2101-COL334 COL334/672 Major Exam 2021

Aayush Goyal

TOTAL POINTS

65 / 75

QUESTION 1

1 Question 1 10 / 10

+ **0 pts** no submission for this Q1

✓ **+ 10 pts** **correct**

+ **6 pts** Q1(a) is correct

+ **7 pts** Q1(a) is correct but Q1(b) is not not correct

✓ **+ 8 pts** **Q1(a) is correct but Q1(b) is either incomplete or has a silly mistake**

+ **5 pts** Q1(a) has incomplete explanations and part(b) is not done .

+ **0 pts** Click here to replace this description.

+ **9 pts** Q1(a) is correct but Q1(b) lacks steps and explanations

+ **3 pts** Q1(a) is only attempted without reaching to the answer

+ **2 pts** Q1(b) is only attempted

+ **1 pts** Click here to replace this description.

+ **4 pts** Click here to replace this description.

+ **9 pts** part(b) (ii) is unattempted

QUESTION 2

2 Question 2 13 / 15

Part A

✓ **+ 1 pts** **Scenario is possible.**

✓ **+ 1 pts** **In a round-robin or sequential manner, when one station is transmitting and no other station transmits**

✓ **+ 1 pts** **Correct time gap calculated between consecutive frames and stations**

+ **0 pts** Incorrect/Not Attempted

Part B

✓ **+ 1 pts** **Pure ALOHA is faster.**

✓ **+ 1 pts** **Pure ALOHA transmits as soon as the frame arrive whereas slotted ALOHA will wait for a slot to begin to transmit**

✓ **+ 1 pts** **At low load, probability of collision is very less**

+ **0 pts** Incorrect/Not Attempted

Part C

+ **0 pts** 2C - not attempted / incorrect

✓ **+ 3 pts** **2C - Correct**

(i) 5120 bits

(ii) 51200 bits

(iii) 512000 bits

Part D

+ **0 pts** 2D - not attempted / incorrect

✓ **+ 1 pts** **2D (i) - Correct**

There will be no collision.

OR

t3 = 4 micro sec (If you assume C was sleeping)

OR

t3 = 3.627 micro sec (If you assume C was waking)

+ **1 pts** 2D (ii) - Correct

t4 = It will never hear the collision

+ **1 pts** 2D (iii) - Correct

ans = na (A will never hear the collision)

✓ **+ 1 pts** **2D (iv) - Correct**

ans = 0 bits

OR

ans = na

Part E

+ **0 pts** 2E - not attempted / incorrect

✓ **+ 2 pts** **2E - correct explanation**

QUESTION 3

3 Question 3 11.5 / 15

✓ **+ 5 pts** **Part A**

+ **2.5 pts** Part A - partial

+ **5 pts** Part B

✓ + 2.5 pts Part B - Identified only problem but no/wrong solution

Part C

+ 1 pts Airtel Sim Card in Berlin registers with O2 operator which in turn registers with Airtel HSS in Delhi

✓ + 1 pts Get Visited Network address in Direct Routing:
Jio in Mumbai -(queries)-> Airtel in Delhi -(replies O2 address)-> Jio in Mumbai

✓ + 1 pts Correct Send in Direct Routing:
Jio in Mumbai exchanges directly with O2 in Berlin.

✓ + 1 pts Correct Send in Indirect Routing:
Jio in Mumbai sends data to Airtel HSS in Delhi

✓ + 1 pts Correct Forward in Indirect Routing:
Airtel in Delhi forwards the datagram to O2 in berlin

+ 0 pts Incorrect/Not Attempted

+ 2 pts Partial Correct

3B - Didn't identify the problem name correctly, solution works though

QUESTION 4

4 Question 4 11 / 11

+ 0 pts Not attempted

✓ + 0.75 pts a.i) 1 Day

✓ + 0.75 pts a i reason :: Records for a region don't change often

✓ + 0.75 pts a ii) 1 Day

✓ + 0.75 pts a ii reason) Same as i... Other answers also acceptable if reason is provided

✓ + 0.75 pts a iii) 1 minute

✓ + 0.75 pts a iii reason) Server load can change- to avoid caching

✓ + 0.75 pts b i) There is a local name server.... ttl is 1 day... so request is made 1 time in 24 hours

✓ + 0.75 pts b i reason

✓ + 0.75 pts b ii There is a local name server.... ttl is 1 day... so request is made 1 time in 24 hours

✓ + 0.75 pts b ii reason

✓ + 0.75 pts b iii) 12 requests

✓ + 0.75 pts b iii reason) ttl is 1 minute so expires frequently

✓ + 2 pts c) Multiple answers possible:
Web Server load could change during DNS response etc. TTL is very low so repeated requests(every min) with high latency.

" The question is 'why high latency might become an issue in his scheme' ". It is given that there is high latency

+ 0 pts Nothing correct

+ 11 pts All correct

QUESTION 5

5 Question 5 4.5 / 9

5(a)

✓ + 0 pts Incorrect choice or Incorrect answer

+ 0 pts Not answered

+ 1 pts Incorrect choice, but a proper explanation of at least 3 choices

+ 2.5 pts Correct choice mentioned with proper explanation of 1 choice

+ 2.5 pts Correct choice mentioned with proper explanation of 2 choices

+ 2.5 pts Correct choice mentioned with proper explanation of 3 choices

+ 3 pts Correct choice mentioned with proper explanation of all 4 choices

5(b)

+ 0 pts Incorrect answer or Incorrect choice

+ 0 pts Not answered

✓ + 1.5 pts Correct choice with partially correct explanation

+ 3 pts Correct choice with proper explanation

+ 0.5 pts Incorrect choice, but partially correct answer containing some valid points

5(c)

+ 0 pts 5(c) unattempted

+ 0 pts 5(c) incorrect

+ 1 pts 5(c) partially correct

+ 2 pts 5 (c) almost correct, with some some minor

flaw.

✓ **+ 3 pts** **5(c) correct**

+ 0 pts p

+ 0 pts call

5(b) sample answer:
Tail drop distributes buffer space unfairly among traffic flows and treats all traffic equally and does not differentiate between classes of service. If one of the flows is occupying most of the queue, the tail drop would let it occupy the complete queue, while the rest of the flows suffer from packet drops. This could also lead to overflooding as the dropped TCP flows try to retransmit w/o any synchronization.
Whereas RED distributes the buffer space much more fairly among different traffic flows, as it can be configured to be Flow-based. Therefore, if one of the flows is occupying most of the queue, RED would start dropping packets of that flow soon after it reached some threshold value, thus leaving space for other flows.

5(a) sample answer:
Disabling exponential backoff of timeouts will enable your TCP to recover from repeated loss (i.e., loss of retransmitted packets) more quickly.
For the others:
• If you disable timeout retransmissions, then you will lose performance any time a lost packet is not followed by enough duplicate acknowledgments to trigger fast retransmission (you will never recover from the loss).
• If you disable fast retransmission, then you will lose performance any time you could have detected a loss quickly by observing 3 duplicate acknowledgments (you will only recover from the loss later when the retransmission timeout finally expires).
• If you do not perform RTT estimation and do not adapt RTO based on it, then you're stuck with a fixed value for RTO. This may be too high, in which case you lose performance since you could have recovered from losses more quickly; or too low, in which case you will lose performance by retransmitting unnecessarily.

QUESTION 6

6 Question 6 **15 / 15**

✓ **+ 3 pts** **6(a) correct**

✓ **+ 3 pts** **6(b) correct**

+ 1.5 pts 6(b), had to explain bit more

✓ **+ 3 pts** **6(c) correct**

✓ **+ 3 pts** **6(d) correct**

- 1 pts 6(d) had to add more points

✓ **+ 3 pts** **6(e) correct**

+ 1.5 pts 6(e) partially correct

+ 0 pts unattempted

1 Question 1 **10 / 10**

+ **0 pts** no submission for this Q1

✓ **+ 10 pts** **correct**

+ **6 pts** Q1(a) is correct

+ **7 pts** Q1(a) is correct but Q1(b) is not not correct

✓ **+ 8 pts** **Q1(a) is correct but Q1(b) is either incomplete or has a silly mistake**

+ **5 pts** Q1(a) has incomplete explanations and part(b) is not done .

+ **0 pts** Click here to replace this description.

+ **9 pts** Q1(a) is correct but Q1(b) lacks steps and explanations

+ **3 pts** Q1(a) is only attempted without reaching to the answer

+ **2 pts** Q1(b) is only attempted

+ **1 pts** Click here to replace this description.

+ **4 pts** Click here to replace this description.

+ **9 pts** part(b) (ii) is unattempted

2 Question 2 13 / 15

Part A

✓ + 1 pts Scenario is possible.

✓ + 1 pts In a round-robin or sequential manner, when one station is transmitting and no other station transmits

✓ + 1 pts Correct time gap calculated between consecutive frames and stations

+ 0 pts Incorrect/Not Attempted

Part B

✓ + 1 pts Pure ALOHA is faster.

✓ + 1 pts Pure ALOHA transmits as soon as the frame arrive whereas slotted ALOHA will wait for a slot to begin to transmit

✓ + 1 pts At low load, probability of collision is very less

+ 0 pts Incorrect/Not Attempted

Part C

+ 0 pts 2C - not attempted / incorrect

✓ + 3 pts 2C - Correct

(i) 5120 bits

(ii) 51200 bits

(iii) 512000 bits

Part D

+ 0 pts 2D - not attempted / incorrect

✓ + 1 pts 2D (i) - Correct

There will be no collision.

OR

t3 = 4 micro sec (If you assume C was sleeping)

OR

t3 = 3.627 micro sec (If you assume C was waking)

+ 1 pts 2D (ii) - Correct

t4 = It will never hear the collision

+ 1 pts 2D (iii) - Correct

ans = na (A will never hear the collision)

✓ + 1 pts 2D (iv) - Correct

ans = 0 bits

OR

ans = na

Part E

+ 0 pts 2E - not attempted / incorrect

✓ + 2 pts 2E - correct explanation

3 Question 3 **11.5 / 15**

✓ **+ 5 pts** **Part A**

+ 2.5 pts Part A - partial

+ 5 pts Part B

✓ **+ 2.5 pts** **Part B - Identified only problem but no/wrong solution**

Part C

+ 1 pts Airtel Sim Card in Berlin registers with O2 operator which in turn registers with Airtel HSS in Delhi

✓ **+ 1 pts** **Get Visited Network address in Direct Routing:**

Jio in Mumbai -(queries)-> Airtel in Delhi -(replies O2 address)-> Jio in Mumbai

✓ **+ 1 pts** **Correct Send in Direct Routing:**

Jio in Mumbai exchanges directly with O2 in Berlin.

✓ **+ 1 pts** **Correct Send in Indirect Routing:**

Jio in Mumbai sends data to Airtel HSS in Delhi

✓ **+ 1 pts** **Correct Forward in Indirect Routing:**

Airtel in Delhi forwards the datagram to O2 in berlin

+ 0 pts Incorrect/Not Attempted

+ 2 pts Partial Correct

3B - Didn't identify the problem name correctly, solution works though

4 Question 4 11 / 11

+ **0 pts** Not attempted

✓ **+ 0.75 pts** a.i) 1 Day

✓ **+ 0.75 pts** a i reason :: Records for a region don't change often

✓ **+ 0.75 pts** a ii) 1 Day

✓ **+ 0.75 pts** a ii reason) Same as i... Other answers also acceptable if reason is provided

✓ **+ 0.75 pts** a iii) 1 minute

✓ **+ 0.75 pts** a iii reason) Server load can change- to avoid caching

✓ **+ 0.75 pts** b i) There is a local name server.... ttl is 1 day... so request is made 1 time in 24 hours

✓ **+ 0.75 pts** b i reason

✓ **+ 0.75 pts** b ii There is a local name server.... ttl is 1 day... so request is made 1 time in 24 hours

✓ **+ 0.75 pts** b ii reason

✓ **+ 0.75 pts** b iii) 12 requests

✓ **+ 0.75 pts** b iii reason) ttl is 1 minute so expires frequently

✓ **+ 2 pts** c) Multiple answers possible:

Web Server load could change during DNS response etc. TTL is very low so repeated requests(every min) with high latency.

" The question is 'why high latency might become an issue in his scheme' ". It is given that there is high latency

+ **0 pts** Nothing correct

+ **11 pts** All correct

5 Question 5 4.5 / 9

5(a)

✓ + 0 pts **Incorrect choice or Incorrect answer**

+ **0 pts** Not answered

+ **1 pts** Incorrect choice, but a proper explanation of at least 3 choices

+ **2.5 pts** Correct choice mentioned with proper explanation of 1 choice

+ **2.5 pts** Correct choice mentioned with proper explanation of 2 choices

+ **2.5 pts** Correct choice mentioned with proper explanation of 3 choices

+ **3 pts** Correct choice mentioned with proper explanation of all 4 choices

5(b)

+ **0 pts** Incorrect answer or Incorrect choice

+ **0 pts** Not answered

✓ + 1.5 pts **Correct choice with partially correct explanation**

+ **3 pts** Correct choice with proper explanation

+ **0.5 pts** Incorrect choice, but partially correct answer containing some valid points

5(c)

+ **0 pts** 5(c) unattempted

+ **0 pts** 5(c) incorrect

+ **1 pts** 5(c) partially correct

+ **2 pts** 5 (c) almost correct, with some some minor flaw.

✓ + 3 pts **5(c) correct**

+ **0 pts** p

+ **0 pts** call

5(b) sample answer:
Tail drop distributes buffer space unfairly among traffic flows and treats all traffic equally and does not differentiate between classes of service. If one of the flows is occupying most of the queue, the tail drop would let it occupy the complete queue, while the rest of the flows suffer from packet drops. This could also lead to overflooding as the dropped TCP flows try to retransmit w/o any synchronization.
Whereas RED distributes the buffer space much more fairly among different traffic flows, as it can be configured to be Flow-based. Therefore, if one of the flows is occupying most of the queue, RED would start dropping packets of that flow soon after it reached some threshold value, thus leaving space for other flows.

5(a) sample answer:
Disabling exponential backoff of timeouts will enable your TCP to recover from repeated loss (i.e., loss of retransmitted packets) more quickly.
For the others:

• If you disable timeout retransmissions, then you will lose performance any time a lost packet is not followed by enough duplicate acknowledgments to trigger fast retransmission (you will never recover from the loss).
• If you disable fast retransmission, then you will lose performance any time you could have detected a loss quickly by observing 3 duplicate acknowledgments (you will only recover from the loss later when the retransmission timeout finally expires).
• If you do not perform RTT estimation and do not adapt RTO based on it, then you're stuck with a fixed value for RTO. This may be too high, in which case you lose performance since you could have recovered from losses more quickly; or too low, in which case you will lose performance by retransmitting unnecessarily.

6 Question 6 **15 / 15**

✓ **+ 3 pts** **6(a) correct**

✓ **+ 3 pts** **6(b) correct**

+ 1.5 pts 6(b), had to explain bit more

✓ **+ 3 pts** **6(c) correct**

✓ **+ 3 pts** **6(d) correct**

- 1 pts 6(d) had to add more points

✓ **+ 3 pts** **6(e) correct**

+ 1.5 pts 6(e) partially correct

+ 0 pts unattempted

भारतीय प्रौद्योगिकी संस्थान दिल्ली
INDIAN INSTITUTE OF TECHNOLOGY DELHI

मुख्य परीक्षा उत्तर पुस्तिका
MAJOR TEST ANSWER BOOK

नाम
Name AAYUSH GOYAL

अनुक्रमांक
Entry No. 2019CS10452

पाठ्यक्रम सं.
Course No. COL334

ग्रुप संख्या
Group No.

पाठ्यक्रम शीर्षक
Course Title Computer Networks

दिनांक
Date 15-11-2021

प्रयोग किए गए अनुवर्ती पृष्ठों की संख्या
No. of continuation sheets used 2

प्रश्न सं. Q. No.	प्राप्त अंक Marks
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	
11.	
12.	
कुल TOTAL	

पाठ्यक्रम निर्धारक के हस्ताक्षर और दिनांक
Signature of Course Co-ordinator and date

अनुचित साधनों का प्रयोग करने वाले छात्रों को निलम्बित/निष्कासित किया जा सकता है।
Students using unfair means are liable to be punished by Suspension/Expulsion

परीक्षा केन्द्र में सेलफोन, काम्युनिकेटर्स व पीडीए साधनों का प्रयोग करना सख्त मना है।
Use of cell-phones, Communicators & PDAs in the Examination Hall is Strictly prohibited.

सभी पृष्ठों पर लिखें। Write on all pages.

7)(a) The numbers are given in the hexadecimal format. Now they will be:

1st 3456 =
0011 0100 0101 0110
2nd ABCC
1010 1011 1100 1100
3rd 02BC
0000 0010 1011 1100
4th FFFF
1111 1111 1111 1111

Adding 1st & 2nd
0 0011 0100 0101 0110
+ 1010 1011 1100 1100

Adding 3
1 1110 0000 0010 0010
+ 0000 0010 1011 1100

Adding 4th
1 1100 0010 1110 1110
+ 1111 1111 1111 1111

1 1100 0011 1100 1110

1's complement
0011 1100 0011 1101
0010 1111 0000 1100 0010

The checksum computed at Host A

Since the 2nd item got changed the new number will be ABCE (1010 1011 1100 1110)

To calculate the checksum :-

1st 0011 0100 0101 0110
2nd + 1010 1011 1100 1110
1110 0000 0010 0100
3rd + 0000 0010 1011 1100
1110 0010 1110 0000
4th + 1110 1110 1110 1110
1101 0001 1100 1110
1
1101 0001 1100 1111
8's complement 0010 1110 0011 0000

Checksum at Host B.

Now the 2 checksum are diff and hence B knows there is some error. B know which bit is wrong. But getting the doing the correction or knowing which one is wrong is not

possible. Only thing it can do is ask to re-send the packet.

1)(b) 50×10^6 b/s

(i) If 90 frames come then it means we have
90×5000 bits to transfer
$= 45 \times 10^4$ b/s.
Since the channel is capable of transmitting ~~45x1~~ 50×10^6 bits in a second, it can transfer the entire 90 frames in less than a second.

Hence there is no queueing delay & transmission time =
$\frac{45 \times 10^4}{50 \times 10^6}$ s
0.9×10^{-2} s
Transmission $= 9 \times 10^{-3}$ s
Queueing $= \frac{1}{90}$ s

(ii) 45×10^5 b/s and hence there will be no queueing delay

Queueing delay $= \frac{1}{100}$ s
Transmission time $= \frac{45 \times 10^5}{50 \times 10^6}$ s
$= 9 \times 10^{-2}$ s

6) (a) A 'nonce', as it means, n-once-in-a-lifetime, is an once in a life time number send to the other party for ~~all~~ identification & verifying purposes. It is generated randomly by the 1st party & then send over in the encrypted-form. If the other party is able to ~~identify the~~ decrypt the message & get the nonce, they send it back to 1st party as a proof that we are real & identified you. Used for authentication purposes & other things related to network security.

b) Man in the middle attack can be performed by taking the message from router and decrypting them using router's public key. Now the man in middle (say Trudy) get's the message and can change the message. ~~Now~~ They can now pass on the message encrypted with their private key & send the public key. Now when the receiver get's the message, it extracts the message using the public

key sent by Trudy (the man in middle). Thus it keeps getting the wrong messages from Trudy & keeps using Trudy's public key for decryption purpose it can also replay the messages ~~the can~~ & it can lead of DoS (Denial of service) for the receiver. Thus as a consequence, the client may keep getting wrong messages or maybe experiences the same message again and again.

(c) The Man-in-the-middle attack was possible because Trudy was able to ~~chang~~ fake the public key. Now in this case what we ~~can~~ do is, we have ~~an~~ a certification authority which provides us with the public key of user's when they are sent the certificate. The certificate is encrypted with CA's private key & ~~hence~~ their public key is not known. Hence Trudy cannot decrypt the certificate & Trudy won't be able to change the public key of router with it's own public key.

once the receiver gets the certificate, they send it over to CA & they decrypt the certificate to get router's public key. This public key is sent to Receiver & with identity of router. Hence the receiver always gets the correct public key & Truly is not able to fake public key. To avoid the repeated messages, they can exchange a (nonce), this will help them identify the replayable messages.

(d) ~~The~~ key management is very important to maintain the authenticity of ~~the~~ encryption & decryption. As we have seen in the above part, how CA needs to keep their encryption & decryption keys private to prevent man in the middle. If the decryption key somehow gets leaked then again it is of no use & the whole point of having such an authority is wasted. Also it cannot happen that no one knows ~~that~~ that key. There will be atleast one person

who knows ~~they~~ the key, but what they can make sure is that there are not much people who know about & can possibly leak it. Similarly the private keys are used for ~~encryp~~ authentication purposes. Hence it is the responsibility to prevent leak of ~~the~~ private key & making digital signatures become possible. Thus key management is very important.

(e) In AH we have only Message Integrity & Authentication. Hence ~~that~~ there is already no point of encrypting the ~~ICP packet or~~ it's TCP header.

So TCP header is not encrypted in AH whether Transport Mode or Tunnel mode.

In ESP, we have Message Integrity, Authentication & Confidentiality. Hence the TCP payload is also encrypted.

In the Tunnel mode we encrypt the entire packet (including the

TCP header) ~~but in Transport~~ and attach a new header to it at the AS. Hence TCP header is encrypted in the ESP tunnel mode.

In ESP transport mode, we don't encrypt the header only the payload is encrypted. Hence TCP header is not encrypted in ESP transport mode.

22) (a) 10^6 bits/s

Each station sends 10 frames.

1 frame = 1000 b

bits/s sent by the station = $1000 (10) = 10^4$ b/s

Since there are 50 stations only, so total 5×10^5 b/s are sent. Hence there can exist a scenario when the packet's are collision free. They can send the packets in a Round robin fashion. The second station sends 0.01 second after first station released it's packet. And similarly for others, each after 0.01 s of previous station.

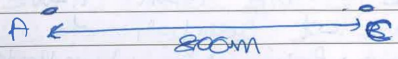
(b) In pure ALOHA, we send the packet whenever we want. But in slotted ALOHA we send the packet only at the start of next slot. Making of slots is done so as to avoid collisions b/w the packets. But at low load, there might not be enough number of packets that we need to check for collisions.

In slotted ALOHA, we are bound to send the packet only at the start of next slot. Hence the packet keeps ~~waiting~~ waiting & there is high chance that the slot was idle, because of low-load. In pure ALOHA, we will not do this waiting & can send the packet directly. Hence delay at low-load is less in pure ALOHA than slotted ALOHA.

(c) As the data rate increase, the time taken to transmit the frame will reduce. Thus as the frame takes less amount of time & assuming that the time gap required to detect collision is constant we will have to increase the time required to send a frame. For that we need to increase the frame size proportionally.

For 100 Mbps,
frame size = 5120 bits
for 1 Gbps
FS = 51200 bits
for 10 Gbps
FS = 512×10^3 bits.

(d)



Time to reach C = $\frac{800}{2.2 \times 10^8}$

$\frac{8}{2.2}\ \mu s = \frac{40}{11}\ \mu s$

$= 3.63\ \mu s$

Thus the frames would have reached C before it starts sending itself.

Hence C detects collision at
$t_3 = 4\ \mu s$

& A will get this message after $t_3 + \frac{800}{2.2 \times 10^8}$ s

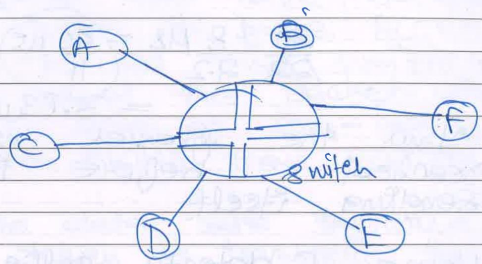
$t_4 = 4\ \mu s + 3.63\ \mu s = 7.63\ \mu s$

Now A would have sent
$7.63 \times 10^{-6} (5)(10^6)$ bits
$= (5)(7.63)$ bits
~ 39 bits

C will not have sent any bit because it detects the collision.

$\frac{3}{7.63}$
38.1

(e) We can centralize the whole process. We can have common switch at center to control & transfer the packets over the wired channel.



Now if a packet is sent ~~form~~ from A to B, it is sent by switch. If at the same time C→B also comes, then it can stop one of the packets & send it after the other one is done.

We can also do Time Division ~~&~~ ~~or Frequency division~~ to avoid the collisions.

(4) (a) (i) Since query for the same NS maybe ~~maybe~~ made again & again, it would be good to keep the NS in cache for longer time. So TTL = 1day

(ii) Similar to above, we can keep the A record for them for a longer time. The TTL = 1day.

(iii) A record for this depends on the most lighty loaded web-server in that region & if we cache it for long time it will actually become the busiest web server. Hence we need to cache it only for a smaller time. So TTL = 1 minute

(b) ~~In one HOUR, we will have 12 Requests.~~

~~(i) 12 times we will access the ROOT since web-servers don't have their own caching.~~

~~(ii) We will query the MS1.hb.com 1 time since the time taken to reply will be less~~

(b) Total we will make 12 requests

(ii) we will query it only once. After that it keeps the record in cache. Since the queries are coming from the same address, we will always find our entry in the cache (assuming TTL = 1 day there).

iii) They will be contacted 12 time for the least busy server since, the least busy server will keep getting changed after every 1 minute (TTL = 1 min). Thus 12 access will be made to it as well.

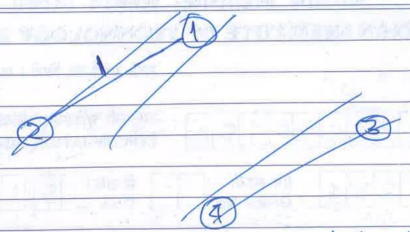
(i) Only once since the Root will have in it's cache the NS record which is needed for www.distributed.hb.com & we will get what we need from the cache itself.

)(c) Since we are only passing the least busy web server, it might happen that some server which is far away remains the least busy. Hence every time we are contacting a far kept server. The propagation time might become much greater than time saved from getting least busy serv

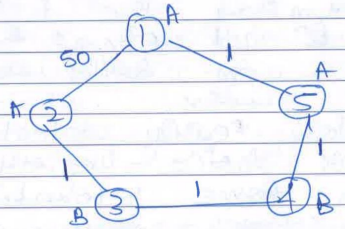
Q5. (a) CDN will be the best choice to get the greatest benefit. By assuming the RTT to be uniform & not doing RTO adaptation, we can save a lot of time.

(b) Random early detection is a better choice. We drop the packets with some probability initially. This saves some time compared to what is needed when the router drops the packet. Router will have to send the message for the same & it takes time. The sender gets to know that packet was dropped & it resends those packets again. To avoid this path, the sender can itself drop some packet & he will know now I need to slow down & re-send this packet instead of router having to tell sender this.

(c)

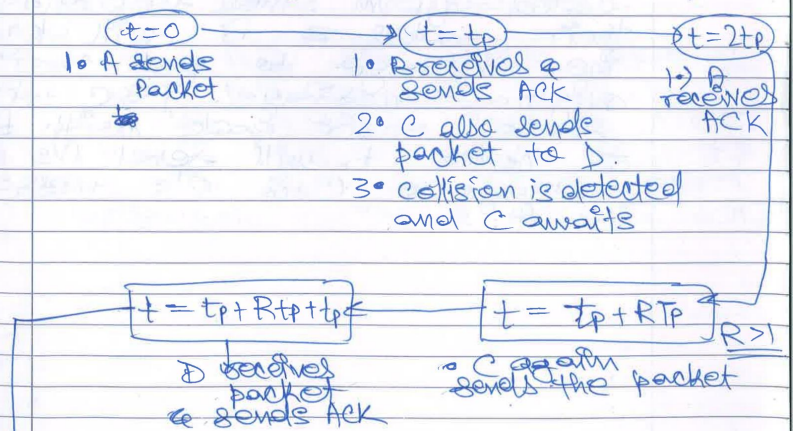


The network could be like this :-

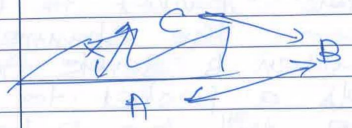


Suppose 2, 1, 5 are in Alice's control & 3, 4 are in Bob's control. Now
To go from 2 to 1, Alice will send packet 3. At B to send packet to 1, 3→2→1 has only 2 hops compared to 3→4→5→1 with 3 hops.
So 3 will send packet 2. But will again send packet to 3 Hence we are stuck in a loop btw 2 and 3 while sending packet from 2 to 1.

(Q3(a)) Initially everything will be fine when A sends packet to B because the channel is idle. But when B sends ACK, C also sends a packet to D. Hence there will be 2 packets at the same time in channel. This will lead to collision say C will have to wait for some time, that time is T_B. Since there is no other data being sent, it will finally send D the message in 2nd attempt.



)) It is called Tunneling problem ☒



A & C cannot contact each other.

It will make the transmission btw A & C long & many hops will be needed.

To solve this :-
A will send to B in coded form & C will send to B in coded form. They will share their codes & B will decode the message to get their original message. A & C will share their code with B & hence B will send A's message to C & C's message to A.

thus message from reaching [illegible]

भारतीय प्रौद्योगिकी संस्थान दिल्ली
INDIAN INSTITUTE OF TECHNOLOGY DELHI
सभी पृष्ठों पर लिखें। Write on all pages.

अनुक्रमांक Entry No. 2019CS10452 अनुवर्ती पुस्तिका संख्या CONTINUATION BOOK No. 2

पाठ सं. Course No. COL334 ग्रुप संख्या Group No. दिनांक Date 15/11/2021

2)(c) (ii) In the shortest routing the message will be sent to servers of Airtel from Jio. They will know that the Airtel user is currently using O2. Hence they will transmit the message from Airtel to O2.

(iii) In this the user's identity will be changed to O2 user by the records kept in Airtel HSS. After changing records, the Jio user can directly send messages to the new O2 user.