Student NO: | | | | | | | | | | CS2105

NATIONAL UNIVERSITY OF SINGAPORE

MOCK FINAL ASSESMENT FOR
CS2105 – INTRODUCTION TO COMPUTER NETWORKS

(Semester 1: AY2022/2023)

Time allowed: 120 minutes

INSTRUCTIONS TO CANDIDATES

1. This assessment paper comprises 10 printed pages, including this page.
2. The total maximum score is **25 marks**.
3. Answer all the questions using the knowledge you learned in CS2105.
4. This is an **OPEN BOOK** assessment. You may bring in any printed materials. Calculators are also allowed, but no laptops or other electronic devices.
5. Each MCQ has one correct answer. Answer each MCQ by shading the letter corresponding to the correct answer on the **OAS form** provided. Shade and write down your **student number** on the OAS form too. You must use a **2B** pencil to shade on the OAS form, or the grading machine might not be able to register your shading.
6. **Submit** both the OAS form and the question paper at the end of the assessment.
7. Leave your student card on the desk throughout this assessment.
8. Do **NOT** look at the questions until you are told to do so.
9. Fill in your student number clearly on all pages.
10. Please write your Student Number only. Do not write your name.
11. This is mock paper, and is **not indicative** of the mark distribution and difficulty of the actual assessment.

This portion is for examiner's use only

This page is intentionally left blank.

Part I

Multiple Choice Questions (6 marks)

For each of the questions below, select the most appropriate option. Each question is worth 1 Mark.

1. Ethernet provides an unreliable service and _____.

   A. CRC is not used for error checking
   B. Ethernet sends a negative acknowledgement to the sender to indicate packet loss
   C. Ethernet drops a frame that fails error checking without retransmission
   D. Ethernet does not function correctly when bit errors in frames are detected
   E. Applications that require reliable delivery cannot run over Ethernet

2. Which of the following statements about 2-dimensional parity bits is FALSE?

   A. It can detect any one-bit error.
   B. It can correct any one-bit error.
   C. It can detect any two-bit error.
   D. It can correct any two-bit error.
   E. It may not be able to detect a four-bit error.

3. Which of the following statements about IP header is TRUE?

   A. The source and destination port numbers in the IP header determine which application on the receiving host will process the datagram.
   B. The TTL field in the IP header determines the time period within which the source IP address is valid.
   C. The 16-bit identifier field in the IP header is not changed during IP fragmentation.
   D. The checksum field in the IP header allows the receiver to check if the IP header or payload is corrupted.
   E. The protocol field in the IP header determines which link layer protocol should be used to transmit the datagram.

4. A Web server supports both HTTP/1.0 and HTTP/1.1. So far 100 clients have downloaded a web page from the server, which contains 1 HTML file and 2 images. Half of the clients run HTTP/1.0 and the other half run HTTP/1.1.

   How many sockets has the Web server ever created since it starts running?

   A. 201
   B. 200
   C. 100
   D. 101
   E. None of the above

5. In many VoIP applications, the audio data is sent in packets that contain 20 milliseconds worth of audio data. This is only about 160 bytes, i.e., much less than the MTU of Ethernet. The reasons for using 20 ms are as follows:

   i. 20 millisecond is the average word length of a human being.
   ii. The packet length is not important and we could just as well choose another value and it would not make any difference.
   iii. The data length (in milliseconds) directly and proportionally adds to the end-to-end delay. Therefore, for interactive VoIP applications we do want to use fairly short packets.
   iv. 20 ms only works well for the English language.
   v. Packets that are much shorter than 20 ms would create a relatively high overhead (the header size in comparison to the payload data size) and also a high number of packets would be generated. Therefore, 20 ms is a good compromise.

   A. (i) only.
   B. (i) and (ii) only.
   C. (i), (ii) and (iii) only.
   D. (iii) and (v) only.
   F. (i), (ii) and (iv) only.

6. Each IP node (host, router) has an ARP table, which stores the mappings of IP to MAC addresses of the same subnet in the following format:

   < IP address; MAC address; TTL >

   What is the function of the TTL (time-to-live) field?

   Assume this is the ARP table on host A and the entry shown above is for host B

   A. The TTL value is a counter value that counts how many times host A has sent frames to host B.
   B. The TTL value stores a counter that counts from certain value (say 120 seconds) down to zero. If the value reaches zero then the entry is deleted from the ARP table. This is to keep the table small and only remember IP/MAC pairs of nodes with which host A had recent communications.
   C. The TTL value is a counter that stores the elapsed time since the host A was last turned on.
   D. The TTL value is a counter that counts how many frames have been sent from host A to host B.
   E. The TTL value stores the average round-trip time between hosts A and B.

Part 2

Multiple Choice Questions (8 Marks)

For each of the questions below, select the most appropriate option. Each question is worth 2 Marks.

96+16 = 112

128 64 32 16 8 4 2 1
0 1 1 0

8 8

7. Which of the following IP addresses belong to the subnet 137.132.96/20?

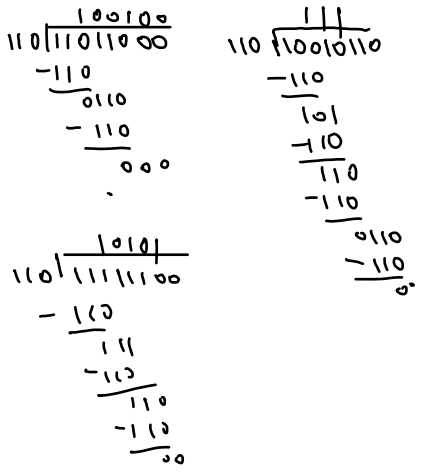
   ✓ i. 137.132.96.96
   ✓ ii. 137.132.104.104
   ✗ iii. 137.132.112.112
   ✗ iv. 137.132.120.120

   A. (i) only.
   B. (i) and (ii) only.
   C. (i), (ii) and (iii) only.
   D. (iii) and (iv) only.
   E. (i), (ii), (iii) and (iv) only.

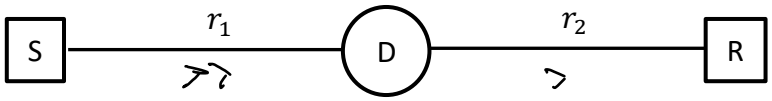
8. Two hosts are communicating using CRC as an error detection scheme, with a generator of 110. Every byte sent consists of six bits of data and two bits of the CRC value. Suppose the following four bytes are received. Which bytes would pass the CRC test and considered as containing no bit error?

   ✓ i. 11011000
   ✗ ii. 11011101
   ✓ iii. 10010110
   ✓ iv. 11111100

   A. (i) and (ii) only.
   B. (i) and (iv) only.
   C. (i), (iii) and (iv) only.
   D. (iii) and (iv) only.
   E. (i), (ii) and (iii) only.



9. 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 and r_2 ($r_1 > r_2$) respectively. Ignore other types of delay, what is the end-to-end delay to send a packet of length L?



A. $\frac{Lr_1r_2}{r_1+r_2}$, if this device, D, is a store-and-forward packet switch.

B. $\frac{L}{2r_1}+\frac{L}{2r_2}$, if this device, D, is a store-and-forward packet switch.

C. $\frac{L(r_1+r_2)}{r_1r_2}$, if this device, D, acts on individual bits and repeats every bit to receiver, R, once receives it from sender, S.

D. $\frac{L}{r_1}+\frac{1}{r_2}$, if this device, D, acts on individual bits and repeats every bit to receiver, R, once receives it from sender, S.

E. $\frac{1}{r_1}+\frac{L}{r_2}$, if this device, D, acts on individual bits and repeats every bit to receiver, R, once receives it from sender, S.

$\frac{1}{r_1}+\frac{1}{r_2}+\frac{L-1}{r_2} = \frac{1}{r_1}+\frac{L}{r_2}$.

10. A subnet contains two hosts with IP addresses 137.132.80.16 and 137.132.67.94 respectively. Which of the following is/are possible address block assigned to the subnet?

i. 137.132.64.0/18

ii. 137.132.64.0/19

iii. 137.132.64.0/20

iv. 137.132.0.0/17

80.16 → 128 64 32 16 → 0 1 0 1

67 → 128 64 32 16 8 4 2 1 → 0 1 0 0 0 0 1 1

A. (i) only.

B. (i) and (ii) only.

C. (i), (ii) and (iii) only.

D. (iii) and (iv) only.

E. (i), (ii) and (iv) only.

Part 3

Short Answer Questions (11 Marks)

For each of the question below, kindly enter your answers in the space provided. Each question is worth 1 Mark.

11. [2 mark] Two hosts *A* and *B* are 2,000 km apart and are connected directly using a link with propagation delay of 800 bit times and propagation speed of 2.5 * 10^8 m/s. *A* is sending a sequence of packets, each is 100 bytes in size, to *B*.

(a) How long does it take for *B* to receive a packet?

0.008s.

16 ms

delay = $\frac{2000 \times 10^3}{2.5 \times 10^8}$ = 0.008 s.

(b) *A* is using a sliding window protocol to communicate with *B*. What is the minimum window size *A* should use for the link to be fully utilized?

3

12. [3 mark] To preserve message confidentiality and integrity, the following information is contained in a secured message sent from Alice to Bob.

- Encrypted hash of the message
- Encrypted message
- Encrypted session key

K_B^+ K_B^-

(a) Briefly describe the purpose of "Encrypted hash of the message"and the key used in generating that

~~It is to enable the detection of alteration in the message, hence conserving message integrity~~ Alice's private key should be used to prove her identity.

(b) Briefly describe the purpose of "Encrypted message"and the key used in generating that

It is to preserve confidentiality where only Alice and Bob are able to understand the content of the message. A symmetric key known only by Bob and Alice should be generating the encryption. ('i.e. the session key).

(c) Briefly describe the purpose of "Encrypted session key"and the key used in generating that

The encryption of session key provides confidentiality since it ensures that only Alice and Bob knows the session key. Bob's public key should be used to encrypt them..

13. [1 mark] Each network interface card has a MAC address. Why not simply use this MAC address for routing of packets on the Internet?

The MAC address does not allow a narrowing of the address range, hence have to search through all devices to send to the correct MAC address, which makes it inefficient. often no hierarchical addressing

14. [1 mark] In a VoIP application (or any media streaming application that requires a continuous, uninterrupted media data playout), then at the receiver side two types of data losses may occur_____ loss and _____ loss.

Network, Delay.

15. [1 mark] Public key cryptography uses both public and private keys. Let Alice's public key be K_A^+ and private key be K_A^-, Bob's public key be K_B^+ and private key be K_B^-. Alice sends a message m to Bob. Describe how they can ensure message confidentiality and integrity using only these 4 keys

Message integrity can be maintained by hashing the message itself, and then encrypting the hash with K_A^-.
The intruder cannot temper with m, since modifying m will cause the hash to be different and Bob can detect this.
Message Confidentiality can be maintained by using a symmetric key K_s to encrypt the concatenation of the message m and $K_A^-(H(m))$. And concatenating that with the encryption of K_s with K_B^+, $K_B^+(K_s)$.

Since only Bob has K_B^-, intruder cannot decrypt $K_B^+(K_s)$ to get K_s.
And without K_s, intruder cannot decrypt m.

Cannot use K_s.

$K_A^-(m)$ → digital signature of Alice

$m \oplus K_A^-(m) \rightarrow K_B^+(m \oplus K_A^-(m))$

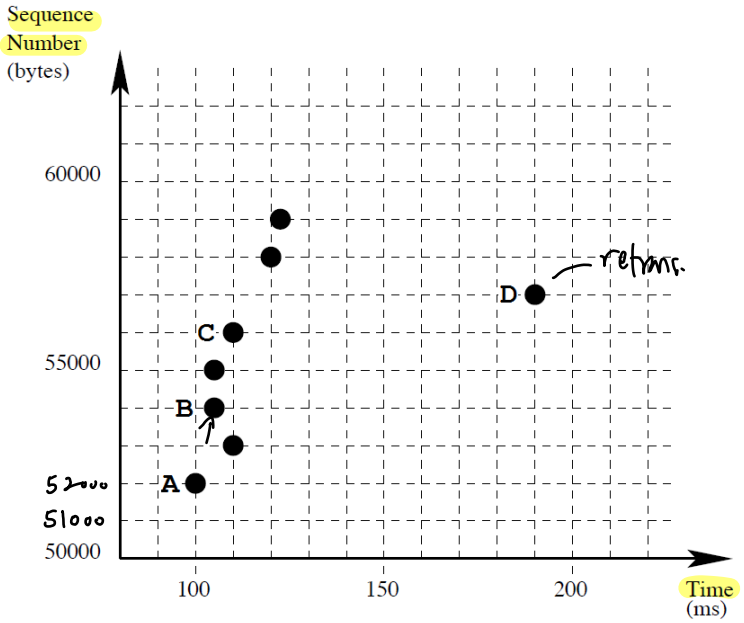
decrypt with K_B^- to get $m \oplus K_A^-(m)$.

and K_A^+ to get m'.

if $m = m'$, message integrity is preserved

message is encrypted → confidentiality is preserved

16. [3 mark] The following graph shows the time sequence graph for a TCP connection between host X and host Y. Each dot represents a TCP segment received at host Y, plotting the sequence number of the segment, versus the time at which it is received. A set of dots stacked above each other represents a series of packets that are received back-to-back by the receiver. The packet labelled with A is the first data packet sent by X. The packet labelled with D is a re-transmitted packet.



(a) How many bytes of data are there in each TCP segment?

1000

next seq. no

(b) Suppose an acknowledgment is sent by Y at time 105ms, after receiving the packet labelled with B. What should be the acknowledgement number in this feedback packet?

52000 A 53000 B 53000

53000

(c) Dose Y buffer out-of-order packets or discard them? Justify your answer.

It buffers. Even though packet #53000 is received after #54000, #54000 is not discarded and retransmitted even after D is transmitted.

=== End of Paper ===

ANSWERS

Part 1

1 C

2 D

3 C

4 A

5 D

6 B

Part 2

7 B

8 C

9 E

10 E

Part 3

11

$d_{prop} = \frac{2\times10^6 m}{2.5\times10^8 m\ per\ sec} = 8ms = 800\ bit\ time$

$1\ bit\ time = 0.01\ ms$

(a) $d = d_{trans} + d_{prop} = 800\ bit\ time + 800\ bit\ time =$ **16 ms**

(b)

$L = 800b$

$R = \frac{1}{bit\ time} = \frac{1}{0.01\ ms} = 100\ b\ per\ ms$

$\frac{L}{R} = \frac{800}{100} = 8\ ms$

$RTT = 2 \times d_{prop} = 2 \times 8 = 16\ ms$

$$U = \frac{w \times \frac{L}{R}}{RTT + \frac{L}{R}}$$

$$1 = \frac{w \times 8}{16 + 8}$$

$w =$ **3**

12 (Multiple possible answers. Below is one example)

(a) ***Encrypted hash of the message***: **digital signature of Alice used to prove her identity to Bob. Alice's private key is used.**

(b) ***Encrypted message***: **message encrypted with the session key to ensure confidentiality of the message. Session key is a symmetric key.**

(c) ***Encrypted session key***: **session key encrypted with Bob's public key. The purpose is to share the session key with Bob.**

13

An IP address logically comprises two parts: network prefix and host ID. This is designed to facilitate routing: routers check prefix and deliver a packet to an aggregated destination network. If MAC address is used instead, hierarchical routing cannot be achieved. For example, MAC address is burnt in ROM and usually cannot be changed. When people carry their laptops around the world, devices in a subnet won't have common prefix in MAC addresses. This makes routing difficult as routers have to remember routing for every single MAC address.

14

Network Loss and Delay Loss

15

1. **Alice encrypts m with her private key to create digital signature $K_A^-(m)$.**
2. **Alice concatenates message with digital signature $m \oplus K_A^-(m)$, and encrypt the extended message with Bob's public key: $K_B^+(m \oplus K_A^-(m))$.**
3. **Alice sends $K_B^+(m \oplus K_A^-(m))$ to Bob.**
4. **Bob decrypts the received message using his private key: $K_B^-\left(K_B^+(m \oplus K_A^-(m))\right) = m \oplus K_A^-(m)$.**
5. **Bob then uses Alice's public key to derive message from digital signature: $K_A^+(K_A^-(m)) = m'$**
6. **If $m = m'$, message integrity is preserved.**
7. **Because message is encrypted during transmission, message confidentiality is preserved.**

16

(a) **1,000**

(b) **53,000**

(c)

Y buffers out-of-order packets. The packet B is an out-of-order packet. However, it is not retransmitted even if a later packet D is already retransmitted. That implies B is buffered and already acknowledged.