CS118 Quiz 4, Spring 2020

Name: _____

Student ID: _____

Notes:

1. This is an open-book, open-notes quiz. You have two hours to work on your quiz, scan or photo your paper copy, and upload to the Gradescope.
2. You need to upload your scanned copy or the photoed picture of your answer sheet to the Gradescope before the deadline.
3. You are allowed to use your calculator. You are advised **not** to use the Internet to search for hints during the quiz. By submitting your quiz, you declare that **your work is solely done by yourself and you have not interacted with anyone else other than the instructor and proctors during the test**.
4. If you have any issues with the quiz, you can tune in the regular Lecture Zoom link and use the Chatroom there during the quiz time. We will provide clarifications there during the quiz.
5. Be **brief** and **concise** in your answers. Answer only within the space provided. If you need additional work sheets, use them but do NOT submit these sheets.
6. If you wish to be considered for partial credit, show all your work.
7. **Show your steps to receive partial credit**.
8. You have 5 problems in 7 pages plus this page.

PROBLEM	MAX SCORE	YOUR SCORE
1	24	
2	21	
3	12	
4	21	
5	12	
TOTAL	90	

Problem 1: Multiple choices (24 points; 3 points each). Select *all* (i.e., possibly more than one) correct answers.

1. Which feature(s) does virtual local area network (VLAN) **NOT** have?

   - Your answer ____ (A) Port-based VLAN divides switch ports into multiple groups; (B) Ports in the same group form a broadcast domain; (C) Broadcasting frames to all ports are still supported even if multiple separate VLAN groups are formed; (D) A table of port-to-VLAN mapping is kept with the switch; (E) A switch never knows that a frame arriving on a trunk port belongs to a particular VLAN.

2. Which protocol(s) would belong to the random access MAC?

   - Your answer ____ (A) slotted Aloha; (B) time division multiple access; (C) frequency division multiple access; (D) CSMA/CD; (E) token-based multiple access.

3. What can be true for address resolution protocol (ARP)?

   - Your answer ____ (A) Given the IP address, ARP can find the MAC address of another host on any part of the Internet; (B) Given the IP address, ARP can find the MAC address of another host in the same subnet; (C) The IP-to-MAC address mapping never expires once obtained by a host; (D) A malicious host can fabricate an ARP reply and pretend to be another host; (E) ARP is not needed if DHCP protocol is used.

4. What attack(s) can nonce defend against?

   - Your answer ____ (A) IP address spoofing attack; (B) sniffing attack; (C) denial-of-service attack; (D) replay attack; (E) message integrity attack.

5. Assume Bob wants to verify the digital signature signed by Alice. What key(s) and/or function(s) will Alice use for the digital signature to work?

   - Your answer ____ (A) Alice's own private key; (B) Bob's public key; (C) Bob's private key; (D) a symmetric key agreed by Alice and Bob; (E) (one-way) hash function that will not uncover the message given the message digest.

6. Which security service(s) does **NOT** use public-key cryptography at all?

   - Your answer ____ (A) confidentiality; (B) authentication; (C) integrity; (D) replay attack prevention; (E) access control.

7. Which of the following mechanism(s) does IEEE 802.11 Wireless MAC use to enable fast loss recovery?

   - Your answer ____ (A) RTS/CTS handshake; (B) link-layer ACK; (C) carrier sensing; (D) binary exponential backoff; (E) deferral upon hearing RTS/CTS by other stations.

8. Which security service(s) are **NOT** provided by SSL (secure sockets layer)?

   - Your answer ____ (A) confidentiality; (B) authentication; (C) integrity; (D) replay attack prevention; (E) man-in-the-middle attacks.

Problem 2 (21 points; 3 points each): Answer the following questions. Be brief and concise.

1. Suppose four active nodes - node A, B, C and D - are competing for access to a wired channel using unslotted (pure) ALOHA. Assume each node has an infinite number of packets to send. Each node attempts to transmit with probability p. What is the best probability p that maximizes the overall channel access for these four nodes? Show your main steps.

2. The emerging virtual reality (VR) applications need variable-rate yet high throughput, and low latency data delivery. Which of the following MAC can best serve the scenario where multiple devices, each of which runs the VR application, compete for the channel, CSMA/CD, slotted ALOHA, polling-based MAC, and TDMA? Briefly justify your answer.

3. Can you list two methods to implement the retransmissions for customized TCP protocol in Project 2?

4. Explain the key difference in terms of objectives between the link-layer acknowledgment (ACK) used by WiFi and the transport-layer ACK in TCP.

5. Briefly explain what is man-in-the-middle attack, and how you can defend against man-in-the-middle attack.

6. Note that IP packet forwarding and routing need to use the IP packet header. If VPN encrypts the IP packet header, explain how the IP packet is routed and forwarded in VPN.

7. For data frame transmissions, can the 802.11 CSMA/CA protocol avoid data frame collisions completely? If yes, justify your answer; if no, describe how the CSMA/CA handle collisions.

Problem 3 (12 points): Layered protocols Alice uses her laptop to browse the Web service at www.google.com. When walking into her office, she immediately boots up her laptop and connects it to the CS department's WiFi network, which is connected to the UCLA campus network that has a link to the Internet. The CS WiFi wireless network has a local DHCP server and a DNS server. Identify protocols used in each step during Alice's Web browsing. Note that Google's Web server is located at a different subnet in another AS domain different from the UCLA campus network. Assume that the DNS cache does not have any entry for Google initially. The ARP table of Alice's laptop is also empty initially.

1. (3 points) Identify three protocols used (in addition to IP protocol) when Alice's laptop is connected to the CS WiFi network and gets her IP address.

2. (2 points) Identify two protocols used (in addition to IP protocol itself) when Alice sends her IP packets to another host over the same WiFi network.

3. (2 points) Alice's laptop needs to know the IP address for www.google.com. Identify two used protocols above the IP layer (not including IP).

4. (2 points) Identify two transport-layer or above protocols used when Alice's laptop is finally able to browse the website www.google.com.

5. (2 points) Identify two routing protocols being used when Alice's laptop is finally able to browse the website www.google.com.

6. (1 point) Identify at least one *plug and play protocol* used in the above process.

Problem 4 (21 points): Ethernet LANs and WiFi Networks The CS and EE departments have been joining efforts to interconnect their departmental Ethernet LANs, and then possibly convert them into wireless WiFi. To this end, they have initially formed a single Ethernet using switches, and deployed 40 Access Points (APs). However, the performance was poor. To improve the situation, they have decided to separate the single Ethernet into four Ethernets: two for CS, and two for EE. However, they need to figure out whether to use switches or routers to interconnect the four Ethernets. Furthermore, they plan to support seamless service (i.e., established TCP connections will keep going without disruptions) as users walk around the WiFi networks.

1. (2 points) Can you identify the main reason why the initial design of a single Ethernet to interconnect EE and CS departments had poor performance?

2. (9 points) If they decide to use switches,

   (a) (2 points) What algorithms are needed for the switch to interconnect four Ethernets and facilitate smart frame forwarding? Will any changes be made to the user devices?

   (b) (2 point) Does the interconnection need manual configuration? Briefly explain why.

   (c) (2 points) The EE department wants to separate its Ethernet that connects its APs from that in the CS department for better privacy. However, both departments want to share the cost by using the same physical switches whenever possible. Describe a solution to achieving this goal.

(d) (1 point) Within the CS/EE departments (i.e., within the two Ethernets deployed within each department), if the Ethernets have been converted to Wi-Fi completely, what kind of solutions are needed to support user mobility?

(e) (2 point) Assume EE's Ethernet is separated from CS's Ethernet by the approach mentioned in 4.2(c). Between the CS and EE departments (i.e., a user walks from CS WiFi to EE WiFi), what kind of solutions are needed to support user mobility?

3. (6 points) If they decide to use Routers,

   (a) (2 point) Will the collision problem as observed with the current single Ethernet case be reduced? Briefly justify your answer.

   (b) (2 points) Will any changes be needed to some of, or all, the user devices? If so, what changes are needed? Explain your answer. (*Hint*: consider routing table at each device)

   (c) (2 points) What kind of mobility solution is needed to support roaming across CS and EE WiFi networks?

4. (4 points) If they decide to use Routers and enable IP broadcast at certain routers to support mobility (as a mobile user moves, IP broadcast will broadcast the packets to all subnets that are connected to those broadcast-enabled IP routers).

   (a) (2 points) Given a mobile user, rather than broadcast all packets to all routers, can you design a solution, so that only the router in the WiFi network where the mobile user currently stays will receive the broadcast packets, but other IP-broadcast-disabled routers will not broadcast the packets. (*Hint*: consider how the mobile user updates its location and enables forwarding as it roams in Mobile IP).

(b) (2 points) Identify one advantage and one disadvantage of this solution compared with Mobile IP.

Problem 5: Network Security (12 points): Alice and Bob are using the Internet for data communications. They are seeking to use the known, available security mechanisms to secure their communications against the attacker Tracy. Meanwhile, Tracy has designed a series of attacks to defeat the network security between Alice and Bob. Initially, before Alice and Bob start data communications, Alice asks Bob's public key, and Bob consequentially replies with his public key to Alice. Similarly, Bob asks and gets Alice's public key too. They will use these two public keys to start with.

1. (2 points) Suppose Tracy is also sending a fake public key (pretending to be Bob) to Alice. Can you design a mechanism so that Alice can know the authenticity of Bob's public key (i.e., she can tell whether it is from Bob or someone else like Tracy)? (*Hint: consider the use of certification authority.*)

2. (2 points) How can Alice and Bob know that the certification authority is authentic?

3. (2 points) Assume that both Alice and Bob obtain each other's true public key now. They first use the public key to encrypt their data communications. However, this is computationally expensive. Can you describe *step-by-step* a more efficient encryption solution? *Hint: symmetric key based encryption is computationally more efficient.*

4. (2 points) Now Alice receives a new certificate, notifying her that Bob's public key is updated to the new one carried in the certificate. The certificate claims to be from CA (certificate authority) but does not carry CA's signature. Assume the CA is temporarily down now. Can you design a solution without going through CA, but letting Alice verify whether this claimed key update is an authentic one from Bob? *Hint: Alice knows the previous public key for Bob is authentic.*

5. (2 points) Tracy intercepts the physical route between Alice and Bob. She found that, the latest data messages sent from Bob have neither Bob's digital signature nor the message authentication code. What attack can Tracy thus launch against Alice?

6. (2 points) Assume that the latest data messages sent from Alice have both Alice's digital signatures and message digest. However, the data messages do not contain the nonce field. What kind of attack can Tracy launch again Bob?