

**School of Computing**

**Final Assessment for AY2021/2022, Semester 2**

**CS2105 - Introduction to Computer Networks**

## Multiple Choice Questions

In this section, each question will have 5 choices and only 1 of them is correct.

You will get full marks if you choose the correct answer; otherwise, you get zero mark. The order of the 5 choices will be randomized.

1. What are the typical behaviors of local DNS servers, authoritative DNS servers and root DNS servers?

(1 mark)

Local and authoritative DNS servers process DNS queries in an iterative manner; root DNS servers process DNS queries in a recursive manner.

Local DNS servers process DNS queries in an iterative manner; authoritative DNS servers and root DNS servers process DNS queries in a recursive manner.

Local and authoritative DNS servers process DNS queries in a recursive manner; root DNS servers process DNS queries in an iterative manner.

All three DNS servers process DNS queries in a recursive manner.

All three DNS servers process DNS queries in an iterative manner.

2. DNS and DHCP are two crucial services of the Internet that are implemented at the \_\_\_\_ of the Internet. DNS is built on top of \_\_\_\_; DHCP is built on top of \_\_\_\_.

(1 mark)

edge; UDP; TCP

edge; UDP; UDP

core; TCP; TCP

core; UDP; UDP

☒ core; UDP; TCP

3. If you want to associate a client-side socket with a particular port number, what should you do?

(1 mark)

let the OS do the job for you

 use the **bind( )** method

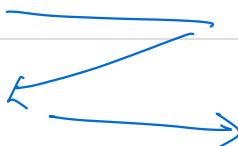
use the **accept( )** method

use the **connect( )** method

use the **listen( )** method

4. What are the minimum number of packets that need to be communicated in order to establish a TCP connection? How many of them need to set the SYN flag to be 1?

(1 mark)

2 and 2	
<u>3</u> and 2	
3 and 3	
4 and 3	
2 and 3	

1 0 0 0 - 00001010

5. An IP datagram with destination address 192.168.1.10 reaches a router with the following 5 routing entries. Which entry will be used to forward this packet?



(1 mark)

0000

	192.168.8.0/22
0	192.168.1.0/24
X	192.168.1.16/27
X	192.168.0.0/23
X	192.168.1.0/29

6. Which of the following is a VALID subnet mask?

(1 mark)

	255.254.255.0
	255.255.208.0
	255.240.0.0
	255.232.0.0
	127.0.0.0

7. The behavior of a TCP sender can be influenced by a feedback packet received from a TCP receiver. Which of the following statement is FALSE?

(1 mark)

☒ It is possible that a TCP receiver's feedback packet triggers the TCP sender to transmit a new data packet.

☒ It is possible that a TCP receiver's feedback packet triggers the TCP sender to re-transmit an old data packet.

☒ It is possible that a TCP receiver's feedback packet triggers the TCP sender to transmit multiple new data packets.

☐ It is possible that a TCP receiver's feedback packet triggers the TCP sender to re-transmit multiple old data packets.

☐ It is possible that a TCP receiver's feedback packet does not trigger any action taken by the TCP sender.



8. An IP datagram is sent along a path from host A to router R1 and then to router R2 and then to host B. The MTUs on the links are as follows:

Link A to R1: MTU = 1,500

Link R1 to R2: MTU = 500

Link R2 to B: MTU = 1,500



Host A sends an IP datagram of total size 1,500 bytes (including IP header) to B. Which of the following statements is **TRUE**?

1480

(1 mark)

R1 will fragment the IP datagram from A into 3 fragments, and R2 will re-assemble the fragments.

☒ R1 will fragment the IP datagram from A into 4 fragments, and R2 will re-assemble the fragments.

☐ R1 will fragment the IP datagram from A into 3 fragments, and B will re-assemble the fragments.

☐ R1 will fragment the IP datagram from A into 4 fragments, and B will re-assemble the fragments.

☐ A will fragment the IP datagram into 4 fragments, and B will re-assemble the fragments.

9. Assuming a router vendor wants to design a NAT router that can support the maximal number of mappings in its NAT translation table. How much memory should the NAT router have, i.e., how big, in bytes, should the NAT translation table be? (Assume a simple table structure with no additional indexing, etc.)

(1 mark)

65,536 bytes	4 bytes $\rightarrow$ 2	12 bytes per entry
<input checked="" type="radio"/> 786,432 bytes	8 bytes	
524,288 bytes	$2^{14}$	
262,144 bytes		
1,048,576 bytes		

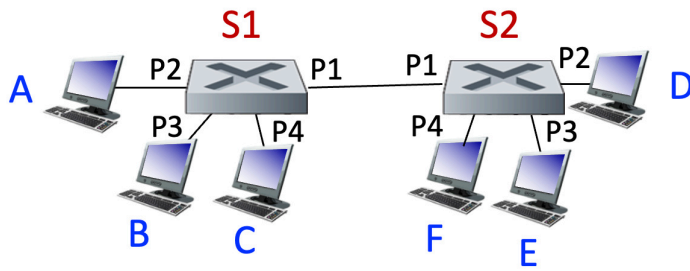
10. Assume we have a subnet that consists of 2 switches, S1 and S2. Each switch has 4 ports: P1 to P4. The port S1.P1 is connected with an Ethernet cable to the port S2.P1. On S1, 3 hosts are connected: A on S1.P2, B on S1.P3, and C on S1.P4. On S2, 3 hosts are connected: D on S2.P2, E on S2.P3, and F on S2.P4.

After S1 has completely learned its switch table after all hosts in the subnet have communicated with each other, what does the switch table look like in S1?

We use the following notations:

S1.P1 means port 1 on switch S1.

A.MAC means the MAC address of host A.



(1 mark)

The switch table on S1 looks like this:

- < A.MAC, S1.P2, TTL >
- < B.MAC, S1.P3, TTL >
- < C.MAC, S1.P4, TTL >

The switch table on S1 looks like this:

- < A.MAC, S1.P2, TTL >
- < B.MAC, S1.P3, TTL >
- < C.MAC, S1.P4, TTL >
- < D.MAC, S1.P1, TTL >
- < E.MAC, S1.P1, TTL >
- < F.MAC, S1.P1, TTL >

The switch table on S1 looks like this:

- < A.MAC, S1.P2, TTL >
- < B.MAC, S1.P3, TTL >
- < C.MAC, S1.P4, TTL >
- < D.MAC, S2.P2, TTL >
- < E.MAC, S2.P3, TTL >
- < F.MAC, S2.P4, TTL >

The switch table on S1 looks like this:

- < A.MAC, S1.P2, TTL >
- < B.MAC, S1.P3, TTL >
- < C.MAC, S1.P4, TTL >
- < D.MAC, S2.P1, TTL >
- < E.MAC, S2.P1, TTL >
- < F.MAC, S2.P1, TTL >

The switch table on S1 looks like this:

< D.MAC, S2.P2, TTL >

< E.MAC, S2.P3, TTL >

< F.MAC, S2.P4, TTL >

11. Assume host A (IP address: 130.54.0.13) and host B (IP: 130.54.0.17) are on a subnet 1 which is also connected to router R1's first port (IP: 130.54.0.1). Host C (IP: 132.168.0.10) is on a different subnet 2, which is also connected to R1's second port (IP: 132.168.0.1). Assume that A has just been booted up and its ARP table is empty. Which of the following ARP queries would you likely see in subnet 1 if all the hosts communicate with each other?

- i) In subnet 1: <MAC FF-FF-FF-FF-FF-FF; 130.54.0.17>  
 ii) In subnet 1: <MAC FF-FF-FF-FF-FF-FF; 130.54.0.1>  
 iii) In subnet 1: <MAC FF-FF-FF-FF-FF-FF; 132.168.0.10>

(1 mark)

i) and ii)

i), ii) and iii)

ii) and iii)

i) and iii)

i) only

12. Which of the following statements is/are **TRUE** about the network and link layers?

- ✓ i) Hosts will not process a received IP datagram if the destination IP address in the datagram does not match the host's interface IP address (except if it is a broadcast IP address).
- ✗ ii) Routers will not process a received IP datagram if the destination IP address in the datagram does not match the router's interface\* IP address (except if it is a broadcast IP address).
- ✓ iii) Hosts will not process a received link layer frame if the destination MAC address in the frame does not match the host's interface MAC address (except if it is a broadcast MAC address).

\*: The interface on which the datagram was received.

(1 mark)

i) and ii)
ii) and iii)
i) and iii)
i), ii) and iii)
None of the others

13. Which of the following statements about digital signatures is **FALSE**?

(1 mark)

If a document signed with a digital signature then usually the document is unencrypted and still readable.



The digital signature of a document has a fixed length (in bits) and in general it is shorter than the document itself, which can have any length.



If Alice applies Bob's public key to a digital signature and the decrypted signature (which is a digest) is equal to the document's digest that Alice computed, then she is assured that Bob signed the document.



A digital signature ensures that only a few recipients can read the signed document.

It is important that Bob's public key can be verified, for example with a Certificate Authority (CA).

14. Which of the following statements about Certificate Authorities (CA) are **FALSE**?  
(1 mark)

The top-level so called Root CAs self-sign their own certificate(s) of their public key(s) because no organization is above them who could do so. So in the CA hierarchy we trust the Root CA public keys because we trust the Root CAs.

A certificate that, for example, certifies Bob's public key may be verified by multiple levels of Intermediate CAs until at the top it is signed by a Root CA.

If the certificate that is used to secure the SSL/HTTPS protocol on a server is successfully verified for a website, then this allows the browser to show a "lock" mark next to the URL as a visual confirmation.

A rogue CA could easily sign a fake certificate, for example, for Meta, and it would be very difficult to track down which CA was responsible for such a malicious action.

A SSL/HTTPS certificate can be self-signed (i.e., not signed by a CA, rather a developer signs it him/herself) to test the functionality of a website. However, browsers will show a warning for self-signed websites.

15. Modern video codecs (compressors/decompressors) such as H.264 use motion compensation (MC) in order to compute a smaller difference and use fewer bits between frames, during the encoding process. Which of the following statements about MC is **FALSE**?

(1 mark)

MC reduces the calculated difference between 2 frames if an object has moved (e.g., a car) between the 2 frames.

MC reduces the calculated difference between 2 frames if the camera was moving (e.g., horizontal rotation, which is also called panning).

If the calculated difference between 2 frames is smaller, then this reduces the number of bits that are required to encode the difference, i.e., a higher compression is achieved.

MC is a very simple algorithm and doesn't require much computation by the encoder.

We could imagine an MC algorithm where we don't just compare frame  $i$  with frame  $i+1$ , but also with frame  $i+2$  or frame  $i+3$ . Then the encoder could use the minimal difference and also put into the bitstream which frame was used to compute the difference.



16. The binary exponential backoff algorithm that is used in the CSMA/CD algorithm has a maximum value of  $m = 10$ . Which of the statements below is correct, if the maximal value of  $m$  is reached in the algorithm?

(1 mark)

The CSMA/CD algorithm waits for a while and then restarts the backoff algorithm with  $m = 0$ .



The value of  $m$  will just stay at  $m = 10$  and the CSMA/CD algorithm will try again.

The CSMA/CD algorithm will use another random value of  $m$  between 1 and 10 and try again.

The CSMA/CD algorithm at the sender gives up and the frame will be dropped, i.e., the algorithm starts to transmit the next frame.

The value of  $m$  will never reach 10.

17. In Lecture 10 we have learned that with audio streaming we may be able to do adaptive playout. Which of the following statement is **FALSE** about adaptive audio playout?
- (1 mark)

Adaptive playout may shorten or lengthen the periods of silence at the client side.

With adaptive playout the end-to-end latency (from microphone to speakers/headphones) sometimes becomes longer or shorter during a session.

With adaptive playout the audio of a talkspurt may be compressed or expanded at different times during a session.

With adaptive playout we want to strike a balance between network loss and delay loss.

It is not simple to implement the idea of adaptive playout with video.

18. When data is transmitted at the application layer (e.g., media data) over a channel that may experience some losses at the lower layers, then 2 of the possible methods to recover lost information at the receiver are:

- (a) packet **retransmissions**, for example using a transport protocol such as TCP, or
- (b) **FEC**, where additional redundant information is transmitted through a lossy channel.

Which of the following statements is **FALSE**?

(1 mark)

If a channel has a very long RTT (round-trip time) then FEC may be a better choice compared to retransmissions.

If a server transmits the same data to many different receivers then FEC may be a good choice (e.g., broadcasting).

If the loss rate varies in the channel, i.e., sometimes the channel has few losses and sometimes a lot, then using retransmissions may be more efficient.

FEC is designed for a certain maximum loss rate. If the loss rate exceeds the designed maximum loss rate, then data will be lost.



FEC adds a variable overhead to data transmissions.

## Multiple Response Questions

In this section, each question will also have 5 choices, but the number of correct answers may range from 1 to 5. The order of the 5 choices will also be randomized. Your final score will be calculated by the following formula:

**Full Marks \* (Number of Selected Correct Answers - Number of Selected Incorrect Answers) / Total Number of Correct Answers**

19. Consider a Go-Back-N reliable transmission protocol with a k-bit sequence number and sending window of size 3, operating over a channel that can delay, corrupt or lose packets, but not reorder them.

The sender has just sent a new packet with sequence number 0.

Which of the following events could have directly preceded (came before) this (i.e. no other packets were sent or received in between)?

(2 marks)

0 1 2 3 ↓

3

- |                                     |  |
|-------------------------------------|--|
| <input type="checkbox"/>            | Sender received an ACK with sequence number 1. |
| <input type="checkbox"/>            | Sender received an ACK with sequence number 5. |
| <input checked="" type="checkbox"/> | Sender sent a packet with sequence number 3.   |
| <input checked="" type="checkbox"/> | Sender sent a packet with sequence number 7.   |
| <input type="checkbox"/>            | Sender received an ACK with sequence number 3. |

20. Which of the following statement(s) about the rdt 2.2 and rdt 3.0 protocols is/are TRUE?  
(2 marks)

☐

When receiving a duplicate packet **pkt0**, the rdt 2.2 receiver sends an acknowledgement **ACK0** for the duplicate packet.

☐

When receiving a duplicate packet **pkt0**, the rdt 3.0 receiver sends an acknowledgement **ACK0** for the duplicate packet.

☐

When receiving a duplicate acknowledgement **ACK0**, the rdt 2.2 sender resends the next packet **pkt1**.

☐

When receiving a duplicate acknowledgement **ACK0**, the rdt 3.0 sender resends the next packet **pkt1**.

☐

When receiving a corrupted acknowledgement, both the rdt 2.2 and rdt 3.0 senders do nothing.

64  
101  
128+32

21. Which of the following IP addresses belong to the subnet 192.168.160.0/19?  
(2 marks)

<input checked="" type="checkbox"/>	192.168.150.202
<input checked="" type="checkbox"/>	192.168.170.22
<input checked="" type="checkbox"/>	192.168.180.1
<input checked="" type="checkbox"/>	192.168.190.254
<input checked="" type="checkbox"/>	192.168.200.25

22. Which of the following information is/are included in the packet headers of both UDP and TCP?  
(2 marks)

<input checked="" type="checkbox"/>	Source and destination port numbers
<input type="checkbox"/>	Source and destination IP addresses
<input type="checkbox"/>	Packet length
<input checked="" type="checkbox"/>	Checksum
<input type="checkbox"/>	Header length

23. Which of the following statement(s) are TRUE about Autonomous Systems (AS)?  
(2 marks)

☐

The routing information (tables) for the internal routing in an AS are normally manually configured.

☐

An AS is controlled by a single administrative entity (organization).

☐

An AS can only contain one subnet.

☒

A single administrative entity (organization) may control multiple ASes.

☐

An AS must use NAT routers at its edges.

24. An IP datagram is sent along a path from host A to router R1 and then to router R2 and then to host B. Both of the routers have 2 interfaces each. We use a subscript notation to identify the interfaces. For example,  $R1_A$  is the interface of R1 that is connected to A.  $R1_{R2}$  is the interface of R1 that is connected to R2, etc.

Which of the following statement(s) are **TRUE** about the ARP tables?

(2 marks)

$A \rightarrow R1 \rightarrow R2 \rightarrow B$



The ARP table in host A contains the following entry:

< IP address of B, MAC address of  $R1_A$ , TTL >



The ARP table(s) in router R2 contain the following entry:

< IP address of B, MAC address of B, TTL >



The ARP table(s) in router R1 contain the following entry:

< IP address of  $R2_{R1}$ , MAC address of  $R2_{R1}$ , TTL >



The ARP table in host A contains the following entry:

< IP address of  $R1_A$ , MAC address of  $R1_A$ , TTL >



The ARP table(s) in router R1 contain the following entry:

< IP address of B, MAC address of  $R2_{R1}$ , TTL >



25. Today, a modern encryption scheme should satisfy certain properties. Which one of the following properties are desired?

(2 marks)

☐

The encryption algorithm should be kept secret.



An encryption algorithm should be based on sound mathematics, and it should have been analyzed by competent experts and found to be sound.



If an encryption scheme is correctly implemented and used (i.e., the attacker only has access to the cipher text), then the most effective attack method for an attacker is brute force search.

☐

Efficiency, i.e., how quickly we can compute the encryption and decryption algorithms with a given input text, is the most important property of encryption.



The encryption key(s) should provide enough strength against an attack even if the encryption algorithm is public.

26. Which of the following are valid statements of the symmetric key and public key encryption algorithms that are in use today?

(2 marks)



Symmetric key encryption algorithms are generally faster to compute.



A symmetric key  $K$  of length  $n$  bits can be recovered by exhaustive search in an expected time on the order of  $2^{n-1}$  attack operations. (Each attack operation is testing 1 key.)



Symmetric keys are generally shorter (fewer bits) than public key encryption keys to provide a similar strength (i.e., resistance against attack).



Public key encryption algorithms are generally easier to implement in hardware.



In a public key encryption system it must be computationally infeasible to derive the private key from the public key.

27. You are using a media player which has a playout buffer size of  $B_{\text{Playout}} = 8 \text{ MB}$ . The buffer is initially empty. The time when you press "play" for a video is  $t_0$ . It takes 4 seconds to fill the buffer  $B_{\text{Playout}}$  to its mid-point, i.e., 4 MB of data. At that point ( $t_0 + 4 \text{ secs}$ ) the media player starts to play the video. The video has a size of 12 MB. The data continues to arrive after ( $t_0 + 4 \text{ secs}$ ) from the server at a constant rate of 8 Mb/s and the player plays (decodes) the media at a rate of 4 Mb/s until the video ends. Which of the following statements are **TRUE**? (Times are measured relative to  $t_0$ ).

(2 marks)

$1 \text{ MB/s} \rightarrow 0.5 \text{ MB/s}$   $4 \text{ MB}$   $4 \text{ s}$   
 $2 \text{ MB}$

☐

The video will play normally for the whole duration of the video and will end at  $t_0 + 28$  seconds.

$4 \text{ s interval} \rightarrow \text{consume } 2 \text{ MB, add } 4 \text{ s}$   
 $= 6 \quad 4 \text{ s interval}$

☒

The  $B_{\text{Playout}}$  buffer will overflow at  $t_0 + 12$  seconds. (And the video may stall/stop.)

$\rightarrow 8$

☐

The  $B_{\text{Playout}}$  buffer will overflow at  $t_0 + 8$  seconds. (And the video may stall/stop.)

☐

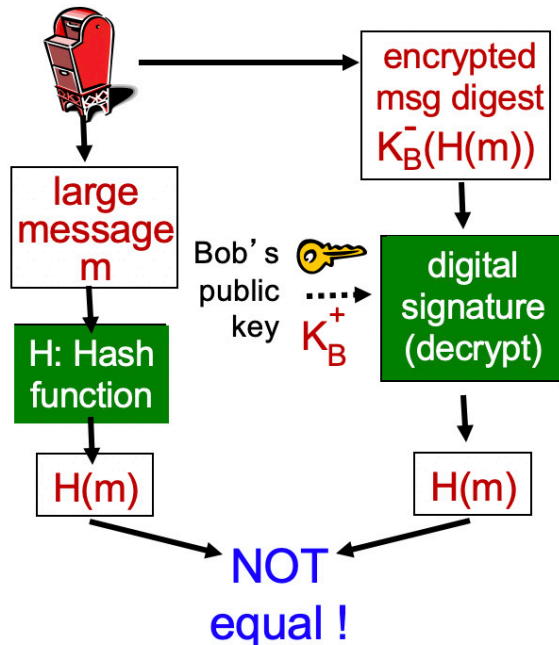
The  $B_{\text{Playout}}$  buffer will underflow at  $t_0 + 12$  seconds. (And the video may stall/stop.)

☐

The server will have delivered all the data of the video to the client at  $t_0 + 12$  seconds.

28. The workflow in the figure below shows the process at the receiver side (Alice) of verifying the digital signature of a message  $m$  that was sent by Bob and where he digitally signed the message digest  $H(m)$ .

The result, shown in blue at the bottom, shows that the message digests  $H(m)$  are not equal. Which of the statement(s) is/are **TRUE**?



(2 marks)

- ☐ We definitely know that Bob did not sign the message digest.
- ☐ We definitely know that the message  $m$  was tampered with.
- ☒ We only know that either Bob did not sign the message digest, or  $m$  was tampered with, or both.
- ☐ We definitely know that either Bob did not sign the message digest or that the message  $m$  was tampered with, but not both.
- ☒ It could be possible that we do not have Bob's correct public key. This could happen if, for example, Bob was not careful in distributing his public key and if there is no certificate so that we could verify his public key.

## Fill-in-the-Blanks

In this section, you are typically required to calculate some numerical values and put them in the blanks as your final answers.

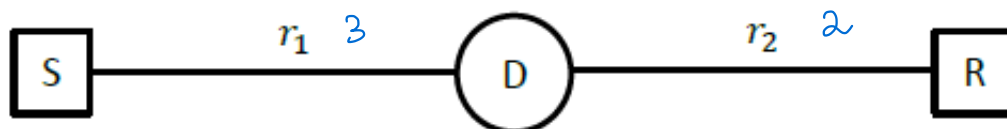
If your answer matches the predefined correct answer value, you will get full marks.

For some questions, a Response Rationale box is provided for you to input more derivation details. Although filling this box is optional, the contents of this box will be used by graders to possibly provide partial marks through manually evaluation, if we identify that your main logic of solving the question is correct, but the final answer is wrong due to careless calculation mistakes.

### 29. Fill in the blanks

(2 marks)

A device (D) is used to connect a sender (S) and a receiver (R). Transmission rates of the links between sender and the device and between the device and receiver are  $r_1 = 3$  Mbps and  $r_2 = 2$  Mbps, respectively.



1. Suppose the sender sends only one packet to the receiver, in this process, the (average) throughput that can be achieved is 1 Mbps. 2.5
2. Suppose the sender sends many small packets continuously to the receiver, and under a fluid model, the (instantaneous) throughput that can be achieved is 2 Mbps.

Enter the correct answer below.

1

Please enter a number for this text box.

2

Please enter a number for this text box.



### Response Rationale/Workings

*Please provide rationale or workings for your answer.*

Font



Size

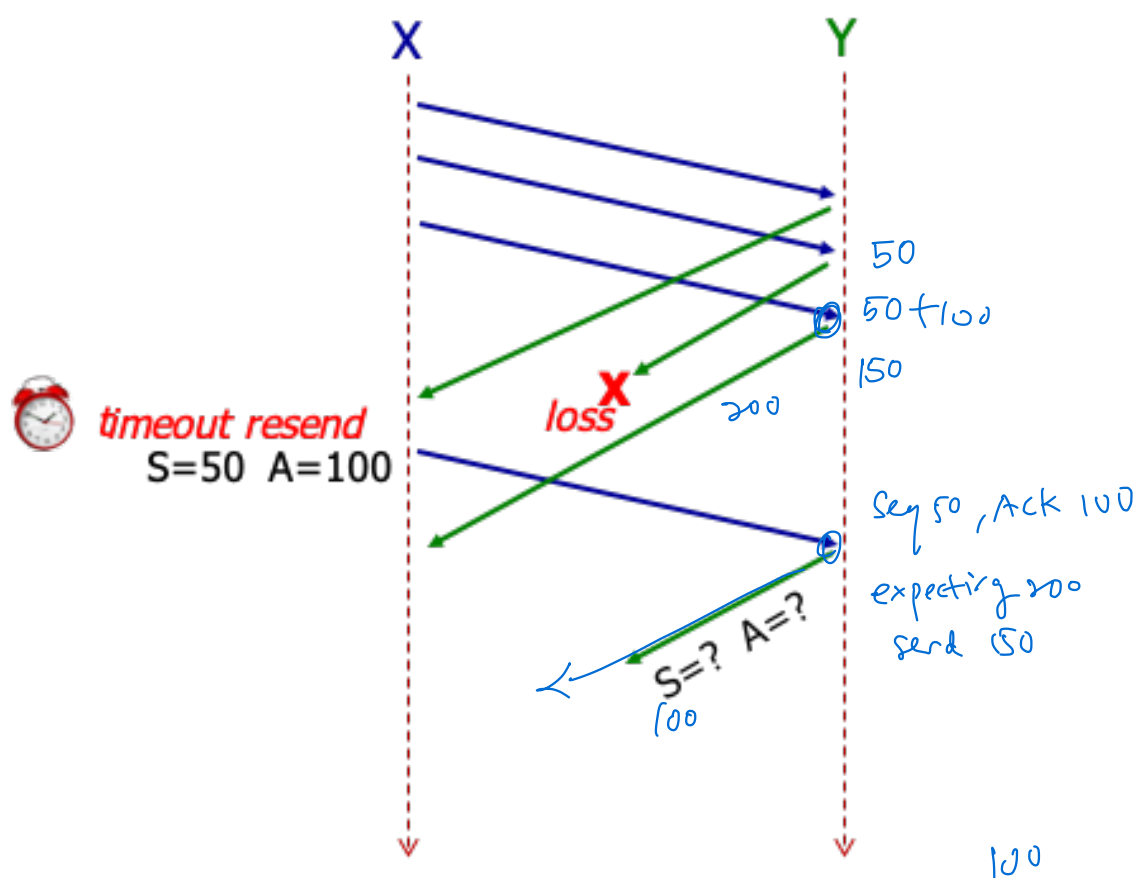


Source

## 30. Fill in the blanks

(2 marks)

The following diagram shows two hosts X and Y communicating over an ongoing TCP connection. X and Y are sending data to each other and each TCP segment contains 100 bytes of application data. The 2nd segment send by Y is lost. The 4th segment sent by X is a retransmission triggered by a time-out event. There is no time-out event at host Y. This retransmission segment send by X has sequence number 50 and ACK number 100. Assume that no other the segments in the diagram are retransmitted packets, none of the segments are corrupted and receiver buffers out-of-order packets for eventual delivery to application.



In the last TCP segment send by Y, the sequence number  $S = \underline{1}$  and the acknowledgement number  $A = \underline{2}$ . 150

Enter the correct answer below.

1

Please enter a number for this text box.

2

Please enter a number for this text box.



## Response Rationale/Workings

*Please provide rationale or workings for your answer.*

Font



Size



Source



## 31. Fill in the blanks

(2 marks)

Host A has 6 segments ready to be sent to Host B. Go-Back-N protocol is used for transmission and sender's window size is 3. Assume that transmission delay of each segment is negligible, timeout value is larger than 3 RTTs and no segment is corrupted during transmission. However, the second ACK and the fifth data segment are lost. In the end, all 6 segments are correctly received by Host B.

Host A has sent   1   segments in total.

Host B has sent   2   ACKs in total.

*A → B*

Enter the correct answer below.

*0 1 2 3 4 2 3 4  
↑ ↑ ↑ ↑ ↑  
· · · · ·*

1

Please enter a number for this text box.

2

Please enter a number for this text box.



### Response Rationale/Workings

*Please provide rationale or workings for your answer.*

Font

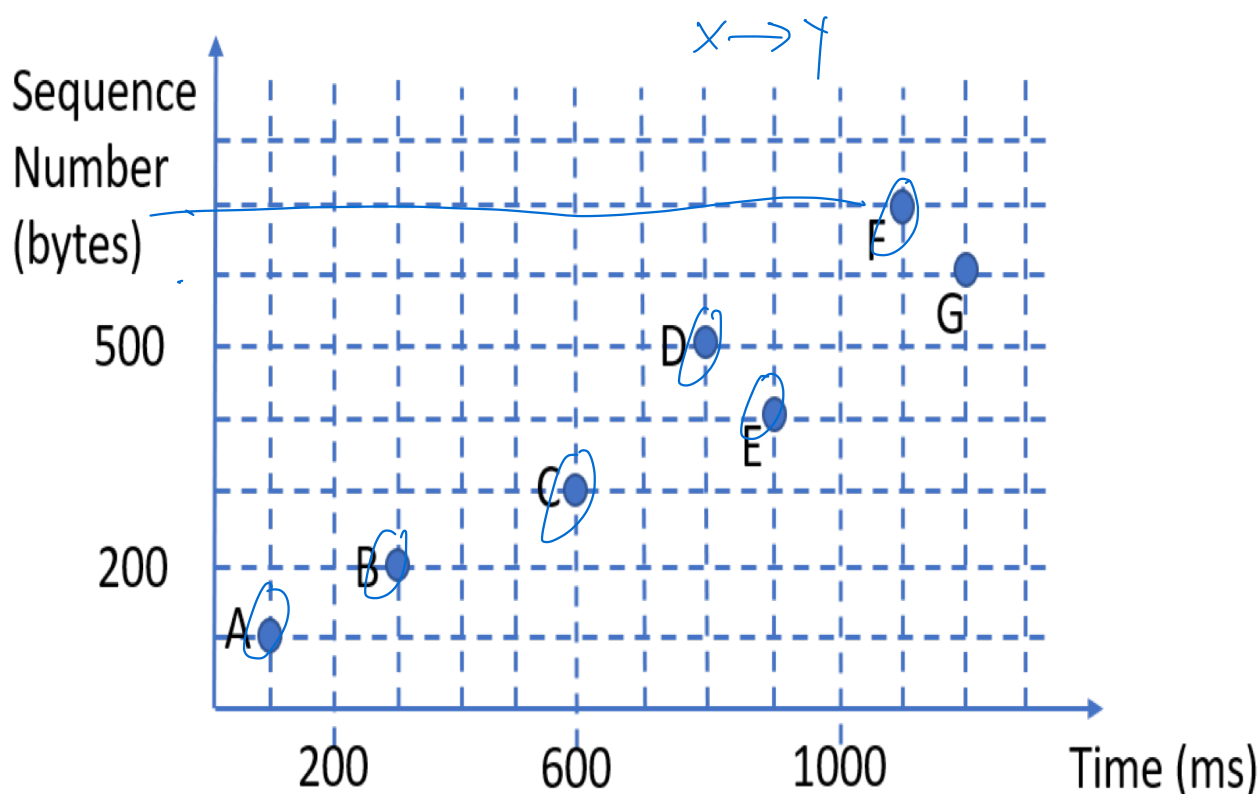
Size

Source

## 32. Fill in the blanks

(2 marks)

The following graph shows a sequence of TCP segments sent from host X to host Y. Each dot represents a TCP segment, plotting its sequence number versus the time it is received by Y. Each segment carries exactly 100 bytes of payload. The segments labeled with A and F are the first and last segments sent by X, respectively. Assume that no segment is corrupted during transmission and Y buffers out-of-order segments for eventual delivery to the application.



Host Y has sent 1 ACKs in total.

The ACK number in the last ACK segment sent by Y is 2.

Enter the correct answer below.

1  Please enter a number for this text box.

2  Please enter a number for this text box.



### Response Rationale/Workings

*Please provide rationale or workings for your answer.*

Font



Size



Source

## 33. Fill in the blanks

(2 marks)

We have designed our own encryption scheme. Assume we are using  $n=2$  substitution ciphers  $M_1$  and  $M_2$  in a continuous cyclic pattern.

The cyclic pattern is:  $M_1, M_2, M_1, M_2, M_1, M_2, \dots$

For both patterns we use a Caesar's Cipher:

$M_1 = \text{'yzabcdefghijklmnopqrstuvwx'}$

$M_2 = \text{'wxyzabcdefghijklmnopqrstuv'}$  

The shift number of  $M_2$  is   1   (enter only the shift number, without the direction).

Apply the above encryption scheme to the plaintext "moon", which results in the ciphertext:   2   .

Enter the correct answer below.

1

Please enter a number for this text box.

2



### Response Rationale/Workings

*Please provide rationale or workings for your answer.*

Font

Size







Source

### 34. Fill in the blanks

(2 marks)

We are designing an Analog-to-Digital Converter (ADC). On the analog side we expect our signal amplitude to be in the range from 0 to 0.875 Volt (V). On the digital side we represent the amplitude with a 3-bit value, i.e., 0V = 000 and 0.875V = 111.

0.125

The digital side, the ADC cannot accurately represent all of the possible input analog amplitude values. What is the maximum, absolute (i.e., either plus or minus) quantization error, in Volts, that this ADC will have? Maximum quantization error (in Volts): 1

Enter the correct answer below.

1

Please enter a number for this text box.



#### Response Rationale/Workings

*Please provide rationale or workings for your answer.*

Font

Size

Source

**Finish Quiz**

**Save For Later**