NATIONAL UNIVERSITY OF SINGAPORE

SCHOOL OF COMPUTING
FINAL EXAMINATION FOR
Semester 2 AY2013/2014

CS2105 Introduction to Computer Networks

April 2014 Time Allowed 2 hours

INSTRUCTIONS TO CANDIDATES

1. This assessment paper contains 13 questions and comprises 12 printed pages, including this page.
2. The last two pages of this paper is the answer sheet.
3. Write all your answers **on the answer sheet**. Detach the answer sheet for submission at the end of the assessment.
4. The total marks for this assessment paper is 50. Answer **ALL** questions.
5. This is an **CLOSE BOOK** examination, but you are allowed to bring in **one sheet of single-layer, double-sided, A4 size paper** with notes.

Part I
Multiple Choice Questions (18 points)

For each of the questions below, select the most appropriate answer and **write your answer in the corresponding answer box on the answer sheet**. Each question is worth 2 points.

If multiple answers are equally appropriate, pick one and write the chosen answer in the answer box. Do NOT write more than one answers in the answer box.

If none of the answers are appropriate, write `X` in the answer box.

1. A Web server acts as an application gateway to CGI scripts. The server just receives an HTTP request. The first three lines of the request are shown below.

```
POST /news.pl HTTP/1.1
Content-Length: 310
Content-Type: application/x-www-form-urlencoded
```

Which of the following is TRUE?

A. The request does not contain a query string.

B. The environment variable `REQUEST_METHOD` should be set to `news.pl`

C. The total size of the HTTP request (including both header and body) is 310 bytes.

D. The application named `x-www-form-urlencoded` will be invoked to decode the URL.

E. The server must close the TCP connection immediately after sending the response.

Write X in the answer box if none of the above is TRUE.

Solution: X. The query string is part of the HTTP request body; the REQUEST_METHOD is POST; content length does not include header; news.pl will be invoked instead; and HTTP/1.1 is persistent.

2. Knowing that you have taken CS2105, a friend comes to you for help with his laptop. He says that he cannot access the Web page hosted at `www.example.com`. Using the tools you have learned from CS2105, you run the following commands on his laptop to troubleshoot what could be the reason.

Which of the following is NOT the correct use of the corresponding tool?

A. You run `telnet` to check if `www.example.com` is listening on port 80.

B. You run `traceroute` to check if there is a route from the laptop to `www.example.com`.

C. You run `dig` to check if his DNS server is able to resolve the IP address of host name `www.example.com`.

D. You run `ping` to check if you can establish a TCP connection to `www.example.com`.

E. You run `curl` to check if `www.example.com` is responding to a HTTP request correctly.

Write X in the answer box if every choice above is correct.

Solution: D. ping checks if a host is alive using ICMP.

3. Consider a Java implementation of the stop-and-wait (RDT 3.0) protocol, using classes and methods similar to your Assignment 2. A student has implemented the sender correctly according to the state diagram of the protocol. In the receiver, the student implemented the following:

```
byte[] recv() throws IOException, ClassNotFoundException
{
    DataPacket p = udt.recv();
    while (p.isCorrupted || p.seq != seq)
        p = udt.recv();
    udt.send(new AckPacket(p.seq));
    seq = 1 - seq;
    return deliverData(p);
 }
```

Here, `seq` is the expected sequence number (either 0 or 1) at the receiver, and `deliverData` is a method that extracts and returns the payload from packet `p`.

The protocol is used over a channel that may lose or corrupt a packet, but always delivers packets in the order that they are sent.

We say that the receiver *waits forever*, if it is blocked at the call `udt.recv()`, waiting to receive a packet that will never be sent. We say that the sender *loops forever*, if it repeatedly retransmits the same packet over and over again.

Which of the following statement CORRECTLY describes the behavior of the protocol implemented above?

A. A single corrupted data packet is sufficient to cause the sender to loop forever.

B. A single corrupted data packet is sufficient to cause the receiver to wait forever.

C. A single loss ACK packet is sufficient to cause the sender to loop forever.

D. A single loss ACK packet is sufficient to cause the receiver to wait forever.

E. A single premature timeout is sufficient to cause the sender to loop forever.

Write X in the answer box if none of the description above is correct.

Solution: C. A loss ACK would cause the sender to send a duplicate packet to the receiver after timeout. Since the receiver does not send an ACK on duplicate packet, the sender keeps timing out and loops forever. Note: if a packet is corrupted, the sender would time out and resend the packet (A and B are wrong). A premature timeout would cause the sender to send a duplicate packet as well, but eventually ACK is received by the sender, so the sender won't loop foever.

4. Which of the following IP addresses belongs 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).

   Write X in the answer box if none of the choices above is correct.

   Solution: B. The IP addresses in the subnet range from 137.132.96.0 to 137.132.111.255.

5. Which of the following statement 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.

   Write X in the answer box if every statement above is correct.

   Solution: D. 2D parity cannot correct a two-bit error, if the error bits are in the same row or the same column.

6. 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

Write X in the answer box if none of the choices above is correct.

Solution: C. A byte would pass the CRC test if it can be divisible by `110`. (i) 110 110 00, (iii) 10010 110 and (iv) 1111110 0 would pass. (ii) 110 11101 is not divisible by 110 (a remainder of 11).

7. Which of the following protocols does NOT run on routers?

   A. IP

   B. UDP

   C. RIP

   D. ICMP

   E. ARP

Solution: B. UDP is in the transport layer and runs only in the end host.

Write X in the answer box if every protocol above runs on routers.

8. A and B are communicating over a link with a sliding window protocol. Which of the following condition would reduce the utilization of a link?

   A. increasing the transmission rate

   B. increasing the size of the packet

   C. increasing the value of retransmission timeout

   D. increasing the size of the sending window

   E. reducing the distance between A and B

Solution: A or C. The utilization U for a sliding window protocol can be expressed as

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

From the formula, increasing R would reduce U; increasing L or N would increase U; reducing RTT would increase U as well. Increasing the timeout value would reduce utilization, since when a packet is loss, the sender spend more time idling waiting for ACK.

Write X in the answer box if none of the condition above would reduce the link utilization.

9. A simple network uses 6-bit network-layer addresses, consists of three subnets connected to a router. The router has three interfaces, labeled A, B, and C.

   - All hosts with addresses ranging from `000000` to `001111` are connected to Interface A.
   - All hosts with addresses ranging from `010000` to `011111` are connected to Interface B.
   - All other hosts are connected to Interface C.

   The router uses longest prefix matching to forward packets. The forwarding table is represented as a sequence of tuples (x, Y), which means a packet with destination address prefix of x will be forwarded via interface Y.

   Which of the following is NOT a correct forwarding table in this router?

   A. (`0`, A) (`01`, B) (otherwise, C)
   B. (`00`, A) (`0`, B) (otherwise, C)
   C. (`000`, A) (`001`, A) (`1`, C) (otherwise, B)
   D. (`00`, A) (`1`, C) (otherwise, B)
   E. (`0`, A) (`010`, B) (`011`, B) (otherwise, C)

   Write X in the answer box if every table above is correct.

   Solution: X. Every forwarding table above is valid.

Part II

Short Questions (34 points)

Answer all questions in the space provided on the answer sheet. Be succinct and write neatly.

10. (7 points) A node x is part of a network running distance vector routing protocol. x has three entries in its routing table:

Destination	Cost	Next Hop
w	4	w
y	α	z
z	β	w

α and β are two unknown values (unknown to you, but not to x). Assume that the distance vector routing protocol has converged and the minimum cost path from x to every other node has been found. We denote $c(x, y)$ as the link cost between x and y, and $d_x(y)$ as the cost of the minimum cost path from x to y. The link cost is a positive integer.

We know that $c(x, w)$ is 4, and $c(x, z)$ is 10.

Solution: I received many questions about this. Here is the clarification. No, positive integer does not include 0. Second, note that x gets to z through w, and x gets to y through z (instead of w as many of you would have expected). This can only happen if the costs for x to get to y through z and through w are equal.

(a) (2 points) What is the minimum possible value for α?

Solution: $\alpha \geq 11$, since $d_z(y) \geq 1$, $c(x, z) = 10$, and $\alpha = d_x(y) = c(x, z) + d_z(y)$.

(b) (2 points) What is the maximum possible value for $d_w(z)$?

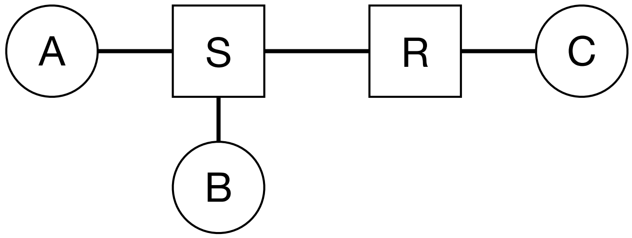
Solution: $d_w(z) \leq 6$. Since $d_x(z) \leq c(x, z)$ (otherwise x would get to z directly instead of going through w) and therefore $c(x, w) + d_w(z) \leq 10$.

Suppose that poison reverse is used, and the link cost for $c(x, w)$ has reduced from 4 to 3. Node x is the first that detects this change and it sends its updated distance vector to its neighbors, w and z.

(c) (3 points) What is the distance vector that x sends to z? Express your answer in terms of variable α and β if necessary.

Solution: $w : 3$, $y : \infty$, $z : \beta - 1$.
Many of you missed out the fact that poison reverse is used, and so the x lies to z about the path to y. Some of you worked out that β is 10. Your answer is also considered correct if you said 9 instead of β-1.

11. (8 points) The diagram below shows a small network with five entities: hosts A and B are connected to a router R through a switch S. Host C connects to R directly. There is no other host, switch, or router in the network.



Solution: This is meant as an easy question, but surprisingly many of you got it wrong. I correct some common misconceptions here: (i) A switch is a link-level device to interconnect between hosts. A switch interface does not have a MAC address, nor does it have an IP address. (ii) An IP address is associated with a network interface. Thus, R has two IP addresses. (iii) At the link layer, C only communicates with R, and A only communicates with B and R. Therefore, the ARP table of C does not contain entries for A and B; ARP table of A does not contain entry for C.

(a) (2 points) What is the maximum number of entries that could be in the switching table of S? Which entities do these entries correspond to?

Solution: 3. A, B, and R.

(b) (2 points) What is the maximum number of entries that could be in the ARP table of A? Which entities do these entries correspond to?

Solution: 2. B and R.

(c) (2 points) What is the maximum number of entries that could be in the ARP table of C? Which entities do these entries correspond to?

Solution: 1. R.

(d) (2 points) How many IP addresses are used in this network? Which entities do these addresses belong to?

Solution: 5. 2 for R, one each for A, B, and C.

12. (8 points) Alice would like to send a message m to Bob over an insecure channel, where a malicious user Trudy can copy and delete any message exchanged between Alice and Bob. Furthermore, Trudy can also insert a message into this channel.

Bob and Alice wants to design a protocol such that the following two properties hold: (I) Bob can ensure that m originated from Alice and not Trudy; and (II) Bob can detect if m is a replay of an earlier message from Alice. Bob and Alice, however, do not care if Trudy eavesdrop on m or modify m.

The notations used to describe the protocol are: K_A^- and K_B^- are the private keys of Alice and Bob respectively; K_A^+ and K_B^+ are the public keys of Alice and Bob respectively; K_s is a shared symmetric key; s is the shared secret; H is a cryptographic hash function; $+$ is the concatenation operator.

You can assume that H is known to everyone; CA can be trusted; K_s and s change for every message exchanged.

For each of the following protocols, indicate if it can ensure Property (I) only, Property (II) only, or both properties. If a property cannot be satisfied, explain.

(a) (2 points) Alice sends $K_A^-(m)$ to Bob.

> **Solution:** Property (I) only. Trudy could buffer $K_A^-(m)$ and replay this message to Bob.

(b) (2 points) Bob sends $K_B^-(K_s)$ to Alice; Alice sends $K_s(m)$ to Bob.

> **Solution:** Neither. Bob cannot be sure that the message m he receives come from Trudy: Trudy could get K_s using Bob's public key. Trudy can then delete Alice's $K_s(m)$ and insert her own $K_s(m')$. Bob cannot verify if m' is from Trudy or Alice.
>
> Many of you think that Property (II) is satisfied, because Bob changes K_s after every message it receives from Alice. But since Trudy knows every K_s, Trudy can do the following: Trudy buffers m from Alice, and intercepts new K_s from Bob. Trudy then constructs $K_s(m)$, with new K_s, replaying m, and sends it to Bob.
>
> To get full marks, you need to explain how Trudy replays m as above. If you simply says Trudy resend $K_s(m)$ to Bob, you will not receive any mark for Property (II).

(c) (2 points) Bob sends $K_A^+(s)$ to Alice. Alice sends $K_B^+(m + s)$ to Bob.

> **Solution:** Property (I) and (II). Only Alice can decode s and Bob can reject any message without correct s. Since s is used once, Bob can detect a replay attack.
>
> (Note: you do not need to explain if a property is satisfied. My explanation here is FYI only)

(d) (2 points) Bob sends $K_A^+(s)$ to Alice. Alice sends m and $H(m + s)$ to Bob.

> **Solution:** Property (I) and (II). Only Alice can decode s and Bob can reject any message without correct s. Since s is used once, Bob can detect a replay attack. Some of you incorrect assume that Trudy knows m and therefore can figure out s. This is

incorrect given the property of cryptographic hash function H. A few of you said that Trudy can search for s using brute force. This is true, but if you make the assumption that Trudy have massive computational power and has plenty of time on her hand, Trudy can break any security protocol!

13. (11 points) Two hosts A and B are communicating over a wireless channel with a signal to noise ratio of 15 and a bandwidth of 100 MHz. The nodes are 300 meters apart. The signal propagation speed over the air is the 3×10^8 m/s.

Answer the following questions. Show your workings.

(a) (2 points) What is the maximum data rate that can be supported by the wireless channel?

Solution: $B \log_2(1 + SNR) = 100 \times \log_2 16 = 400$ Mbps.

(b) (2 points) Suppose that A transmits at 20 MBaud using 64-QAM as the modulation scheme. What is the transmission rate of A in bps?

Solution: Transmission rate is $20{\times}6 = 120$ Mbps. (64-QAM = 6 bits per signal unit).

(c) (3 points) Suppose that A transmits a frame of size 1000 bytes at 100 Mbps, starting at time $t = 0$. At what time will the frame reach B completely? Give your answer in the unit of μs (Note: 1 μs = 1×10^{-6}s).

Solution: $t_{trans} = L/R = \frac{8000}{100\times10^6} = 80\mu s$
$t_{prop} = m/s = \frac{300}{3\times10^8} = 1\mu s$
The frame will completely reach B at $t = 81\mu s$.

(d) (4 points) Suppose that A is using CSMA/CA with RTS/CTS for medium access. Consider the following ideal situation, (i) where no one else is transmitting besides A; (ii) RTS, CTS, and ACK frames have negligible size; (iii) DIFS and SIFS is negligible – i.e., assume no additional waiting time before a node sends out a frame; (iv) A always picks a back-off timer of 10 μs and have a data frame of size 1000 bytes to transmit; and (v) there is no bit error. What is the utilization of the channel if A transmit at 100 Mbps? Give your answer as a ratio of two integers. Draw a timing diagram to explain your answer.

Solution: I accept two answers, depending on the assumption of whether you consider the first frame (no backoff timer) or all other frames (A always wait 10 μs before sending RTS).

RTT = 2 μs, one RTT taken for RTS/CTS, one for transmission and ACK. With backoff timer, the total time is 10 μs + RTT + t_{trans} + RTT = 94 μs. Transmission time is 80 μs Utilization is 80/94 = 40/47.

Without backoff timer, the utilization is 80/84 = 20/21.

One common mistake is the omission of the ACK frame, causing the total time taken to be off by $\frac{1}{2}$RTT.

Some of you just apply the formula $\frac{L/R}{L/R+RTT}$. This is disappointing since it means you are just memorizing the formula instead of understanding what utilization means!

END OF PAPER

This page is intentionally left blank.

Matriculation Number: | | | | | | | | |

Answer Sheet

Write all your answers on this sheet of paper. Submit only this sheet of paper at the end of the examination.

1. ☐ 2. ☐ 3. ☐ 4. ☐ 5. ☐ 6. ☐ 7. ☐ 8. ☐ 9. ☐

10. (a)

. . . .

(b)

. . . .

(c)

Destination	Cost

11. (a)

. . . .

. . . .

(b)

. . . .

. . . .

(c)

. . . .

. . . .

(d)

. . . .

. . . .

12. (a)

(b)

(c)

(d)

13. (a)

(b)

(c)

(d)