University of San Francisco

CS621: Network Programming

Exam

Student's Name: _____

Student's ID: _____

Professor: Dr. Vahab Pournaghshband

Question	Score
Problem 1 (3)	
Problem 2 (2)	
Problem 3 (2)	
Problem 4 (2)	
Problem 5 (2)	
Problem 6 (2)	
Problem 7 (2)	
Total (15)	

Q.1) Short Questions

1/1/1=3 points

a) You are to design a timeout for TCP acknowledgment system. What is the minimum value (lower-bound) for the timeout of a reliable transmission protocol?

RTT. This is a reasonable lowerbound to ensure timeout doesn't go off prematurely (i.e., packet marked as lost while the ACK is still on its way).

b) During normal IPv4 packet forwarding at a router, which packet field(s) are always updated? (only list the header fields)

TTL and checksum

c) What is the main problem in Strict Priority Queuing when it comes to low priority traffic?
Starvation of low priority packets.

Does Traffic Shaping have this problem?
No

How about Weighted Fair Queuing?
No

Q.2) Firewall Policy

0.5/0.5/1=2 points

Below is a firewall implementation.

Source (Address:Port)	Destination (Address:Port)	Protocol	Action
201.22.192.4:*	131.197.2.101:22	TCP	Allow
131.197.2.3:*	201.22.192.4:80	TCP	Drop
131.197.2.101/24:*	201.22.192.4:80	TCP	Allow
*	*	*	Drop

a) What is the default policy?

Deny-all (aka whitelisting)

b) In one sentence, describe what does the first policy in this firewall implementation entail? (SSH: Port 22)

Allow all TCP connection from 201.22.192.4 (our webserver) to 131.197.2.101 port 22 (ssh).

c) Fill in the second (and third if you need it) policy rule so that all hosts in the 131.197.2.0/24 prefix can access our webserver on port 80 (HTTP) except the known malicious host 131.197.2.3.

Q.3) Symmetric-Key Encryption

2 points

Tatebayashi, Matsuzaki, and Newman (TMN) proposed the following protocol, which enables Alice and Bob to establish a shared symmetric key K with the help of a trusted server S. Both Alice and Bob know the server's public key K_S. Alice randomly generates a temporary secret K_A, while Bob randomly generates a new key K to be shared with Alice. The protocol then proceeds as follows:

$$Alice \rightarrow Server \quad enc_{K_S}(K_A)$$

$$Bob \rightarrow Server \quad enc_{K_S}(K)$$

$$Server \rightarrow Alice \quad K \oplus K_A$$

$$Alice\ recovers\ key\ K\ as\ K_A \oplus (K \oplus K_A)$$

In this protocol, Alice sends her secret to the Server encrypted with the Server's public key, while Bob sends to the Server the new key, also encrypted with the Server's public key. The Server XORs the two values together and sends the result to Alice. Therefore, both Alice and Bob know K.

Suppose that evil Charlie eavesdropped on Bob's message to the Server. How can he, with the help of his equally evil buddy Don, extract the key K that Alice and Bob are using to protect their communications?

Assume that Charlie and Don can engage in the TMN protocol with the Server, but they don't know the Server's private key. In other words, Charlie and Don can use the TMN protocol to establish their own shared key.

$$Charlie \rightarrow Server \quad enc_{K_S}(K) \quad (replay\ Bob's\ message)$$

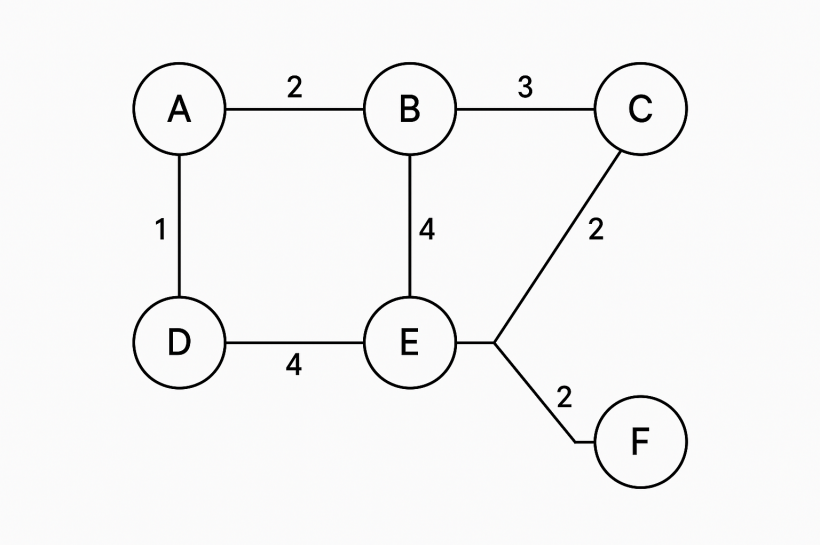
$$Don \rightarrow Server \quad enc_{K_S}(K_D) \quad (Don\ sends\ his\ random\ number\ to\ server)$$

$$Server \rightarrow Don \quad K \oplus K_D$$

$$Don\ recovers\ key\ K\ as\ K_D \oplus (K \oplus K_D)$$

Q.4) Routing 1/1=2 points

You are given the following network topology and associated link costs:



Assume that all routers use a link-state routing protocol and compute shortest paths using Dijkstra's algorithm.

i) Before Router A receives any Link-State Advertisements (LSA) from other routers, what does its initial routing table look like?

Node	**Cost**	**Next Hop**
A	0	—
B	2	B
C	∞	—
D	1	D
E	∞	—
F	∞	—

ii) In highly dynamic networks such as vehicular network (where link failures and additions occur frequently), some implementations of link-state routing use LSAs with a *scoped TTL* (i.e., a small TTL value) to limit the flooding radius. Explain one benefit and one drawback of using scoped TTL LSAs in such a network.

Benefit:

Due to partial flooding, the network is not overwhelmed by frequent LSA broadcasts/flooding. This improves the overal goodput of the network and increases the available bandwidth for actual data transmission.

Drawback:

A short TTL can be problematic in link-state protocols if essential updates (like link failures) don't reach all routers that rely on that link in their path computation.

Q.5) TCP 1/1=2 points

Traditional TCP assumes that packet loss indicates congestion, which causes the sender to reduce its transmission rate. However, in TCP in error-prone, low-congestion networks like satellite or wireless links, packet loss may occur due to bit errors, even when there is no congestion. This leads to underutilization of available bandwidth. Propose any modification to TCP that allows it to distinguish between congestion-induced and corruption-induced packet loss. Your response should address both of the following:

i) *Loss classification mechanism:* How does the sender or receiver detect whether a loss is due to congestion or corruption?

Use an explicit signal—such as a separate packet or a header field—from the router, receiver, or both to inform the sender that a packet is corrupted (due to a checksum failure). The sender still relies on the traditional timeout and ACK mechanism to detect packet loss.

ii) *Protocol behavior:* How should TCP respond differently to each type of loss?

If loss is due to corruption: Do not reduce the congestion window (cwnd); instead, retransmit the lost packet while maintaining rate.

If loss is due to congestion: Follow traditional TCP behavior (e.g., fast retransmit, congestion avoidance).

Q.6) DNS 1.5/0.5=2 points

A local DNS resolver is configured to use iterative resolution and currently has only one cached entry: the IP address of the authoritative name server for `cs.usfca.edu`. It has no cached information about `.edu`, `usfca.edu`, or any other domain.

i) How many queries will the local DNS server generate to resolve `student1.lab.cs.usfca.edu`? List the queries in order, and specify to which server each query is sent.

Since only cs.usfca.edu's authoritative name server is cached, but the target is student1.lab.cs.usfca.edu, the local resolver must query hierarchically below cs.usfca.edu.

Total: 2 queries.

Queries:

Query: lab.cs.usfca.edu to cs.usfca.edu's name server → gets referral to lab.cs.usfca.edu's name server.

Query: student1.lab.cs.usfca.edu to lab.cs.usfca.edu's name server → gets final A record.

ii) Two users, Alice and Bob, are on the same corporate network that uses a shared recursive DNS resolver.

- At 9:00 AM, Alice visits `student1.lab.cs.usfca.edu`, which causes the local DNS resolver to query the authoritative name server and cache the A record with a TTL of 1800 seconds (30 minutes).
- At 9:10 AM, the authoritative name server updates the A record for `student1.lab.cs.usfca.edu` to a new IP address.
- At 9:15 AM, Bob visits the same domain for the first time.
- Will Bob receive the updated IP address? Why or why not?

No, Bob will not receive the updated IP address. The corporate resolver already cached the old IP when Alice visited at 9:00 AM, and since the TTL is 30 minutes, it will continue to return the cached value until 9:30 AM, regardless of the update at the authoritative name server.

Q.7) Public-Key Encryption

0.5/1/0.5=2 points

i) Let S be a publicly available trusted service that knows the public keys of all users. Alice communicates with S to obtain Bob's public key (PK_B) using the following protocol: (S's keys are (SK_S, PK_S)).

1. $A \rightarrow S \ : \ A, B$
2. $S \rightarrow A \ : \ Enc(SK_S, \{PK_B, B\})$

(i.e., the message $\{PK_B, B\}$ is encrypted using S's private key.)

In step 1, Alice sends along her identity A and asks S for Bob's public key. In step 2, S responds by returning Bob's public key PK_B along with his identity B, and signs the message. Assume S has the current key Bob is using. Which of the following attacks is this protocol vulnerable to? **Mark ALL that apply.**

a. Mallory can tamper with S's response so as to substitute her own public key PK_M instead of PK_B.
b. Since S's response is not encrypted, Mallory can use PK_B to decrypt any messages Alice sends to Bob in the future.
c. Mallory can tamper with S's response so as to substitute an older key PK'_B that Bob might have revoked.
d. None of these.

(c) is the correct answer. (a) does not work because it requires Mallory to forge S's signature. (b) is factually incorrect – Mallory requires SK_B to decrypt the messages.

ii) For the same situation as in the previous question, what should the message in step 2 ($S \rightarrow A$) (or steps 1 and 2) be instead, to defend against the attacks that the protocol in that question is vulnerable to?

$S \rightarrow A : Enc(SK_S, \{PK_B, B, T\})$ where T is a timestamp.

The server can prevent a replay attack by including a timestamp in its response (if we assume the clocks are synchrnoized). Using a nonce or a random number instead of a timestamp in S's response is a better approach but it requires A to send the nonce to S in step 1.

iii) In parts (i) and (ii), we assumed that the server S always has the most up-to-date key for Bob. Now, let's relax that assumption. It's possible that Bob's previous key has been revoked and he is now using a new key pair, but the server S has not yet updated its records.

To address this, what additional steps should Alice take—beyond steps 1 and 2—to verify that the key she retrieved from S is actually the current key in use by Bob? This verification is referred to as *proof-of-possession* in cryptography.

Alice generates nonce, r (a random number)
Step 3: $A \rightarrow B : r$
Step 4: $B \rightarrow A : Enc(SK_B, r)$
Alice verifies the key by decrypting what Bob sent using PK_B.