SUNetID: ________

CS144
Intro to Computer Networks
Final Exam – Thursday, December 9, 2021

Rules: 2 note pages, closed book, computers off

Your Name: Answers

SUNet ID: root @stanford.edu

In accordance with both the letter and the spirit of the Stanford Honor Code, I neither received nor provided any assistance on this exam.

Signature: ____________________

Check if you would like exam routed back via SCPD: ☐

- The exam has 6 questions totaling 64 points.
- You have 90 minutes to complete them.
- Please keep your answers concise. You may lose points for a correct answer that also includes incorrect or irrelevant information.
- If you would like to make any additional commentary on a multiple-choice answer, please write it below the answer section, but nothing additional is necessary to receive full credit.
- Please box your final answers.

1	/15
2	/11
3	/10
4	/12
5	/8
6	/8
Total	/64

SUNetID: __________

I Accessing a Website

What happens when you type the URL of your favorite cat-related blog in your Web browser and press "enter"?

Below is a template list of packets that you would observe being sent from and received by **your machine** if this communication is the **only one on the network** at the time.

Please (1) **fill in the blanks**; and (2) indicate **the order of steps** in which your machine will send or receive these packets. (You should write the order as a sequence of letters, e.g. BDECA. . . ; all letters should be listed exactly once.)

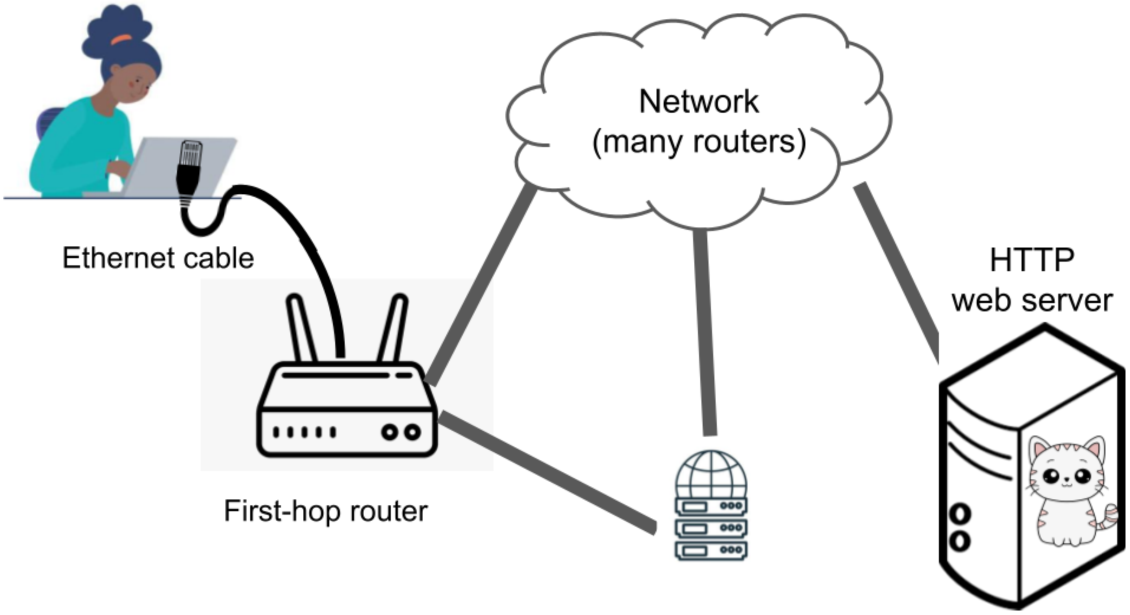

Figure 1: Image description: An illustration of some of the assumptions about the network listed below. (No additional information relevant to the problem is in this image.)

Assumptions:

- All local caches on your machine are initially empty.
- Your device's ARP cache — which starts out empty — is populated as in the NetworkInterface in the lab.

- Packets between your machine and the target Web server travel through multiple routers.
- Your device is connected to a network via an Ethernet cable and has been assigned an IP address.
- You have a single gateway, or "first hop," router. Its IP address is the target of the default route, which is the only entry in your device's routing table. Your DNS resolver is accessible via this router.
- There are no middleboxes (intermediary devices) involved in the communication (no proxies, no NApTs, no firewalls, etc.)
- The Web server uses HTTP over TCP over IP.
- We say that a packet is "sent by X" if X originates the packet. We say that this packet is sent "to Y" if Y is the target (**final**) destination of the packet.

Hint: terms that might be useful in filling in the blanks:

- *DNS resolver*
- *Your machine (client)*
- *Target (cat blog) web server*
- *First-hop router (from your machine/the client)*

1. **[15 points]:**

   (A) A TCP segment with the SYN flag and the ACK flag set; sent by ______________________________ to ______________________________.

   (B) A TCP segment with the SYN flag set (ACK flag not set) sent by ______________________________ to ______________________________.

   (C) A TCP segment with the ACK flag set (SYN flag not set) sent by ______________________________ to ______________________________.

(D) HTTP request(s) over an established TCP connection, asking for the content of the Web page sent by ________________________ to ________________________.

(E) HTTP response(s) over an established TCP connection, containing the contents of the Web page sent by ________________________ to ________________________.

(F) A DNS request sent by ________________________ to ________________________, requesting the ________________________ (IP / Ethernet: choose one) address of ________________________.

(G) An ARP request sent by your machine to Ethernet broadcast, requesting the ________________________ (IP / Ethernet - choose one) address of ________________________.

(H) An ARP response sent by ________________________ to your machine.

(I) A DNS response sent by ________________________ to ________________________, providing the ________________________ (IP / Ethernet - choose one) address of ________________________.

Order of steps: *(your answer here)*

Answer:

G. An ARP request sent by your machine to Ethernet broadcast, requesting the **Ethernet** *address of* **first-hop router***.*
H. An ARP response sent by **first-hop router** *to your machine.*

Explanation: Your machine sends an ARP request for the first-hop router. It has the IP address of the router in its routing table, but it needs the Ethernet address. Note that, as in your network interface lab, the router will learn your machine's Ethernet address when it receives this request, so it won't have to make an ARP request later.

F. A DNS request sent by **your machine** *to* **DNS resolver***, requesting the* **IP** *address of* **target web server***.*
I. A DNS response sent by **DNS resolver** *to* **your machine***, providing the* **IP** *address of* **target web server***.*

Explanation: Your machine needs the IP address associated with the domain so that it can route packets. These go to the DNS resolver, usually run by an ISP, which will perform a DNS recursive lookup or return a result from its cache.

B. A TCP segment with the SYN flag set (ACK flag not set) sent by **your machine** *to* **target web server***.*
A. A TCP segment with the SYN flag and the ACK flag set; sent by **target web server** *to* **your machine***.*
C. A TCP segment with the ACK flag set (SYN flag not set) sent by **your machine** *to* **target web server***.*

Explanation: This is the TCP 3-way handshake. Since your machine is playing the role of client, it initiates the connection to the server.

D. HTTP request(s) over TCP for the content of the web page sent by **your machine** *to* **target web server***.*
E. HTTP response(s) over TCP for the content of the web page sent by **target web server** *to* **your machine***.*

Explanation: now the connection is established, so you can request content and the server can send it back to you!

Order of steps: *G, H, F, I, B, A, C, D, E*

II Home networking

2. [**11 points**]:

Say you're at home, and you connect your laptop to your home Wi-Fi network. Running `hostname -I` shows you that your computer's network interface's IP address is 192.168.1.10 (a "private" IPv4 address). Later, you take your laptop to your friend's house and connect to their home Wi-Fi network. Running the same command shows that your computer's network interface's IP address is now 10.0.0.8.

(a) What protocol is your computer using to choose its IP address on each of these networks?

Circle the best answer.

- **A** IP
- [✓ **B**] DHCP
- **C** ARP
- **D** DNS
- **E** Bitcoin
- **F** HTTP/3
- **G** Zoom

(b) Which of the following are services typically provided by a "home router"?

Circle all that apply.

- [✓ **A**] IP router
- [✓ **B**] NAT
- [✓ **C**] DNS resolver
- **D** HTTP proxy
- [✓ **E**] DHCP server
- [✓ **F**] Wi-Fi access point
- [✓ **G**] Cable/fiber modem
- **H** SMTP server
- **I** VPN server

III Throughput of TCP Flows

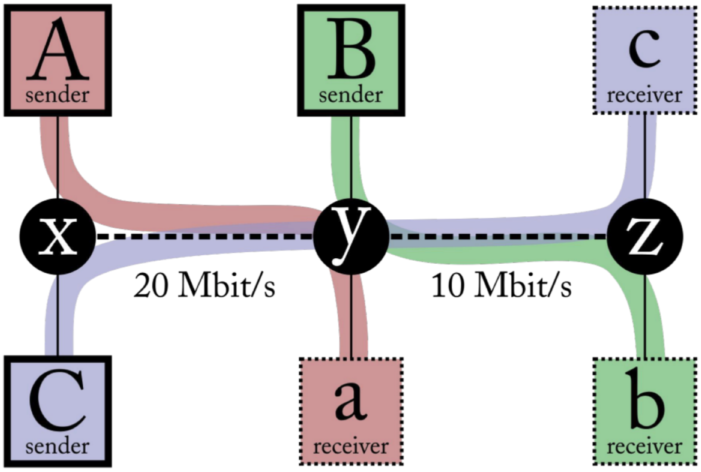

Figure 2: Image description: A network with three TCP flows (A, B, C), three routers (x, y, z), and two links. The flow "A" goes over the link from "x" to "y," which has a link rate of 20 Mbit/s. The flow "B" goes over the link from "y" to "z," which has a link rate of 10 Mbit/s. The flow "C" goes over the path from "x" to "y" to "z," crossing both links.

Please assume that:

- All routers maintain separate queues for each flow.
- Router X uses weighted fair queueing, with a weight of 0.4 for the flow coming from sender A and 0.6 for the flow coming from sender C.
- Router Y uses fair queueing (with each flow receiving an equal weight).
- If some flow queues are empty, the routers will continue transmitting from any non-empty queues.
- No packet loss or corruption occurs.
- All connections start at the same time.
- All connections use TCP, and run for a sufficiently long time to reach steady state. (You may think of these as uni-directional file transfers transmitting gigantic files.)

- All TCP receivers advertise the same, **fixed and finite window size**, of W bytes, which is sufficiently large for all flows together to keep the links busy.
- The senders **do not** use congestion control. The senders **do** respect TCP flow control (each sender respects the receiver-advertised window as an upper bound on its bytes in flight).
- All senders transmit segments of the same, fixed size.

3. [10 points]:

(A) In the network above, all connections start up at the same time, and all senders begin sending segments. What will be the approximate throughput of each flow during **this** time (at the beginning, before any sender has sent W bytes)?

Aa=

Bb=

Cc=

Answer:

A = 8 Mbit/s (0.4 · 20); C = 5 Mbit/s; B = 5 Mbit/s

(B) In the network described above, what will be the throughput of each flow over the **long term**? (That is, after the flows have been running for a long time such that they have converged to constant throughputs). Why? (2-3 concise sentences)

Aa=

Bb=

Cc=

Answer:

A = 15 Mbit/s; B = 5 Mbit/s; C = 5 Mbit/s.

C is initially sending segments faster than it's receiving acknowledgments. This means that it will eventually fill up its receiver-advertised window, so will only be able to send new segments when it receives acknowledgments. It will receive acknowledgments at a rate equivalent to the throughput of its flow, which is 5 Mbit/s because of the bottleneck link rate.

IV Adaptive Bitrate Algorithm

Ben Bitdiddle is streaming a video using a player running the following variant of the Buffer-Based Algorithm (BBA): use the lowest bitrate to download the first two chunks (1 Mbps) and subsequently select the bitrate to download further chunks based on the video player's **current buffer occupancy**, according to the function shown and described below. Assume:

- Each video chunk represents 4 seconds of video.
- A video chunk becomes available for playback immediate after the entire chunk has finished downloading. For example, if it takes x seconds to download the first chunk, the first chunk will start playing at second x and finish playing at second $x + 4$.
- In other words: at the moment that a video chunk finishes downloading, four seconds are added to the playback buffer occupancy.
- Ben's network connection has a link speed of 4 Mbps, and his transport protocol can fully utilize the link speed whenever downloading a chunk. (In other words, goodput = 4 Mbps, also known as 4 Mbit/s.)
- The video player downloads one chunk at a time, and always starts downloading the next chunk immediately when the previous chunk has arrived.

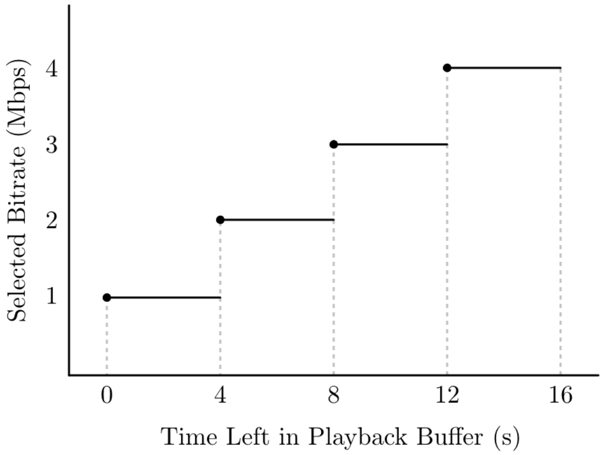

Figure 3: Image description: The video player chooses the bitrate of the next chunk to download, based on a step-wise function of the number of seconds left in the playback buffer. If the number of seconds in the playback buffer is x (in seconds), the chosen video bitrate will be: 1 Mbps if $0 \leq x < 4$; 2 Mbps if $4 \leq x < 8$; 3 Mbps if $8 \leq x < 12$ and 4 Mbps if $x \geq 12$.

4. [12 points]:

(a) How long does it take the video to start playing (startup time) in seconds?

Answer:

Rubric: 2 points

1 second. The first chunk is downloaded at 1 Mbps. 4 seconds × 1 Mbps = 4 Mb. At linkspeed of 4 Mbps, it takes 1 second to download a 4 Mb chunk.

(b) Please fill in the blank cells in the following table for the third and fourth chunks: when they start and end downloading, and the amount of video in the playback buffer when they start downloading (which affects the bitrate chosen to download that chunk). Please provide SPECIFIC NUMBERS as the answer, do not provide answers in terms of "Answer to (a)". We have included the first two rows as reference.

Chunk	Time Chunk Starts to Download (seconds)	Time Chunk Finishes Download (seconds)	Amount of video in buffer when chunk starts to download (seconds)
1	0	Answer to (a)	0
2	Answer to (a)	Twice the answer to (a)	?
3			
4			

Answer:

Rubric: 1 point per empty cell in row 3 and 4

Chunk	*Chunk Download Start time*	*Chunk Download End Time*	*Amount of video in buffer when chunk starts downloading*
1	*0*	*1*	*0*
2	*1*	*2*	*4 (not graded)*
3	*2*	*4*	*7*
4	*4*	*7*	*9*

(c) What bitrate will be used to download the third chunk?

Circle the best answer.

- **A** 1 Mbps
- [✓ **B**] 2 Mbps
- **C** 3 Mbps
- **D** 4 Mbps

Answer:

Rubric: 1 point
2 Mbps. The first chunk arrives at time $t = 1$, so the second chunk can start downloading at time 1, at 1 Mbps, and the first chunk can start playing at time 1. The second chunk finishes downloading at time 2, but by now, 1 second from the first chunk has played, so there are 7 seconds of video in the buffer. Thus, 2 Mbps is used for the 3rd chunk.

(d) What bitrate will be used to download the fourth chunk?

Circle the best answer.

- **A** 1 Mbps
- **B** 2 Mbps
- [✓ **C**] 3 Mbps
- **D** 4 Mbps

Answer:

Rubric: 1 point
The third chunk starts downloading at time $t = 2$, at a bitrate of 2 Mbps. It is 8 Mb large, so it takes 2 seconds to download, so it will finish downloading at time $t = 4$. At $t = 4$, when the fourth chunk is about to start downloading, there will still be 1 second of video in the buffer from chunk 1, the entire second chunk, and the entire third chunk, so a total of 9 seconds of video. So it will start downloading at a bitrate of 3 Mbps at time $t = 4$; it will be 12Mb large, so will take 3 seconds to download at 4 Mbps and finish downloading at time $t = 7$.

(e) Assume at some later time t, right before a chunk is downloaded, there are 12 seconds of video in the playback buffer, but Ben's link rate drops to 800 Kbps (0.8 Mbps). Assume Ben continues to use the same stepwise function to choose which bitrate to download video at. How long will the video stall while the next chunk is downloading? Here, stalling is defined as time when there is **no** video in the playback buffer (so the client player can't play anything).

Answer:

Rubric: 2 points

8 seconds.

If there are 12 seconds in the buffer, the chosen bitrate for the next chunk will be 4 Mbps. This means the next chunk is 4 Mbps × 4 seconds or 16 Mb large. At 800 Kbps (0.8 Mbps), this takes 20 seconds to download. Since there are already 12 seconds of video in the buffer, the resulting rebuffering time will be 8 seconds. (20-12).

V TLS

5. [8 points]:

You are connecting to https://www.youtube.com to watch some cat videos. Consider an attacker who is able to listen/modify/send all traffic between any user and YouTube at any link of the connection.

(a) If the attacker obtains a copy of YouTube's **certificate**, the attacker could:

Circle the best answer.

- **A** Impersonate the YouTube web server to a user (e.g., pretend to be YouTube and send CS144 lectures instead of cat videos).
- **B** Discover some of the plaintexts of data sent during a past connection between a user and YouTube.
- **C** Discover all of plaintext of data sent during a past connection between a user and YouTube
- **D** Replay data that a user previously sent to YouTube server over a prior HTTPS connection
- **E** All of the above.
- [✓ **F**] None of the above.

Answer:

YouTube certificate is already public, everyone can have it.

(b) If the attacker breaks into Google's datacenter[1] and obtains the **current private key of YouTube**, the attacker could:

Circle the best answer.

- **A** Impersonate the YouTube web server to a user (e.g., pretend to be YouTube and send CS144 lectures instead of cat videos).
- **B** Discover some of the plaintexts of data sent during a past connection between a user and YouTube.

---

[1] Do not do this.

C Discover all of plaintext of data sent during the current connection between a user and YouTube.

D Replay data that a user previously sent to YouTube server over a prior HTTPS connection

[✓ **E**] All of the above.

F None of the above.

Answer:

With YouTube's private key, the attacker can derive the current or past symmetric key based on TLS handshake and basically decode and encode any information.

(c) Following the previous question, YouTube suspects an attack. YouTube closes your connection and deletes the session key. You establish a new connection to YouTube, with YouTube presenting the same public key as before. Now, the attacker could:

Circle the best answer.

A Impersonate the YouTube web server to a user (e.g., pretend to be YouTube and send CS144 lectures instead of cat videos).

B Discover some of the plaintexts of data sent during a past connection between a user and YouTube.

C Discover all of plaintext of data sent during the current connection between a user and YouTube.

D Replay data that a user previously sent to YouTube server over a prior HTTPS connection

[✓ **E**] All of the above.

F None of the above.

Answer:

Since the private/public key pair is unchanged, the attacker can still do anything from previous part.

(d) Following the previous question, YouTube decides to change their asymmetric public-private key pair completely and get a new certificate. They close the connection, and you reconnect again (with YouTube presenting the new certificate). Now, the attacker could:

Circle the best answer.

A Impersonate the YouTube web server to a user (e.g., pretend to be YouTube and send CS144 lectures instead of cat videos).

[✓ **B**] Discover some of the plaintexts of data sent during a past connection between a user and YouTube.

C Discover all of plaintext of data sent during the current connection between a user and YouTube.

D Replay data that a user previously sent to YouTube server over a prior HTTPS connection

E All of the above.

F None of the above.

Answer:

Attacker cannot decrypt any further information. However, they still can decode things from previous traffic using the old key pair.

(e) If the attacker obtains the private key of a certification authority (CA) trusted by your Web browser, the attacker could:

Circle the best answer.

[✓ **A**] Impersonate the YouTube web server to a user (e.g., pretend to be YouTube and send CS144 lectures instead of cat videos).

B Discover some of the plaintexts of data sent during a past connection between a user and YouTube.

C Discover all of plaintext of data sent during a past connection between a user and YouTube

D Replay data that a user previously sent to YouTube server over a prior HTTPS connection

E All of the above.

F None of the above.

SUNetID: ___________

Answer:

The attacker cannot decrypt past data because they don't have YouTube's private key. They can use the CA key to create fake certificates which can fool the users to think that they are YouTube.

VI Lower Layers

6. [8 points]:

Recall Shannon's formula for the channel capacity (link rate) C for a channel with one sender and one receiver with additive white Gaussian noise,

$$C = W \log_2(1 + \tfrac{S}{N}),$$

where W is the bandwidth of the channel in hertz, S is the signal power in watts, and N is the noise power in watts.

(a) Imagine you have two links, link A and link B. Link A uses a frequency band of 100 MHz to 200 MHz. Link B uses a frequency band of 5 GHz to 5.1 GHz. The two links have equal signal and noise power. According to the formula, which link has a higher capacity?

Circle the best answer.

A Link A

B Link B

[✓ **C** Neither]

Answer:

These two links have the same bandwidth despite using different frequencies, since (5.1 GHz - 5 GHz) = (200 MHz - 100 MHz) = 100 MHz, so they have the same Shannon Channel Capacity.

(b) Imagine you have a wired link consisting of a copper cable wrapped in plastic insulation. You notice that the cable is affected by interference or noise from the environment (e.g., nearby power source, nearby wireless communications, cosmic rays, etc.), so you modify the link by adding additional plastic insulation and braided metal shielding to protect the cable from this outside influence. Which term in the formula would most be affected by this modification, and would it increase or decrease?

Circle the best answer.

A W, increase

B W, decrease

C S, increase
D S, decrease
E N, increase
[✓ **F**] N, decrease

Answer:

Adding shielding to protect the cable from interference would decrease the noise power, N, because there's less noise.

(c) Would the overall channel capacity increase or decrease from the change in part (b)?

Circle the best answer.

[✓ **A**] Increase
B Decrease

Answer:

Decreasing the noise power would increase the channel capacity. Intuitively, a link with less interference should be a better link for sending data. Symbolically, smaller N means larger S/N, means larger $\log_2(1 + S/N)$, means larger C.