ID: 1800411120

CSE-4511 : Computer Networks

Mid Examination

Ans. to Q.no. 1(a)

For a pure Aloha, the throughput depends on vulnerability time.

Total = 2P

If we define P as the transmission time, then vulnerability time is 2P.

Now, in pure Aloha, the packet arrival rate is fixed but the packets can arrive randomly. This follows the Poisson probabilistic distribution.

180041120

We know, Poisson distribution for k packets will be

$$P_k(t) = \frac{(\lambda t)^k e^{-\lambda t}}{k!}$$

where, $k = 0, 1, 2 \ldots$

λ = arrival rate

Now, we define load of system as G which is the average no of attempts to send the packet.

The throughput is S,

$S = G \cdot P_s$ where P_s is probability of packet succeeding. ——— (i)

Now, $P_s = P\{\text{Packet 0 is successful}\}$

$= P\{0 \text{ packets in } 2P \text{ time (vulnerability time)}\}$

$= \frac{e^{-\lambda P}(\lambda P)^0}{0!} * \frac{e^{-\lambda P}(\lambda P)^0}{0!}$

$= e^{-\lambda P} \times e^{-\lambda P}$

$= e^{-2\lambda P}$

Now, $G = \lambda P$ which is according to Little's Formula.

$\therefore P_s = e^{-2G}$

Putting, the value of P_s in eq(i), we get,

$S = G \cdot e^{-2G}$ ——— (ii)

To find the maximum value of S or maximum throughput, we differentiate it with respect to t.

$$\frac{dS}{dt} = \frac{d}{dt}(G \cdot e^{-2G})$$

$$\Rightarrow 0 = \frac{d}{dt}(\lambda t \cdot e^{-2\lambda t})$$

$$\Rightarrow 0 = \lambda \cdot e^{-2\lambda t} + \lambda t \cdot (-2\lambda) \cdot e^{-2\lambda t}$$

$$\Rightarrow 0 = \lambda \cdot e^{-2G} + G \cdot (-2\lambda) \cdot e^{-2G}$$

$$\Rightarrow 0 = \lambda e^{-2G} (-2G + 1)$$

$$\Rightarrow -2G + 1 = 0$$

$$\therefore G = 1/2$$

Putting $G = 1/2$ in (ii), we get,

$$S_{max} = 1/2 \cdot e^{-2/2}$$

$$\therefore S_{max} = \frac{1}{2e} = .184$$

$$\therefore S_{max} = 18.4\ \%$$

So, maximum throughput of pure Aloha is 18.4 % (Ans).

Average transfer delay:

~~Avg. no. of unsuccessful transmission~~

Avg. no. of unsuccessful transmission per successful transmission is

$$N_r = \frac{G}{S} - 1 = \frac{G}{G \cdot e^{-2G}} - 1$$

$$= e^{2G} - 1$$

Now, transmission delay = unsuccessful delay + successful delay

$= N_r (P + B) + P$ where B is backoff time.

Now, B average backoff time,

$$\bar{B} = \frac{P \sum_{k=0}^{k-1} k}{k} = \frac{P(k-1)(k-1+1)}{2k}$$

$$\therefore \bar{B} = \frac{Pk(k-1)}{2k} = \frac{P(k-1)}{2} \qquad \left[\because S_n = \frac{n(n+1)}{2}\right]$$

So, average transmission delay, $\bar{T} = N_r \times (P + \bar{B}) + P$

$$= (e^{2G} - 1)\left[P + \frac{P(k-1)}{2}\right] + P$$

$$= P(e^{2G} - 1)\left(1 + \frac{k-1}{2}\right) + P$$

$$= P(e^{2G} - 1)\left(\frac{k+1}{2}\right) + P$$

$$= P\left\{(e^{2G} - 1)\left(\frac{k+1}{2}\right) + 1\right\}$$

$$\therefore \bar{T}/_p = (e^{2G} - 1)\left(\frac{k+1}{2}\right) + 1$$

This is the average transmission delay (Ans.) for pure Aloha.

Ans. to Q. no 1(b)

Average input rate, λ = 1 packet/sec. (150 stations)

packet length = 1000 bits

channel capacity = 1 Mbps

(i) In 1 second, 10^6 bits are sent

= 1000 packets are sent.

(ii) λ = @ 1000 packets / station

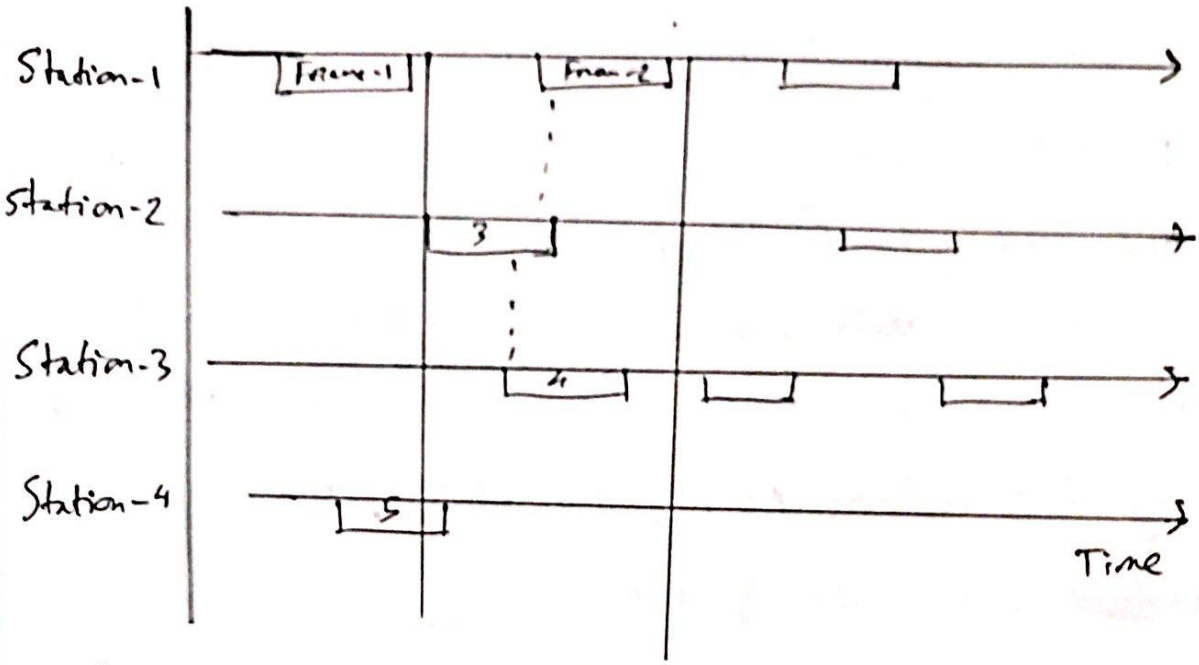
(iii) $N_r = e^{2G} - 1 =$

(iv) $\bar{T}/_p = \left(e^{2G} - 1\right)\left(\frac{k+1}{2}\right) + 1 =$

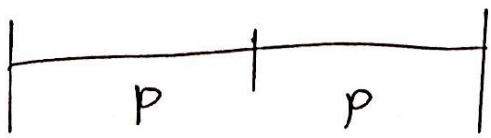
Ans. to Qno. 1(c)

Aloha:

In Aloha, we calculate the vulnerability time based on the the frame transmission time P.



As, we can see 4 stations are transmitting. Frame-3 is colliding with frame-2 and 4 because frames are sent randomly. When one station sents, it has the probability to collide with another frame. The frames won't collide if with in a certain time period frames aren't sent. That time period is ~~vulnerabili~~ vulnerability time. The vulnerability time for pure Aloha is.



$V = P + P = 2P$ where P is transmission time.

Collision won't occure if frames are not sent within this time interval.

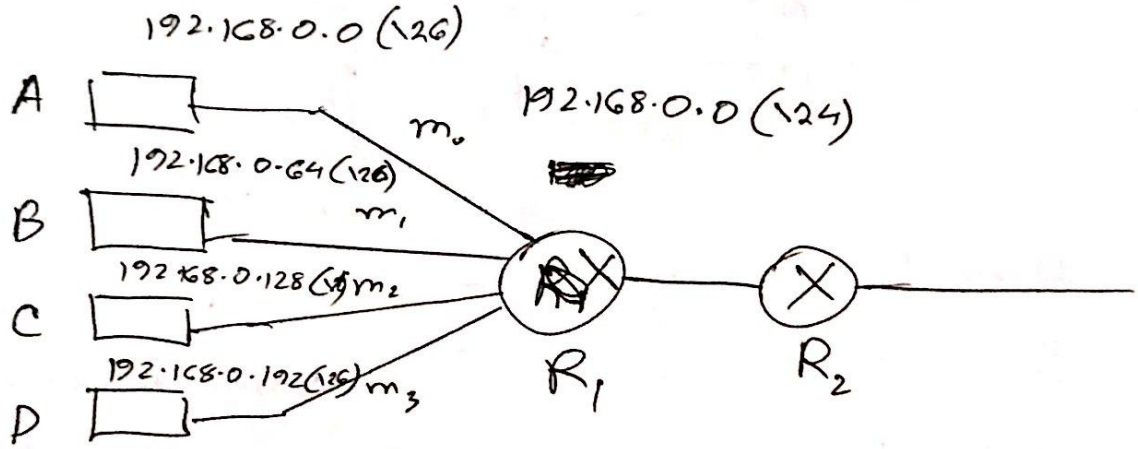
As we can see if the ~~propa~~ frame transmission time is higher, then more packets will be sent ~~the~~ in collision durcation and thus increasing the vulneranibility time.

② ~~For~~ CSMA/CD, the propagation delay ~~comes~~ influences ~~a~~ ~~very~~ vunnealibility time. Because CSMA/CD, the packet is send and the sender constanly recieves the sent bits. If the packet is ~~to~~ too small it will go fast in the ~~othe~~ medium and the packet can't be stored in senders buffers to check receiving bits. Thus, this is why the ~~reduced~~ propagation delay, influences the ~~vulene~~ vulneranibility time.

18004/120

Ans to Q.no. ~~2(5)~~ 3(a)

Address Aggregation: In a network, there can be a router with many subnets. The ~~hosts~~ networks under that IP address are not referenced individually by other devices. Instead, the IP address of the router is stored in order to reduce the size of the routing table. When the packet is forwarded to IP address of router, it can forward it to the hosts in its network. In this way, the router's address act as an aggregate address for all ~~hosts~~ networks underneath the router and the process is called address aggregation.

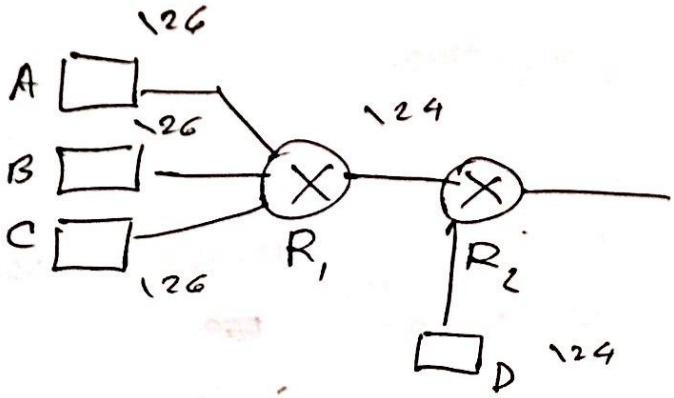


Here, when a frame needs to be sent to A from R_2, it is instead forwarded to R_1 as it has the aggregate address stored in the routing table of R_1. R_1 would then forward it to A using its own routing table.

Longest Prefix matching: During forwarding using address aggregation, there can be a problem where the host under the aggregate address is not found. This is called blackhole problem and occurs due to inappropriate aggregation. We solve using longest prefix matching where longest mask is at the top in routing table and it is sorted in descending order of masks.

Mask	IP Address	Interface
\26		
\24		

Longest at top ↑



Here, D falls under aggregate address of R_1. But it is located in R_2. So, blackhole problem occurs. To solve this we look for more specific address and start matching from longest prefix. Then R_2 will find D's \26 address first and forward to D instead of R_1.

Ans to Q.3(b)

172.16.88.255 /20

20 bits are used for networking.

For third octet it is $(11110000)_2 = 240$.

So, subnet address is 172.16.240.0 (Ans)

~~255.255.240.0~~

For broadcast address it will be $(11111111)_2 = 255$

So, broadcast address is

172.16.255.0 (Ans.)

For, 172.16.46.191 (/26)

10 ~~2~~ bits are used for subnetting it this class-B address.

Last 2 octets in binary is

00101110 . 10 | 111111

Network | Host

From host portion, we can say it is broadcast ~~address~~ packet. A router discards broadcast address to prevent broadcasting chaos. So, this packet will be discarded. (Ans.)

Ans to Q.no 3(a)

Class B: 180.18.0.0 in (/27)

(i) Here, 27 - 16 = 11 bits are used for subnetting.

So, there will be 2^{11} subnets.

(ii) 32 - 27 = 5 bits are used for hosts

So, there will be $2^5 - 2 = 32 - 2 = 30$ hosts/subnet.

(iii) Block size for third octet is 256 - Mask

= 256 - 255

= 1.

Block size for 4th octet is 256 - 224 = 32

(iv) Valid last 8 subnets are

180.18.255.254

180.18.255.253

180.18.255.252

180.18.255.251

180.18.255.250

180.18.255.249

180.18.255.248

180.18.255.247.

(v) Broadcast Address

180.18.255.255

255.223

255.191

255.159

255.127

255.95

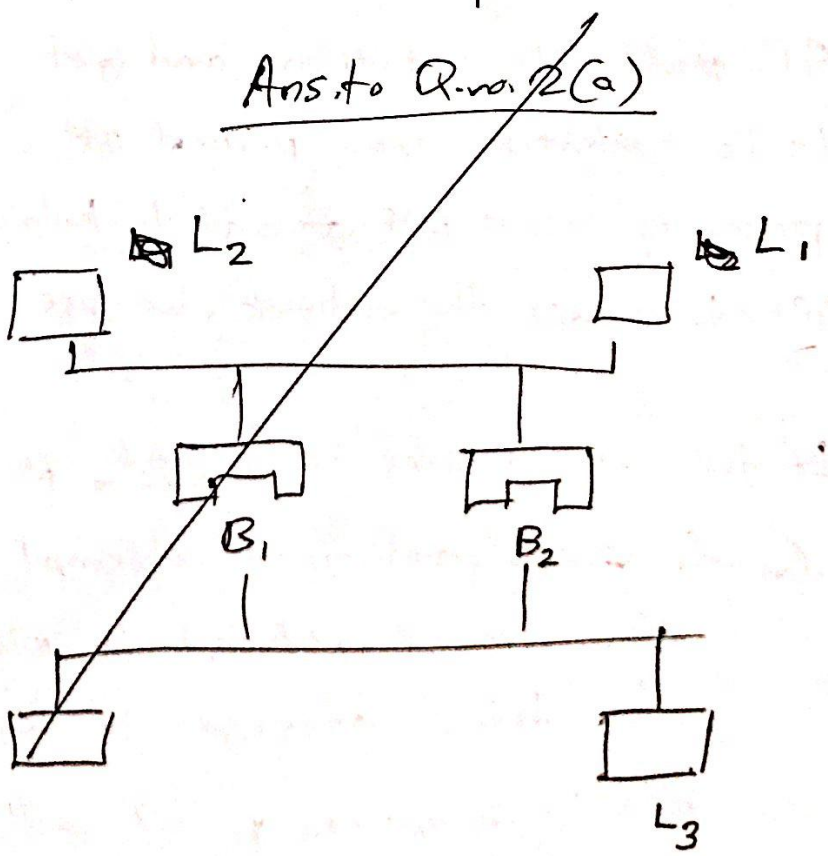
255.63

255.31

180041120

Subnets	255.0	255.32	255.64	255.96	255.128	255.160	255.192	255.224
First Address	255.1	255.33	255.65	255.97	255.129	255.161	255.193	255.225
Last Address	255.30	255.62	255.94	~~255.126~~ 255.126	255.158	255.190	255.222	255.254
Broadcast Address	255.31	255.63	255.95	255.127	255.159	255.191	255.223	255.255

Ans. to Q.no. 2(a)



Ans to Qno. 2(b)

DCF → Distributed Co-ordination Function is a ~~function~~ ~~of~~ sublayer on MAC ~~attitude~~ layer which is a contention period. Here CSMA/CA is used where stations fight to get access to medium.

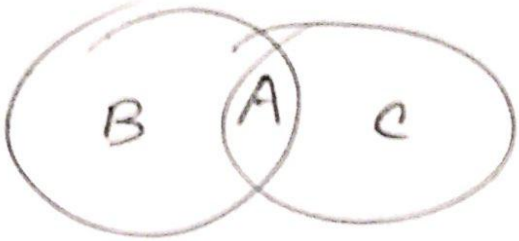
PCF → is an optional sublayer where a centralized AP polls the stations and gets accesse to medium. It is contention free period ~~not~~. PCF is has higher priority over DCF ~~on~~ and to help devices with only DCF to access the network, we use repeatation interval.

If the initial value is $8 = 2^3$, it means initially $k=3$.
In ~~for second attl~~ first attempt it will be $2^3 = 8$
for second attempt it will be $2^4 = 16$
for third attempt it will be $2^5 = 32$
In next attempt the packet will be transmitted.

Ans: 8, 16, 32.

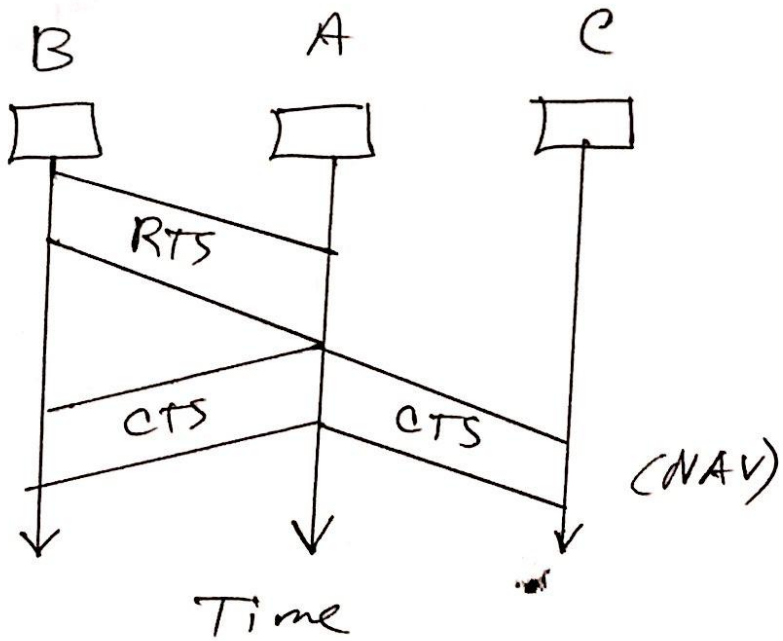
Ans to Q.no 2(c)

RTS-CTS can eliminate hidden station problem,



Here station B if sends to A will not know the existance of C since it is out of Range of station B. So, C is hidden with respect to B.

Using, RTS, station B can send an RTS to A. Then A will send a broadcast CTS. When C gets this CTS, it knows A is busy and sets NAV i.e. stops sensing medium.



In this way handshaking prevents the hidden station problem.

(4) (5)

~~(iv) $\bar{T}/p = (e^{2G} - 1)\left(\frac{k+1}{2}\right) + 1$~~

~~$G = 150 \times 1$, $k = 19$~~

~~$\therefore \bar{T}/p = (e^{2\times 150} - 1)\left(\frac{19+1}{2}\right) + 1$~~

Ans. to Q. no. 2(a)