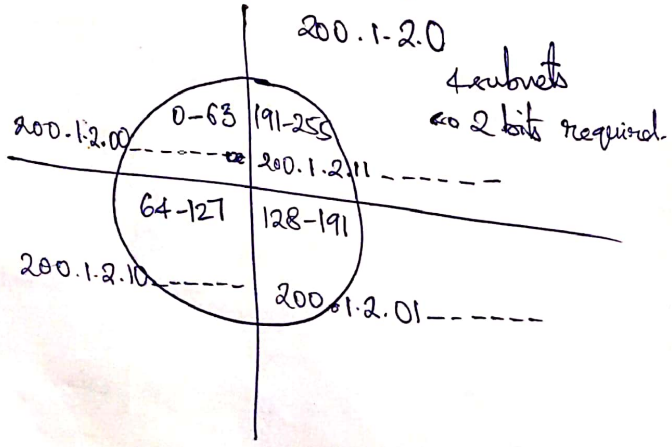
11111111.11111111.11111111.10000000

11001000.00000001.00000010.01111000

11001000.00000001.00000010.00000000

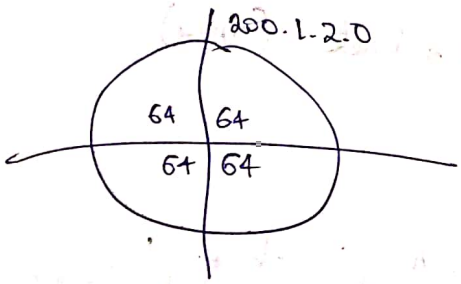
eg. Class C IP address with NID 200.1.2.0, configure 4 subnets, NID, subnet mask, bits for broadcast ID and network ID. Take a destination IP address 200.1.2.63. Identify the subnet it belongs to.





5/10/19.

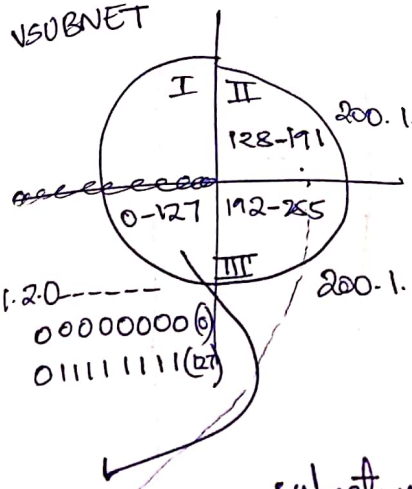
Variable length subnet



what if we want only 3 subnets

→ it reduces the no. of IP addresses wasted

→ 128 64 64



10000000 (128)
10111111 (191)

1100 0000 (192)
11111111 (255)

subnet mask: 32 bit: 1's → net ID + sid
0's → host id

SM: 255.255.255.128

For II : 255.255.255.192

III : 255.255.255.192

routing table

Net ID	Subnet mask	Interface
200.1.20	255.255.255.128	a I
200.1.2.128	255.255.255.192	b II
200.1.2.192	255.255.255.192	c III

If subnet mask is 255.255.255.192, what all info can we gather

NETID + SID = 26

for class A, 8 + SID = 26 SID = 18 → 2^{18} subnets

if class B:

NETID + SID = 26

16 + SID = 26 $\rightarrow$ SID = 2^{10} subnets (1024)

class C:

SID = 2^2 subnet = 4 subnets

eg:

subnet mask	no. of host	class A no. of subnet	class B no. of subnet	class C no. of subnet
255.0.0.0	$2^{24}-2$	0	–	–
255.254.0.0	$2^{17}-2$	2^7	–	–
255.192.0.0	$2^{22}-2$	2^2	–	–
255.255.255.254	2-2			–
255.255.255.0	2^8-2			
255.255.252.0	2^9-2			

22/10/19

$\Rightarrow$ Who is handling IP addressing?

IANA — Internet Assign Network Authority.

↳ assigns ~~IP4~~ IPV4 and IPV6.

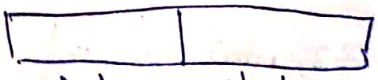
$\rightarrow$ 1983 $\rightarrow$ IPV4 $\rightarrow$ 1999 $\rightarrow$ IPV6

$\rightarrow$ classless IP vs class IP

↳ waste of IP if not properly used.

CIDR: Classless Inter Domain Routing

No classes will be represented with block ID, host ID.



↳ no. of blocks ↳ within each block how many hosts

- So we avoid wastage of IP addresses.

disadvantages:

eg: 200.1.2.100 /25 — block no.

32 bit: 32-25 = 7 $2^7 = ?$

→ Rules to represent CIDR, IP address.

i) All IP address belongs to block should be continuous.

ii) The block size should be power of 2 (2^n)

iii) The 1st IP address of a block should be evenly divisible block size 2^n

eg: 10.20.30.32
10.20.30.33
⋮
39

$39 - 32 + 1 = 8$

$2^n = 8;\ n = 3$

rule 1 ✓ rule 2 ✓

10.20.30.00100|000
2^{5-n}

eg: 20.30.40.32
⋮
20.30.40.63

$63 - 32 + 1 = 32$

$2^n = 32 \Rightarrow n = 5$

rule 2: should be power of 2.

rule 3: ? 20.30.40.001|00000
2^5

eg: 200.30.40.60 /25

32-25=7

IP address | block ID | host ID

HID

200.30.40.0 0000000
block ID
⋮
1111111

eg 100.1.2.3/23

32-23=9

2^9 host

100.1.0000001 | 0.00000000 HID
BID
1.11111111

eg. 20.30.40.32/27 (HW)

20.30.40.0000 0000
BID ↓ host ID.
subnet ID

1111

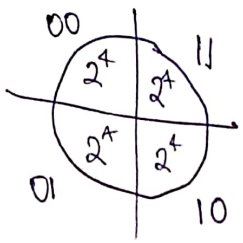
20.30.40.000 0000
BID

eg. 20.30.40.128/27

20.30.40.000 10000

20.30.(11)00000 → 128+64+32

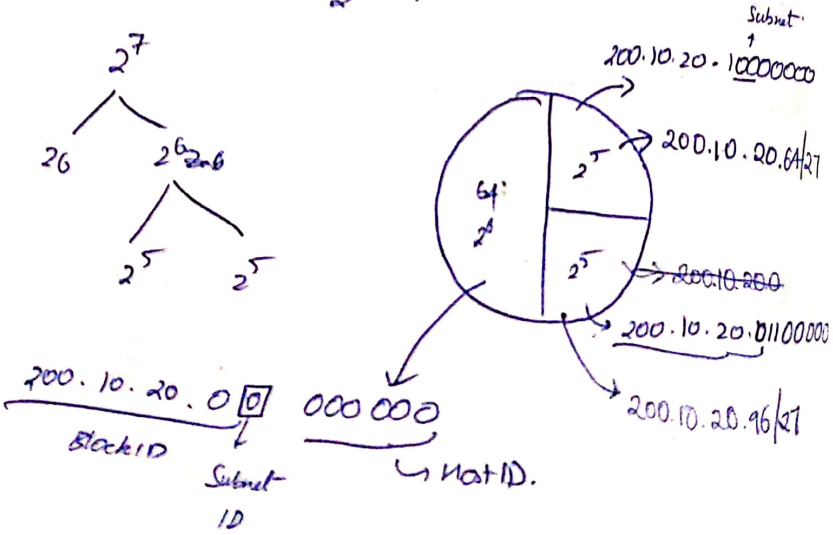
eg. 1.2.3.4/26 4 subnet

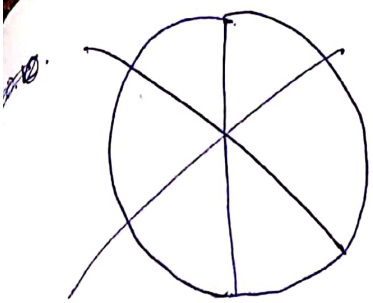


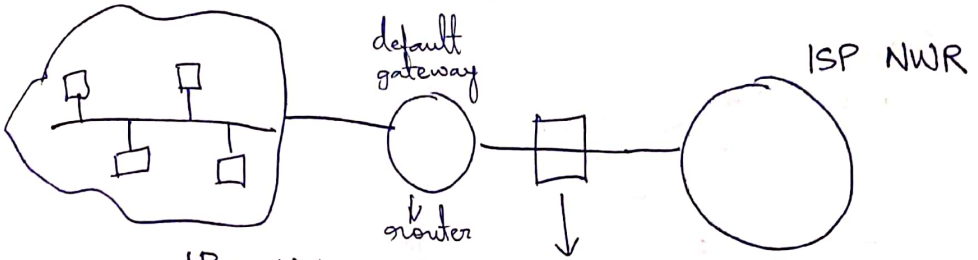
CIDR Variable length Subnetting.

Q): 200.10.20.35 /27

32 - 27 = 7







IP config
IPV4
DNS
Default gateway.

NAT:
Network Address translator

* What is default gateway?

IP_A : 200.10.20.40

$subnet_A$: 255.255.255.128
200. 10. 20. [illegible] → subnet ID

IP_B : 200.10.20.130

$subnet_B$: 255.255.255.192

IP_B : 200.10.20.64
subnet A : 255.255.255.128
200.10.20.0 → subnet ID.

given subnet: 255.255.255.192
8. 8. 8. 2 → /26 32-26=6 2^6 hosts

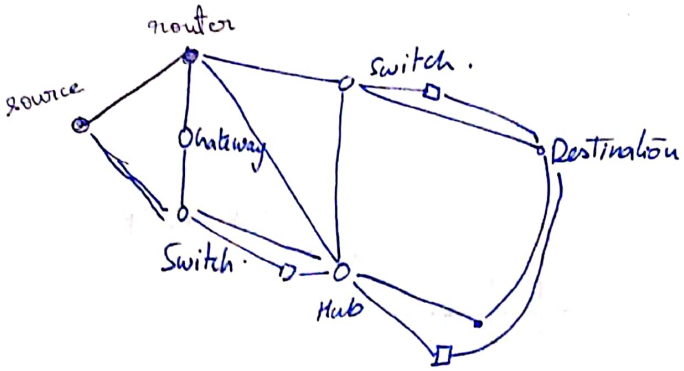
255.255.0.0
8.8.0.0 ⇒16 32-16=16 2^{16} hosts

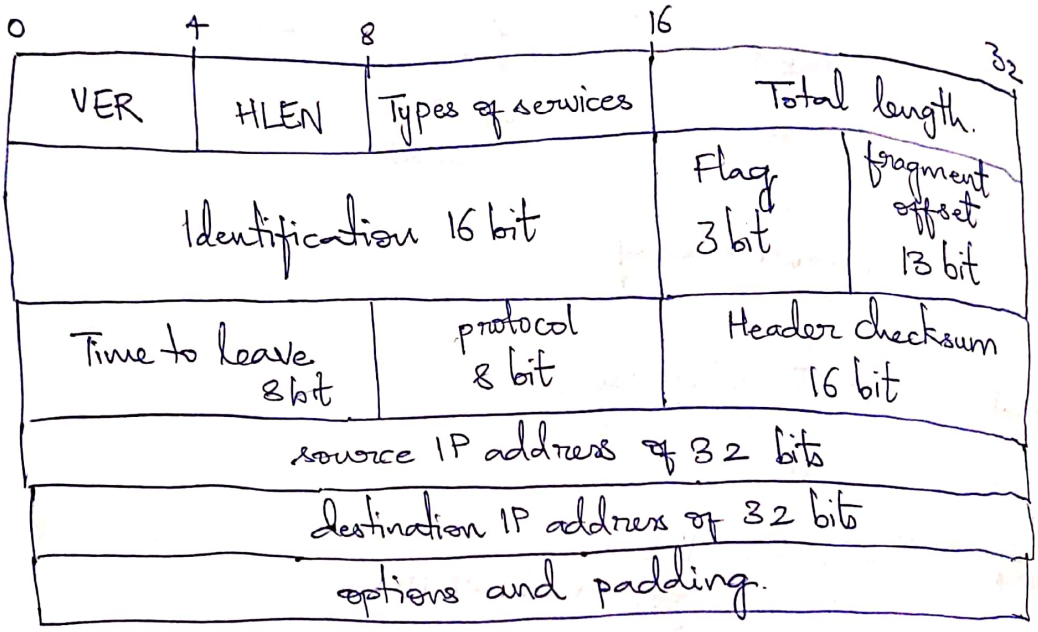
Given subnet mask, configure 4 subnets, how?
↳ 255.255.255.192

8.8.8.2.6 — host ID
[illegible] subnet ID

⇒ IPV4 Packet formula

- Connection less
- Datagram approach.





Header → 20 byte → 60 byte.

\+

payload → 0 byte → 65515 byte.

500 byte

20 byte → header

480 byte → payload.

→ Types of services

8 bit

P	P	P	D	T	R	C	0

P P P → priority

D → delay

T → throughput

R → reliability

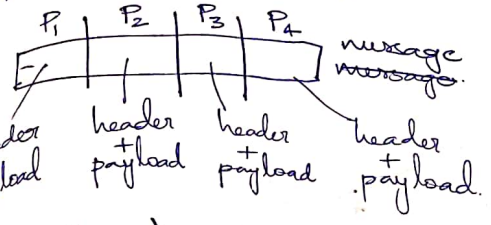
C → cost

0 → reserved for future use.

→ total length (16 bit)

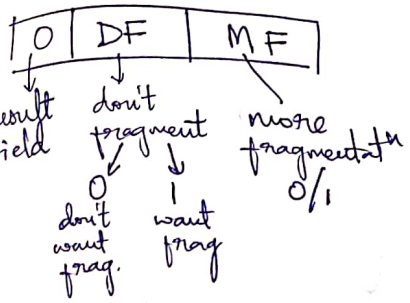
500 byte
- 20 byte
480 byte.

→ Identification (16 bit)



each packet has a unique id.
max $2^{16} = 65535$ ~~addresses~~ can be assigned.

→ Flag (3 bit)



→ Fragment offset (13 bit)

checks how many datapackets a there ahead of me. (or payload)

→ Time to leave (8 bit)

$2^8 \rightarrow 256$ are the max no. of hops from the source to destination. i.e. max 256 intermediate device can visualize your packet

→ Protocol (8 bit).

→ Header checksum (16 bit)

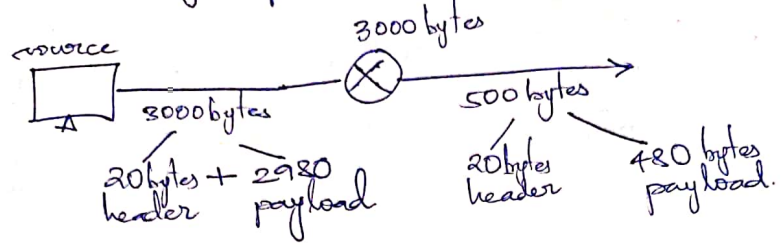
we do error detection and notify ~~the~~ if some packet is lost.

→ Options & padding

provides additional utilities

eg. counting intermediate devices visited, delay, ~~etc~~, i.e. accounting info, etc.

eg. A datagram of 3000 bytes (20 byte of IP header + 2980 bytes of payload) reaches at the router and router forwards the packet of max. 500 bytes (i.e. MTU). Calculate how many fragments will be generated and also write MF, offset and the total length of the packet.



$$\left\lceil \frac{2980}{480} \right\rceil = \lceil 6.27 \rceil = 7$$

P_7	P_6	P_5	P_4	P_3	P_2	P_1
↓	↓	↓	↓	↓	↓	↓
20	20	20	20	20	20	20 header
+	+	+	+	+	+	+
100	480	480	480	480	480	480 payload
	↓	↓	↓	↓	↓	↓
	500	500	500	500	500	500

$2980 - 480 \times 6 = 100$ → 7 fragments

↓

120

0 1 1 1 1 1 1 → MF

P_2 behind P_1

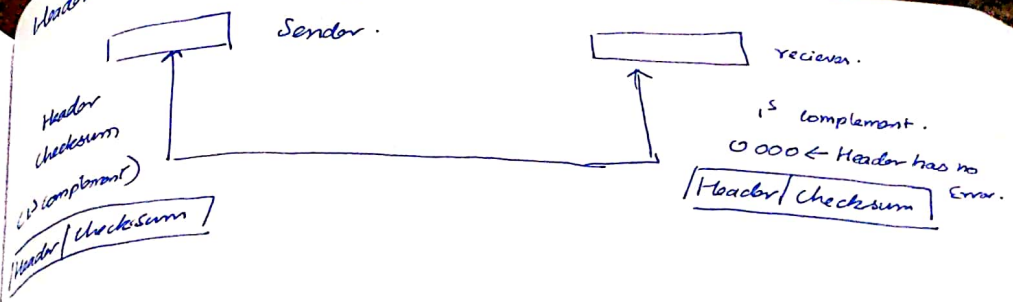
360 300 240 180 120 60 0 → offset $\left(\frac{\text{payload}}{8}\right)$

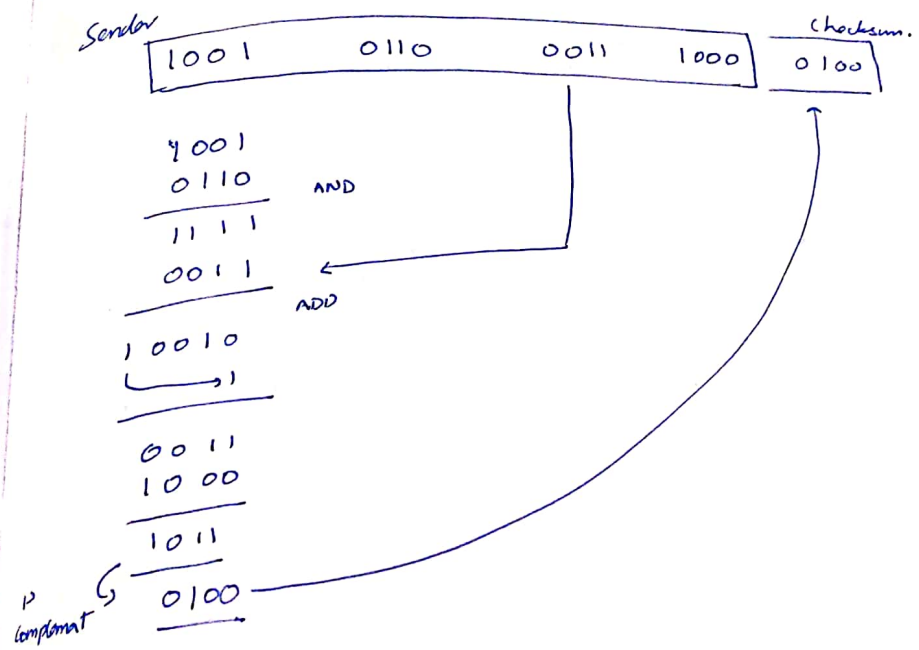
$\frac{480+480+480+480}{8}$ $\frac{480+480}{8}$ $\frac{480}{8}$ as there is no one ahead of this

$\frac{480+480+480}{8}$

$360 \times 8 = 2880$, 100 bytes left

Header Checksum (Layer 3).





Reciever:

```
 1 0 0 1
 0 1 1 0      (AND)
 1 1 1 1
 0 0 1 1
 1 0 0 1 0
     → 1
 0 0 1 1
 1 0 0 0
 1 0 1 1
 0 1 0 0
 1 1 1 1
 0 0 0 0  ← Header has no error.
```

⇒ IPV6 Header formulae

Baseheader = 40 byte → Fixed IPV6

connection less datagram

$2^{16} \rightarrow 65535$

VER 4 bit	Priority field 8 bit	Flow label 20 bits
Payload length 16 bit	Next header bit 8 bit	Hop count 8 bit
source address (128 bit)		
destination address (128 bit)		
Option and padding.		

Default ~~header~~ message

Baseholder	payload
40 byte	65535 byte

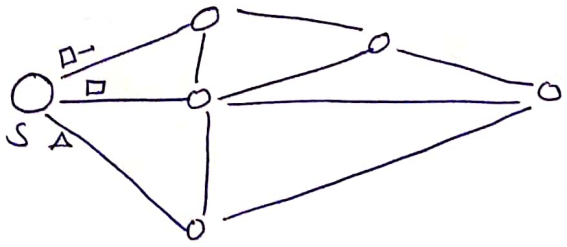
Extension header

1) Routing header (43)

Base header	Extension header	------	extension header	payload

2) Hop by hop (0)
3) Fragmentation header (44)
4) Authentication header (53)
5) Encapsulate security payload (50)

Flow Label: gets virtual circuit



only packet from Source.

Payload:

Routing header: The source decides how the ~~product~~ packet (route) will reach the destination

Hop by hop: for multiple hops.

Fragment head
destination.
Authentication
Encapsulate
Destination op
the
Hop count :

Source: gen
frequency
Packet swi
no con
Message
each me
tower.

⇒ Link

1) It divi

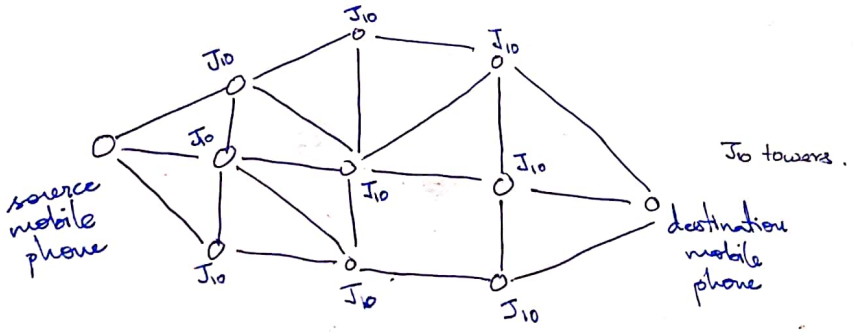
Fragment header: no fragmentation between the source and destination.

Authentication header:

Encapsulate security payload: to improve further security.

Destination option: only with destination host. no other hops can read the data. Only the header can be read.

Hop count. maximum hops = 255



Source: generate a number, & using the number will provide a frequency. Used in cellular phones.

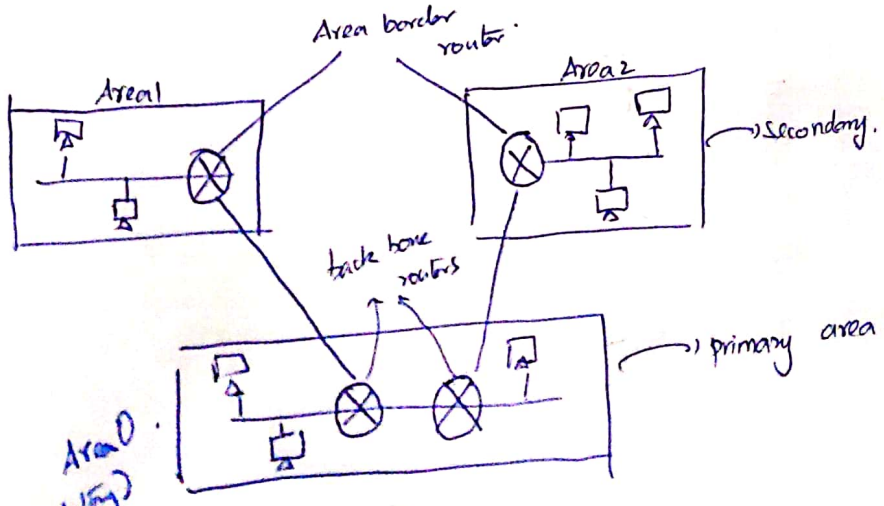
Packet switching: (datagram)
no connection between source and destination.

Message switching (similar to store & forward)
each message is stored and then sent to corresponding next tower.

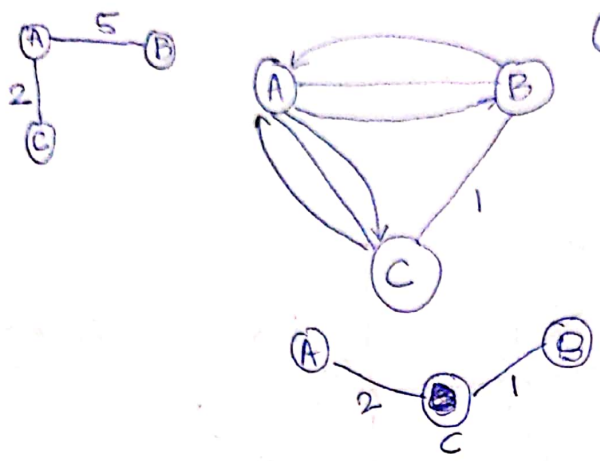
→ Missed a class here.

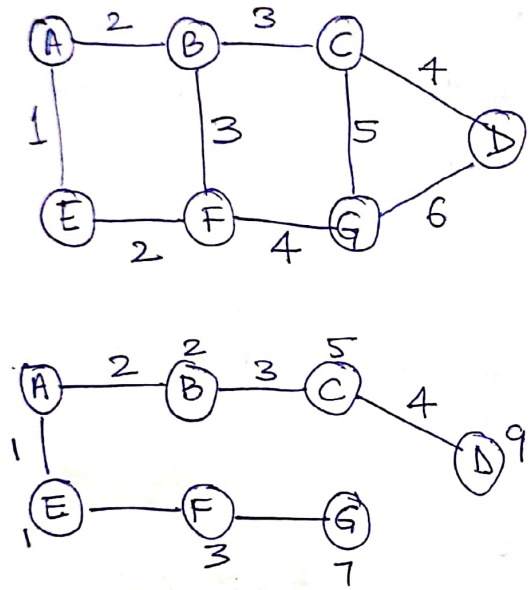
⇒ Link state protocol (OSPF) → Open shortest path first

1) It divides the whole autonomous system into different areas.



i) Creating a link state also called link state packets
ii) Disseminate the link state packets to all routers through flooding.
iii) Create a shortest path tree (Dijkstra algorithm).



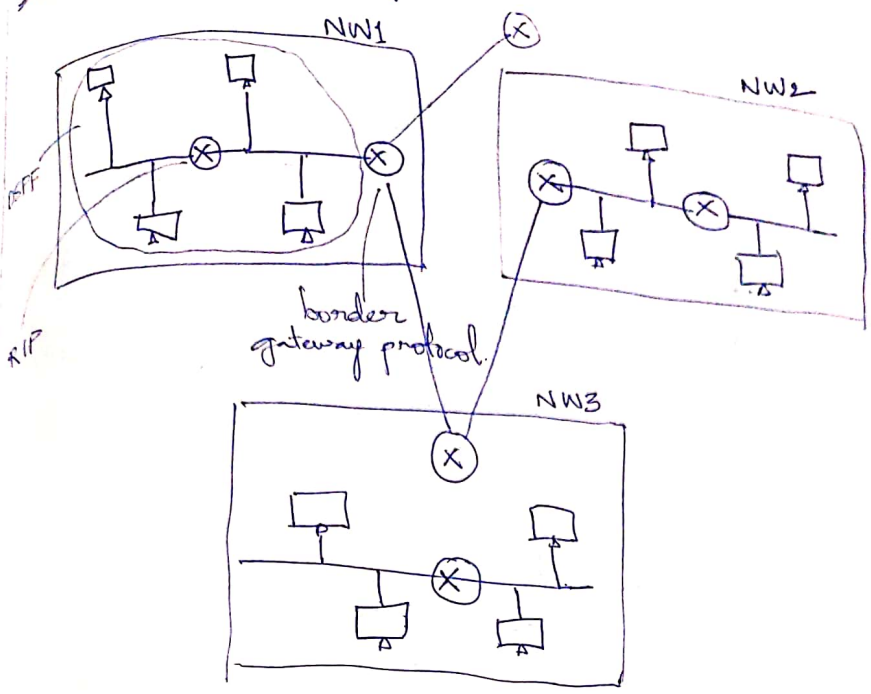


Destination	cost	next router
A	0	—
B	2	—
C	5	B
D	9	B, C
E	1	—
F	3	E
G	7	E, F

ackets

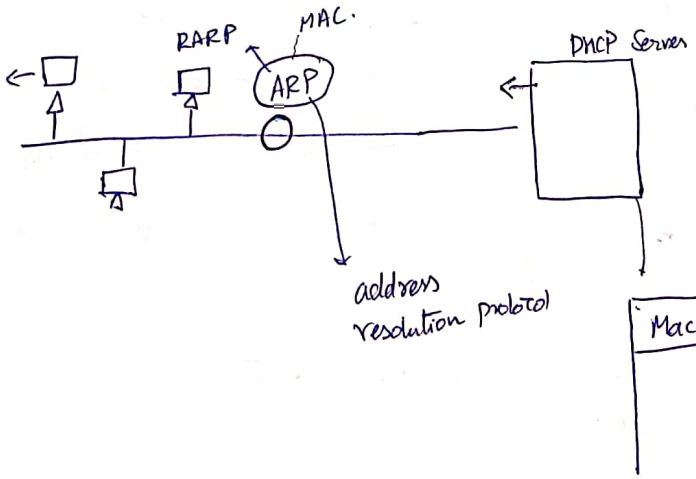
ers through

→ BGP (Border gateway protocol)



DHCP (Dynamic host configuration protocol)

192.168.82.255



RARP

: reverse address Resolution protocol.

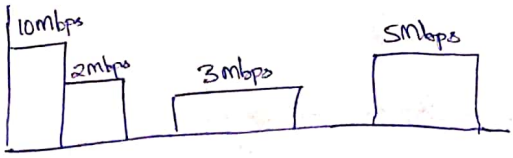
Free IPs are allocated.

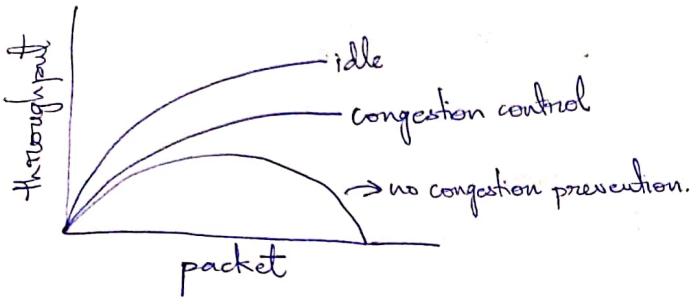
Mac	IP	Alloted

8/11/19.

Congestion control: It is a load beyond the capacity of link.

1) Switch/router
2) Bursty traffic





Congestion control

open loop
(prevention and avoid congestion)
- → Retransmission policy
- → Window policy
- → Admission policy
- → Discard policy.

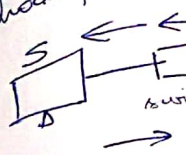
closed loop
(It allows congestion and then apply congestion avoidance techniques)
- → choke packet
- → back pressure
- → implicit signalling
- → explicit signalling.

→ Retransmission policy — Piggybacking.

→ Window policy: determines flow control. (best is selective repeat ARQ).

→ Admission policy: whether ~~we can~~ the router should allow the packet to flow in the network or not. identifying the network resource to admit the packet on the network.

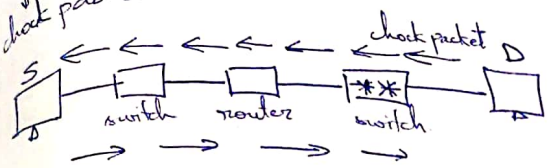
→ Discard policy

closed loop
choke packet

Back pressu

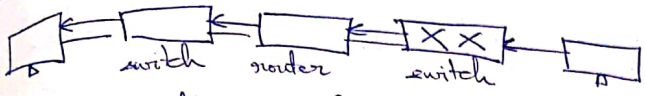
Implicit si
Assume th
retransmis
Explicit sig
→ QOS usi
1) Leaky bu
2) Token bu
eg. Lets
control
After th
6 Mbps
5 Mbps
→ Token

closed loop congestion

choke packet



Back pressure:



Implicit signalling/feedback:

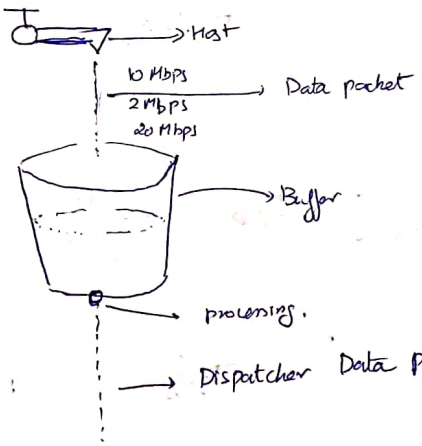
Assume there is a congestion based ack delay, packet delay, retransmission.

Explicit signalling:

→ QOS using traffic shaping (bursty traffic)

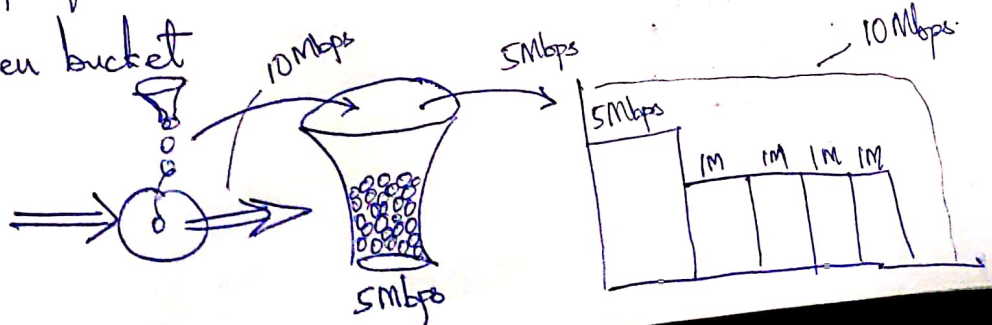
1) Leaky bucket algo

2) Token bucket algo



Eg: Lets say the router is using leaky bucket congestion control where host sends bursty traffic of 15 Mbps for 3 sec. After that host remains silent for 2 sec. Again host sends 6 Mbps for 2 sec and remains silent for 2 sec. Again host sends 5 Mbps for 3 sec. What is the output datarate of leaky bucket.

→ Token bucket



eg: A host machine uses token bucket algo. The token bucket capacity is 1 megabyte and max output rate is 20 MBps. Token arrives at a rate to sustain output at 10 Mbps. The token bucket is currently full & the machine needs to send 10MBps. What will be the min time req. to transmit data in sec.

14th Nov'19

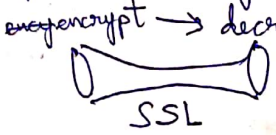
	Message type	Devices	Protocol
Application	Data/information	Gateway/firewall/ PC/mobile	→
presentation layer	Data/information	Firewall gateway	MIME (multipurpose mail extension), SSL
Session layer	Data/information	Gateway firewall	PAP, RPC
Transport layer	Segmentation	Gateway firewall	TCP, SCTP, UDP
Network layer	Packets	Router, B-Router, Layer 3 switch	ICMP, ARP, IGMP, RARP, IPV4, IPV6
Datalink layer	Frame (MAC / LLC)	Switches, bridges, 2layer	IEEE 802.3, CSMA (short range), IEEE 802.5, HDLC
Physical layer	Bits	Cables, fibre, hub, repeater	IEEE 802.11 (different cable formats)

TCP/IP application

2^{16} ports →

1–1024 well defined ports

* SSL – Secure socket layer : used for secured connection.
used for tunneling mechanism.



Tunneling – doesn't use any port

PAP: Password Authentication Protocol : for authentication
RPC: Remote procedure call. eg. for online compiler.
SCTP: Screaming control transfer protocol
Brouter – bridge router (?)
ICMP – internet
IGMP:

⇒ Application layer protocols.

Protocol name	port no.	Transfer protocol
~~NTP~~		~~UDP~~
1) Echo	7	TCP/UDP
2) FTP	20/21 data control	TCP
3) SSH (secure shell)	22	TCP
4) Telnet	23	TCP
5) SMTP (push the mail to server)	25	TCP
6) DNS	53	UDP
7) DHCP	67/68 data control	UDP
8) TFTP	69	UDP
9) HTTP	80	TCP
10) POP (pops the mail from server)	110	TCP
11) NTP	123	UDP
12) HTTPS	443	TCP
13) RIP	520	UDP