Sample Final Exam Solutions
Csci4211: Introduction to Computer Networks
Spring 2018
Prof. Zhi-Li Zhang

Last Name: **First Name:**

Student Id.

Instructions:

1. This is a **open-book** and **open-note** exam.
2. There are **five** questions in total, each of which has several sub-questions. *There are a total of 100 points.* You have **two hours** to answer the questions.
3. Please write down your name and student id. on the top of this page first before you start answering any question. *Answer all questions directly on the exam papers.* If you need additional sheets, please let us know.
4. Partial credit is possible for an answer. Please try to be as concise and make your exam as neat as possible. We *must* be able to read your handwriting in order to be able to grade your exam.
5. Good luck. Enjoy!

---

1. General True/False Questions: (15 points total. approx. 8 minutes)

Please circle your answer to the following **true or false** *questions.*

a. (3 points) **True or False:** A key advantage of a *layered* network architecture is that it hides implementation details and complexity of a lower layer from higher layers.

Ans. **True**

b. (3 points) **True or False:** When your computer joins an IP network and obtains an IP address via DHCP, your computer also learns the IP address of the local DNS server.

Ans. **True**

c. (3 points) If the underlying network establishes a virtual circuit between two end hosts (e.g., via MPLS), then there is no need to use TCP at the transport layer to ensure in-order, reliable data delivery between the two hosts.

Ans. **False**

d. (3 points) **True or False:** To set up a virtual circuit between two end hosts, the two hosts follow a 3-way handshake protocol to establish the end-to-end virtual circuit connection.

Ans. **False**

e. (3 points) **True or False:** When an IP router receives a datagram with the "don't fragment" flag set, but the size of the datagram is larger than the MTU of the link it is to be forwarded, it will simply drop the datagram.

Ans. **True**

2. Network (Intra-Domain) Routing Algorithm (26 points total. Approx. 25 minutes)

Consider the network in Figure 1(a), where the cost of the links are given above the corresponding links. The network uses *distance vector* routing algorithm to compute routing tables. The distance vector/routing tables at routers B, C, and D have been computed for you, as shown in the figure.

a. (10 points) Suppose a new router A is added to the network with a link of cost 1 to router B, as shown in Figure 1(b). Compute the distance vector/routing table for the new router A (show the intermediate steps in your computation). Also, what new entries will routers B, C, D *eventually* add to their distance vector/routing tables after a few round of routing information exchanged among themselves? Write down the updated distance vector/routing tables at routers B, C and D.

Ans.

Using the DV distance computation formula 1 – i.e., the Bellman-Ford Algorithm, we get the following table:

$$D^X(Y,Z) = c(X,Z) + min_w\{D^Z(Y,w)\} \quad (1)$$

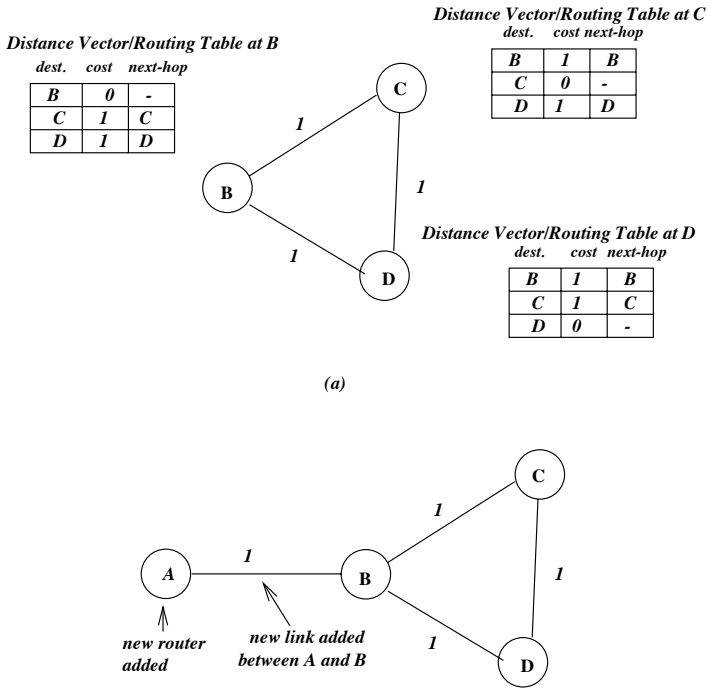


Figure 1: Figure for Question 2.

Destination	Cost	Next-Hop
A	0	-
B	1	B
C	2	B
D	2	B

Then, using the same formula, we get the following additions to the following routers:

Router	Destination	Cost	Next-Hop
B:	A	1	A
C:	A	2	B
D:	A	2	B

b. (5 points) Suppose now the new link between A and B goes down. After the next round of routing information exchange among routers B, C, and D, what will the updated distance vector/routing tables at routers B, C and D look like?

Ans. *Assuming that neither the split horizon hack nor the split horizon hack with poisonous reverse is used*, after the *next* round of routing information exchange among routers B, C and D, the updated distance vector/routing tables (with respect to the destination A) at routers B, C and D look like the following

Router	Destination	Cost	Next-Hop
B:	A	3	C (or D)
C:	A	3	D
D:	A	3	C

If you assume that the split horizon hack or the split horizon hack with poisonous reverse is used, then after the *next* round of routing information is exchanged among routers B, C and D, the updated distance vector/routing tables (with respect to the destination A) at routers B, C and D look like the following:

Router	Destination	Cost	Next-Hop
B:	A	∞	-
C:	A	3	D
D:	A	3	C

c. (5 points) Suppose at this point, router C receives a packet destined to router A. Who will the router C send the packet to? Upon receiving the packet from router C, who will this next router send the packet to?

Ans.

Whether you assume the split horizon hack (or the split horizon hack with poisonous reverse) is used or not, C will send the packet to router *D*, which is the next-hop on the

shortest path to A, according to its *current* routing table (as given in Problem 2.**b**). Once D receives the packet, it will send it back to C!

[*Note that the packet will be caught in a forwarding loop, it will eventually get discarded once its TTL reaches 0, assuming that the TTL value is smaller than the time before the next round of DV exchanges among the routers starts.*]

d. (6 points) What is the *split-horizon* hack? Will it solve the problem (if there is any) you see in your answer to c.?

Ans. The *split-horizon* hack is a way of fixing the count-to-infinity problem. It sets a router to never advertise the cost of a destination to a neighbor, *if it uses the neighbor as the next-hop to reach the said destination.*

Unfortunately, the split-horizon hack won't fix the problem in question **c.** – that's why is called a *hack*; they can only fix the "county-to-infinity" problem when the loop only involves *two nodes*. When the loop involves three or more nodes, it breaks down.

[Note that the *split-horizon* with *poisonous reverse* hack adds a "poisonous reverse" as follows: if X routes to Z via Y, then X tells Y that its distance to Z is *infinity* (instead of just not telling it anything) – adding poisonous reverse speeds up the convergence.

Unfortunately, the *split-horizon* with *poisonous reverse* hack will not fix the the problem in question **c.** neither. Just as in the case of the *split-horizon* hack, it breaks down when the loop involves three or more nodes.

There is another *hack* that can potentially address this problem using the so-called *hold-down timer*. Again it's a hack and can break down depending on the size of the loop and the value of the timer used. If you are interested, look it up by yourself.

So you ask: Is there a real *solution* to the "count-to-infinity" problem? Yes, there is. But it is very convoluted, and is implemented in the Cisco EIGRP protocol. If you are interested in a pointer to the solution, please ask Prof. Zhang!]

3. Inter-Domain Routing and BGP (18 points. Approx. 20 minutes)

Consider Figure 2 , where AS A is a *customer* of ISP X and ISP U, and AS B is a *customer* of ISP X and ISP V. ISP X in turn has two *provider* ASes U and V, while AS C is a customer AS of AS W and AS U. The three ASes U, V and W have *peering* relationships among themselves. AS X owns the prefix `64.1.0.0/16`, and AS C owns the prefix `180.1.0.0/16`. AS A owns two network prefixes: `64.1.10.0/24`, and `128.101.34.0/24` and, and AS B also owns two prefixes: `64.1.24.0/24` and `134.10.35.0/24`. The inter-domain routing protocol BGP is used among the ASes to exchange routing information. Answer the following questions.

a. (3 points) For a packet from a host in AS A with the destination IP address 180.1.34.35, which ASes would this packet *most likely* traverse to reach its final destination? Briefly explain your answer.

Ans. This packet would most probably take $A \rightarrow U \rightarrow C$ route. Since both X and U are providers of A, and the route announced by U, `180.1.0.0/16 CU`, will be shorter than that

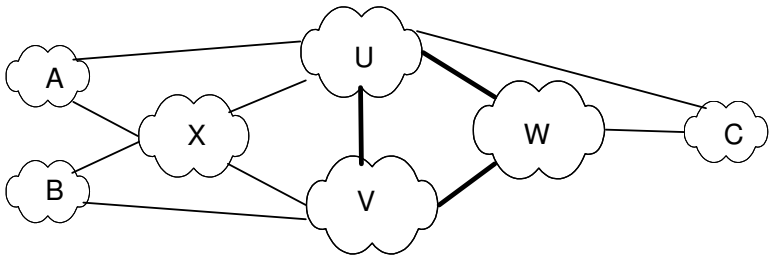


Figure 2: Figure for Question 3.

announced by X, say, `180.1.0.0/16 CUX`.

b. (4 points) Suppose AS A wants the traffic to its prefix `128.101.34.0/24` to come from AS U while the traffic to its prefix `64.1.10.0/24` to come from AS X. What route(s) should AS A announce to AS U, and what route(s) should AS A announce to AS X?

Ans. `128.101.34.0/24 A` to U, and `64.1.10.0/24 A` to X.

c. (6 points) Following up on **b.**, now suppose AS B announces the following routes to both AS X and AS V: `64.1.24.0/24 B` and `134.10.35.0/24 B` , and suppose AS X announces the following routes to AS V and AS U: `64.1.0.0/16 X` and `134.10.35.0/24 XB`. (Note that AS X does *not* need to propagate the routes `64.1.10.0/24 A` and `64.1.24.0/24 B` it learned from AS A and B, since both the network prefix `64.1.10.0/24` owned by AS A and the network prefix `64.1.24.0/24` owned by AS B are sub-prefixes of the prefix `64.1.0.0/16` owned by AS X, and thus can be aggregated into the route `64.1.0.0/16 X` it has announced to AS U and AS V.) Furthermore, suppose that AS V always sets a local preference of value 100 to routes learned from AS X, while a local preference of value 50 to routes learned from AS B. Answer the following questions: (i) For packets from AS V that are destined to the prefix `134.10.35.0/24`, will these packets go through AS X first, then to AS B? (ii) What about packets from AS V that are destined to the prefix `64.1.24.0/24`? Briefly explain your answers.

Ans.
(i) Yes! AS V learns two *customer* routes about the network prefix `134.10.35.0/24`, the shorter one `134.10.35.0/24 B` from AS B and the longer one `134.10.35.0/24 BX`. However, since AS V sets the local preference for the routes from AS X is higher than those for AS B, it will pick the longer route from X and installs it in its routing tables. As a result, packets from V destined to the prefix `134.10.35.0/24` will take the path $V \rightarrow X \rightarrow B$.

(ii) packets from V destined to the prefix `64.1.24.0/24` will take the direct path $V \rightarrow B$. Although AS V prefers the routes from AS X over those from AS B, because longest prefix matching, the packets from V destined to the prefix `64.1.24.0/24` will match the prefix learned from AS B, *not* the *shorter* prefix `64.1.0.0/16`.

d. (5 points) Based on your answer in **b.** above and the assumptions in **c.**, answer the following questions: (i) how many routes regarding the network prefix `128.101.34.0/24` will AS W receive? (ii) How many routes regarding the network prefix `134.1.35.0/24` will AS W receive? (iii) How many routes regarding the network prefix `64.1.10.0/24` will AS C receive?

Ans.

(i) Only one from AS U, namely, `128.101.34.0/24 UA`.

(ii) Two: one from AS U, `134.1.35.0/24 UXB`; and one from AS V, `134.1.35.0/24 VXB`.

(iii) None!

[Note that as stated in **a.**, AS A announces only `64.1.10.0/24` to AS X, which aggregates it with its own (larger) prefix `64.1.0.0/16` and announces only the aggregated route `64.1.0.0/16 X` to AS U and AS V (as stated in **b.**).]

4. Media Access Control (20 points. Approx. 20 minutes)

a. (6 points) Which technology, Ethernet or Token Ring, would be more efficient in a network that is *lightly loaded* (e.g., only one station has data to send at any given time)? Which of the two would be more efficient in a network that is *heavy loaded* (e.g., every station has data to send at any given time)? Briefly explain your answers.

Ans.:

On a *lightly loaded* network, Ethernet would be more efficient as any station who has data to send can immediately "grap" the channel and transmit without any collision (under the assumption that only one station has data to send at any given time), whereas a station on a *lightly loaded* Token Ring has to wait for the token before it can transmit. In contrast, on a *heavily loaded* network, Ethernet would *not* be very efficient, as several stations are likely to transmit data at the same time, causing collisions, which trigger the use of exponential back-off mechanism that further delays the transmission of data; whereas a *heavily loaded* Token Ring network would be more efficient, as each station takes turns to send data without any collisions.

b. (5 points) Briefly explain why in an 802.11 wireless LAN using CSMA/CA, a station receiving a data frame always needs to send an ACK frame back to the sender.

Ans.:

This is because in an 802.11 wireless LAN a station sending a framework has no way to know whether the transmitted frame is received successfully by the received or not, due to the hidden terminal problem. In addition, while transmitting a frame, the sender often shuts off its receiver to save power. As the sending station needs to inform the upper layer whether the transmission is Okay or not; it relies on the receiver to send an ACK to inform it whether the transmission is successful. Otherwise it would retransmit the frame until it receives the ACK.

c. (4 points) Following up on **b.**, briefly explain how the 802.11 wireless CSMA/CA MAC protocol ensures that the receiving station always has a *higher probability* to "seize" the wireless channel and send out an *ACK* frame before any other stations.

Ans.:
In CSMA/CA any station that wants to start the transmission by sending a data frame (or by sending an RTS request frame, if CA is enabled) must find the medium empty for at least DIFS time, whereas for sending the ACK receiving station would wait for only SIFS time. In 802.11 $DIFS >> SIFS$, hence the station receiving a data frame has a *higher probability* to seize the wireless channel and send out an *ACK* frame before any other stations.

d. (5 points) Give an example to show that the above mechanism does not provide a *100% guarantee* that the receiving station will always be able to send out the *ACK* frame *without collision*.

Ans.:
The key here is the *hidden terminal problem*. Depending on whether CA is used or not (recall that stations in an 802.11 LAN typically do not use CA when sending small data frames; more generally, a station can even disable CA altogether). In the simpler scenario where we assume that CA is not used, suppose a station C cannot hear station B's transmission (to station A). Hence station C is not aware of that a station A is receiving a packet from station B. Station C waits for DIFS amount of time, and finds that the channel is idle throughout the duration o the DIFS time period. It starts transmitting a frame (say, to station A) just as station A starts replying the ACK frame to station B, after waiting for SIFS amount of time after receiving the frame from station B. Hence a collision occurs.

In a slight more complicated scenario where we assume that CA is used. If even though the RTS/CTS mechanism to design to avoid collision (thus the name *collision avoidance* or *CA* in CSMA/CA), we see that it may not completely eliminate collision, as illustrated below using a similar scenario as before. Again we assume that due to the hidden terminal problem, station C cannot hear station B's transmission (to station A). Furthermore, while station C *can* hear station A's transmission, station C just started listening to the channel after station A's has sent the CTS reply to station B, granting station B to transmit a data frame to it. In other words, station C started sensing the channel in the middle of the frame transmission from station B to station A. Since station C cannot hear the transmission from station B, and thus finds the channel idle for the entire duration of the DIFS time period. It thus sends a RTS frame to station A, requesting to transmit a data frame to it. At the same time, station A starts replying the ACK frame to station B. The RTS frame from station C to station A thus collides with the ACK frame from station A!

5. Ethernet Switches and 802.1 Wireless Access Point (20 points total. Approx. 25 minutes)

Consider a campus LAN environment as shown in Figure 3, which consists of multiple Ethernet LANs and an 802.11 wireless LAN connected through three Ethernet switches ($S1$,

$S2$ and $S3$) and one 802.11 wireless access point (AP). There are also two IP routers, $R1$ and $R2$, which connect these LANs and several servers to each other and to the rest of the Internet. The numbers (1,2, or 3) besides the three switches, the AP, two routers and a couple of "dual-homed" machines indicate their network interface numbers. (The DNS server N connects to both the Ethernet switch $S2$ and router $R1$, and the laptop L is currently connecting to both the Ethernet switch $S2$ and the wireless access point AP.) In answering the following question, you can assume that $R2$ is the *default* router/gateway for all the machines that are connected to the IP subnet formed by the Ethernet switches $S1$, $S2$, $S3$ and the wireless access point AP. The *current* snap shots of the forwarding tables at the AP and the three Ethernet switches are shown at the bottom of the figure. In particular, three machines (Laptop J, Laptop L and Mobile Device M) are currently *associated* with the wireless access point AP.

Answer the following questions *briefly*. (A few sentences would be sufficient in general!)

a. (7 points) Consider the scenario where Host A wants to access the web server W, but doesn't know its IP address. Hence A issues a DNS query to the local DNS server N to find out the IP address of W. Host A encapsulates the UDP packet containing the DNS query in an IP datagram, which is then encapsulated in an Ethernet frame. Suppose A has N's MAC address in its local ARP cache.

i) (1 point) What will be the destination IP address of the IP datagram?

Ans. N's IP address.

ii) (1 point) What will be the destination MAC address of the Ethernet frame?

Ans. N's MAC address.

iii) (1 points) What will Switch $S1$ do when it receives the Ethernet frame?

Ans. $S1$ will use the destination MAC address N to look up its forwarding table. Since N's MAC address is currently not in $S1$'s forwarding table, it will forward the frame to all other interfaces (1, 3, 4) except where it comes from (interface 1).

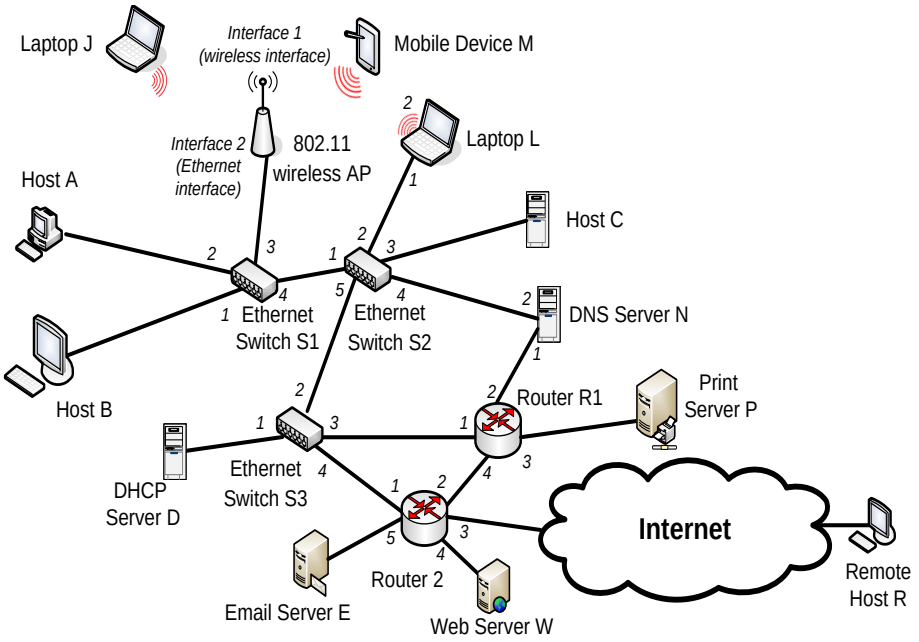
Using the source MAC address A, $S1$ will also refresh the timer for the forwarding entry of A – this is an optional answer for the students.

iv) (2 points) What will Switch $S2$ do when it receives the Ethernet frame?

Ans. $S2$ will use the destination MAC address N to look up its forwarding table, and forward it to interface 4.

Using the source MAC address A, $S2$ will add a new forwarding entry [$A1$] – this is required; deduct 1 point if this is not answered!

v) (2 points) Will the wireless access point AP receive the Ethernet frame? If yes, what will it do with it?



Wireless AP's Forwarding Table

Host	interface
J	1 (wireless)
L	1 (wireless)
M	1 (wireless)
A	2 (Ethernet)
B	2 (Ethernet)
R2	2 (Ethernet)

Ethernet Switch S1's Forwarding Table

Host	interface
A	2
B	1
AP	3
D	4
R1	4
R2	4

Ethernet Switch S2's Forwarding Table

Host	interface
C	3
D	5
L	2
N	4
R1	5
R2	5

Ethernet Switch S3's Forwarding Table

Host	interface
D	1
N	2
R1	3
R2	4
E	4
W	4

Figure 3: Figure for Question 5.

Ans. Yes, it will. As AP has only two interfaces, the Ethernet interface 1 where the frame comes from, and the 802.11 WiFi interface 2. Since N is *not* associated with its WiFi interface (i.e., N is not on the 802.11 Wireless LAN), it will simply drop it!

b. (4 points) Following up on **a.**, when the DNS server N sends the DNS reply back to Host A, the UDP packet containing the DNS reply is encapsulated in an IP datagram, which is in turn encapsulated in an Ethernet frame with A's MAC address as the destination MAC address and N's MAC address as the source MAC address.

i) (1 point) What will Switch $S2$ do when it receives the Ethernet frame containing the DNS reply?

Ans. $S2$ will use the destination MAC address A to look up its forwarding table, and forward it to interface 1 – *cf.* Answer to **a.**(iv).

Using the source MAC address N, $S2$ will also refresh the timer for the forwarding entry of N – this is an optional answer for the students.

ii) (2 points) What will Switch $S1$ do when it receives the Ethernet frame?

Ans. $S1$ will use the destination MAC address A to look up its forwarding table, and forward it to interface 2.

Using the source MAC address N, $S1$ will add a new forwarding entry $[N4]$ – this is required; deduct 1 point if this is not answered!

iii) (1 point) Will the Ethernet switch $S3$ receive the Ethernet frame?

Ans. No! – *cf.* Answer to **a.**(iv).

c. (9 points) The following questions are concerned with the different roles that the wireless access point AP and Ethernet switches play in forwarding data frames between hosts. (In these questions, we assume that Laptop J knows the MAC addresses of Laptop L and Host C.)

i) (2 points) Consider the following two scenarios. Case 1: Laptop J sends a data frame to Laptop L on the same 802.1 wireless LAN; and Case 2: Laptop J sends a data frame to Host C. How does the access point AP know that in *case 1*, it needs to forward the data frame back (through its *wireless interface 1*) to the same 802.11 wireless LAN in order to reach laptop L; whereas in *case 2* it needs to forward the data frame to the Ethernet Switch $S1$ (through its *Ethernet interface 2*) in order to reach Host C?

Ans.

Case 1. Using the Address 3 (target destination) of the WiFi frame, namely, L, AP checks its forwarding table, and knows that L is associated with its WiFi interface 1, thus forwards it to its WiFi interface 1.

Case 2.

Using the Address 3 (target destination) of the WiFi frame, namely, C, AP checks its forwarding table, and finds that it has no forwarding entry for C is. (Hence C *can't* reside in its 802.11 wireless LAN, as all machines on its 802.11 wireless LAN must explicitly associate with AP.) Hence AP *assumes* that it resides on the local area network connected to its Ethernet interface (interface 1). It therefore forwards the frame to interface 2.

Note that in case 2, AP functions *almost* exactly like an Ethernet switch — if it doesn't find a forwarding entry for a destination MAC, it forwards the frame to all other (Ethernet) interfaces except the WiFi interface (which it knows precisely all machines that are currently on its WiFi LAN) and the (Ethernet) interface it comes from.

ii) (4 points) In terms of MAC addresses carried in the data frame, what changes does the access point AP need to make in *case 1*, namely, when forwarding a data frame from Laptop J to Laptop L; and what about *case 2*, namely, when forwarding a data frame from Laptop J to Host C?

Ans.

The 802.11 frame from Laptop J to AP contains the following:
Address 1: AP's MAC address, Address 2: J's WiFi MAC address, Address 3: L's MAC address. Also: the "To-AP" bit is set to 1 (and the "From-AP" bit is set to 0).

Case 1. The new 802.11 frame contains:

Address 1: L's MAC address, Address 2: AP's WiFi MAC address, Address 3: J's MAC address. Also: the "From-AP" bit is set to 1 (and the "To-AP" bit is *reset* to 0).

Case 2. The new Ethernet frame contains:

Destination MAC address: C's MAC address; Source MAC address: J's MAC address.

iii) (2 points) In *case 1* above, will Switches $S1$ and $S2$ eventually learn about the existence of Laptop J? (In other words, will they add an entry about laptop J in their respective forwarding tables?) What about *case 2*? Simply answer yes or no for both questions.

Ans.

Case 1. No.
Case 2. Yes.

iv) (1 point) Consider the *case 2* above. Suppose that after Host C has received the data frame from Laptop J, it sends back a data frame to Laptop J. Does Host C need to know the MAC address of the wireless access point AP in order to send the data frame to Laptop J? Simply answer yes or no.

Ans. No.