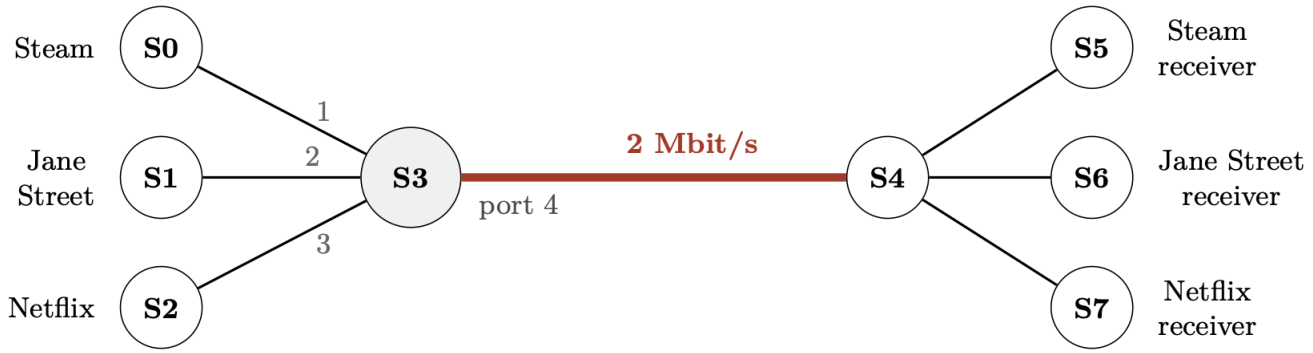
Quiz 2

You can ask the course staff any specific and factual questions you like during the quiz, and we will answer them! You are responsible only for reasoning, not knowing facts. Examples of factual questions include details of how an algorithm works, any formulas, and definitions of terms. Specific means that you need to know what question you may ask.
For essay questions, try to keep your answers as brief as possible while covering all the important points.

Question 1: Queue depth and delay

In A2 Part 1 you chose how deep each queue is. Here is what that choice costs Steam.

We run your team's A2 program on every switch below. S3 has the usual 40,000bytes buffer and 4 ports. All three customers leave S3 by the same port, the thin 2 Mbit/s link to S4. The table shows how each customer's sender reacts to loss and the most it will send. Your switch is told all of this.



Customer	Rule	Asks for
Steam	AIMD	no limit
Jane Street	AIMD	0.1 Mbit/s
Netflix	rate matching	0.6 Mbit/s

Steam's packets are 1,000 bytes.

Apart from waiting in S3's queue, a Steam packet's trip takes 7 ms.

1 Numeric 1 point

(a) What is Steam's queue limit on S3's port to S4, in packets? (If you drop early, give the drop line.)

Answer

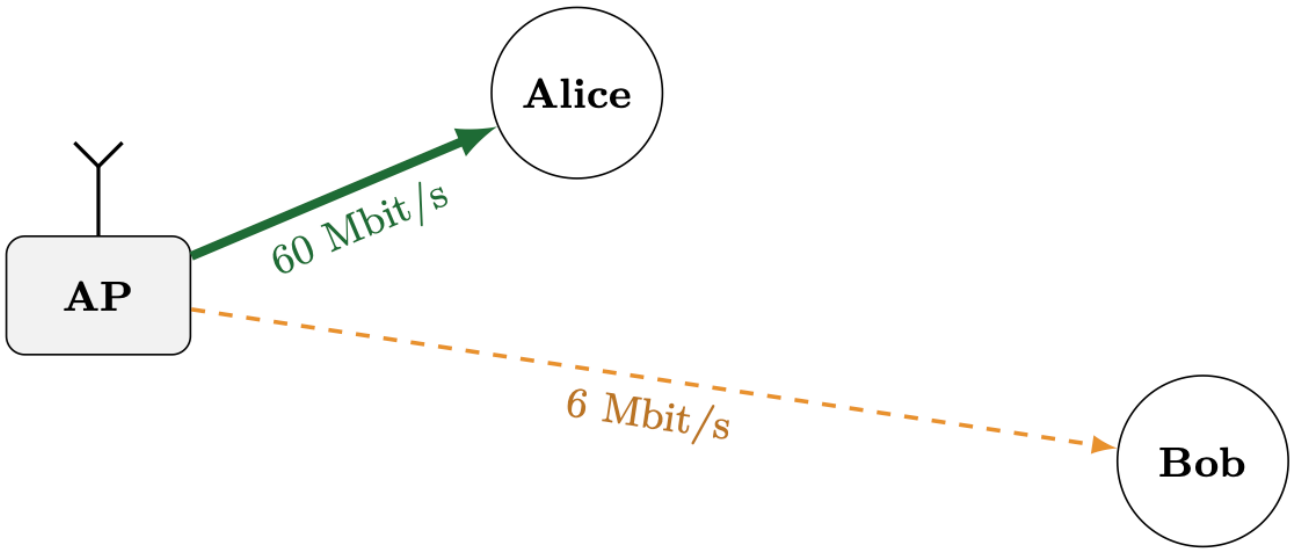
2 Numeric 3 points

(b) Assume Steam's sender keeps its queue at S3 full. How long does a Steam packet take to reach its receiver (ms)?

Answer

Question 2: Equal airtime (Wi-Fi)

Wireless media are shared: a Wi-Fi access point (AP) transmits to one phone per equal time slot, at 60 Mbit/s to Alice (close) or 6 Mbit/s to Bob (far). The AP always has data for both, and there is no overhead or loss. A phone receives data only during its own slots, so its throughput (its average bits per second) is its rate times the fraction of slots it gets.



3 Numeric 1 point

(a) If the AP gives both phones the same throughput, what does each get, in Mbit/s?

Answer

4 Numeric 1 point

(b) Now the AP splits its time evenly instead: half of every second sending to Alice, the other half sending to Bob. Call this equal airtime. What do the two phones get in total, in Mbit/s?

Answer

5 Multiple Choice 1 point

(c)(i) With equal airtime, Bob gets less than he gets with the same throughput.

- True
- False
- I don’t know (IDK)

6 Multiple Choice 1 point

(c)(ii) With equal airtime, if Bob moves closer and his speed rises to 12 Mbit/s, Alice gets more.

- True
- False
- I don’t know (IDK)

7 Multiple Choice 1 point

(c)(iii) If the AP sends one packet to Alice, then one same-size packet to Bob, and repeats, that is equal airtime. (A packet takes as many slots as it needs at that phone's rate.)

- True
- False
- I don’t know (IDK)

8 Multiple Choice 1 point

(c)(iv) With the same throughput, if Bob moves closer and his speed rises to 12 Mbit/s, Alice gets more.

- True
- False
- I don’t know (IDK)

Question 3: Authentication and secure encryption

Answer each part in at most 100 words.

9 Essay 3 points

(a) A stranger on the internet tells you: "I am Alice. This is my public key pk. Why don't you send me a challenge?" You send a random string r. They send back a valid signature on r made with the private key that goes with pk. Are you convinced you are talking to Alice? Start your answer with "Yes" or "No", then explain in at most 100 words.

100%

100 max (word limit)

10 Essay 3 points

(b) Consider the following definition of security for a symmetric encryption scheme, similar to what we discussed in class. An encryption scheme E_k(m) has an L-bit key k and takes as input an arbitrary bit-string to produce a cipher text (also an arbitrary bit-string). E_k(m) may be randomized function. It is secure if Bob cannot win the following game as L grows where Bob can only do poly(l) operations:

Stage 1 of the game:

Alice picks a secret key k
Bob sends a sequence of messages m_1, m_2, ... to Alice. She responds with E_k(m_1), E_k(m_2), ... in the same order

Stage 2 of the game
Bob picks two messages M_0 and M_1
Alice responds with either E_k(M_b) where $b \in \{0, 1\}$ is chosen randomly

Bob has to determine b with better chance than half [1] .

AES[2] does not meet this definition. Why? Answer in at most 100 words.

[1] More precisely, he wins if he can find the correct answer with probability greater than 1/2 + 1 / poly(L) for some polynomial

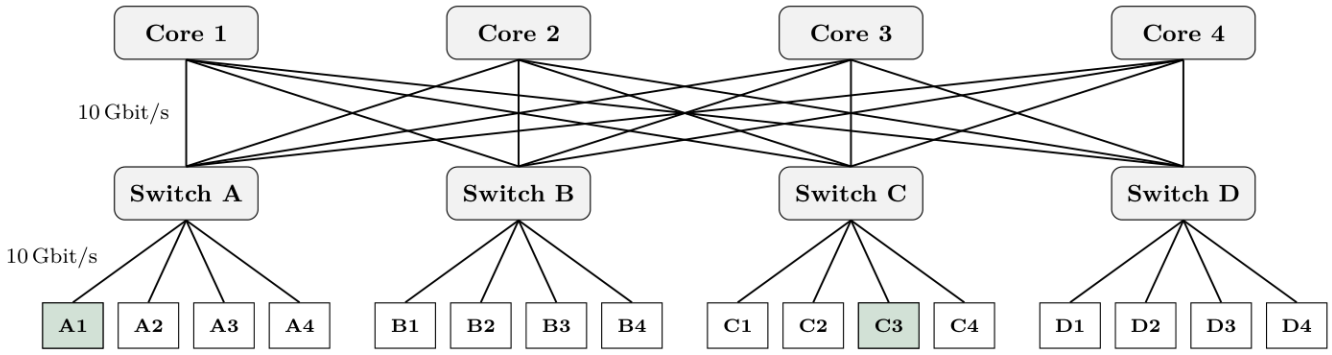
[2]AES using the block-wise encryption with random initialization vector as discussed in class

100%

100 max (word limit)

Question 4: Specialized congestion control

An AI lab trains its models on 16 computers in four groups of four (A–D). Each group has its own switch, and every group switch connects to each of the four core switches. Every link runs at 10 Gbit/s. All 8 switches, group and core, are the same kind: like your A2 switches, each queues packets only at its output ports, one FIFO queue per port; packets that don't fit are dropped. With empty queues, a round trip (Rm) takes 8 µs. Packets are 1,000 bytes.



Every link runs at 10 Gbit/s. A1 and C3 are one pair.

During training, every computer passes its results to exactly one other computer, and only that computer sends to it (A1 and C3 are one such pair). Training jobs start and stop all the time, so the pairs keep changing.

The routing team has pulled off a miracle. Every flow instantly gets the best route when traffic changes.

You are in the congestion control team. You could use something standard like AIMD. But the routing team has been insufferable after their spectacular success. They're egging you to do better. Can you? You may specialize for this exact topology.

11 Essay 4 points

Describe your design and why it is good. Answer in at most 200 words.

100%

200 max (word limit)

Q5. Where should we be fair?

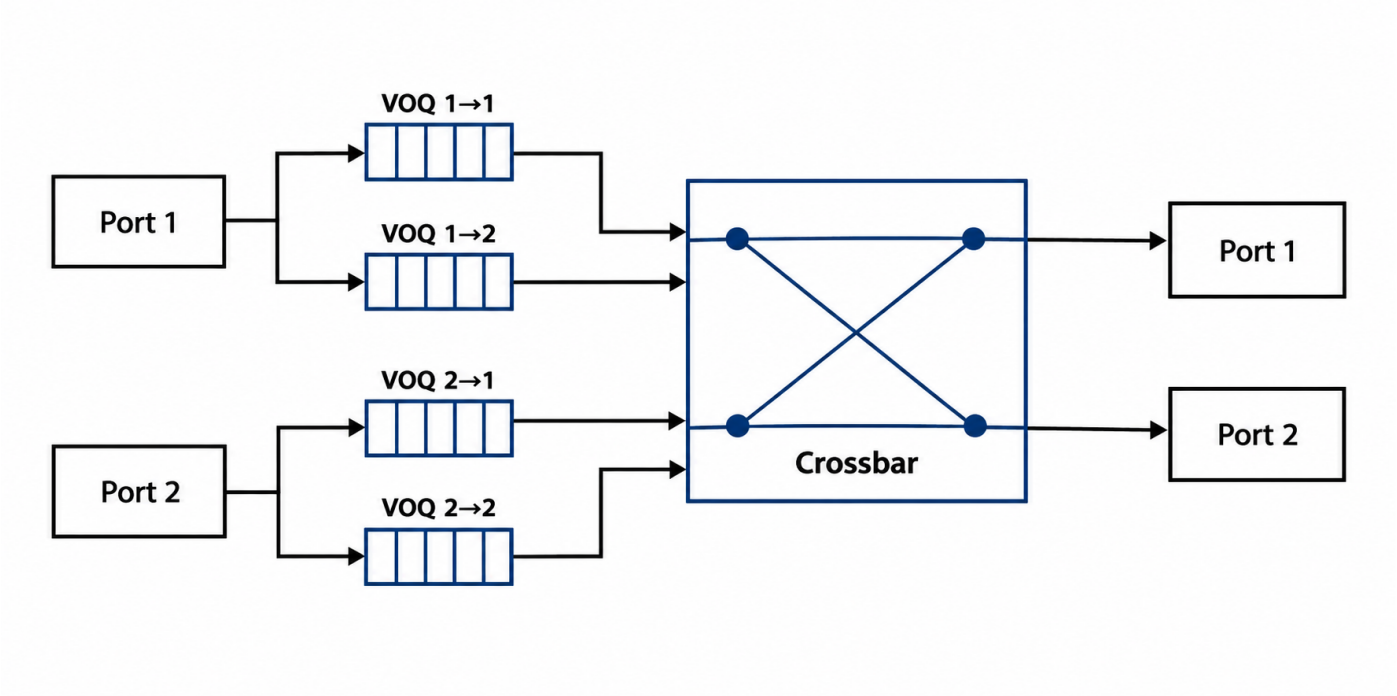
Consider a switch as shown below with two ports (each divided into an input and an output port). The ports and the crossbar all operate at the same speed (say 100 Gbit/s).

The crossbar is fair: Among all possible matchings, it chooses so that no input or output port is privileged.

We need to decide where to place the fair queues. A fair queue divides flows based on source and destination IP and serves packets equally from all the flows.

For each design, you must quantify the worst-case fairness. That is, you need to find the configuration of flows such that the ratio of the flow that gets the most throughput and the one that gets the least throughput is maximized.

Congestion control is perfect. That is, loss never occurs and flows are always able to keep several packets in the switch at all times, and hence are not disadvantaged due to the switch not having enough packets to send.



12 Essay 2 points

There is a fair queue only on the output queues

100%

200 max (word limit)

13 Essay 2 points

There is a fair queue on each of the Virtual Output QUeues

100%

200 max (word limit)

14 Essay 2 points

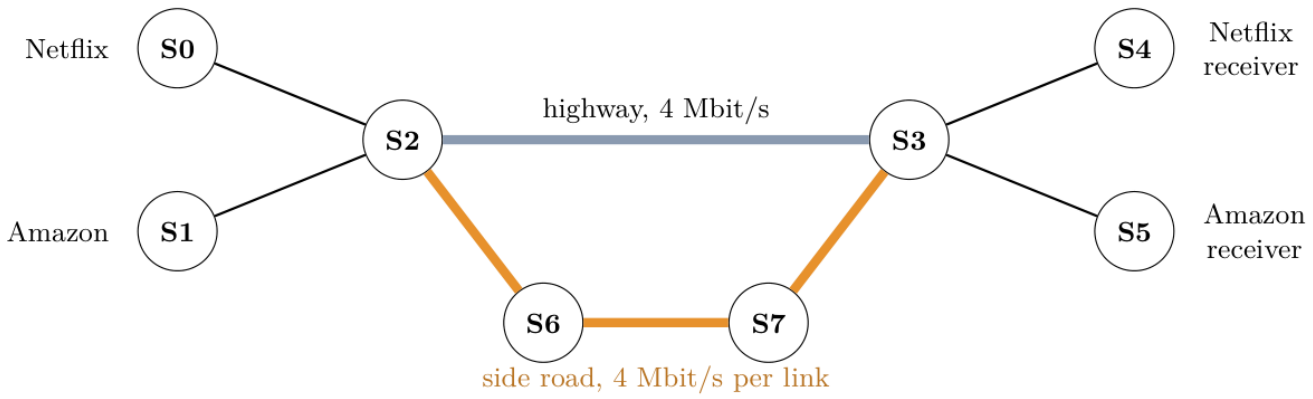
There is a fair queue on each of the Virtual Output Queues and the output queues

200 max (word limit)

Question 6: How fast does your network react?

In A2 Part 2 your program moved a customer onto the detour by calling `install_route`. This question asks **when** it makes that call.

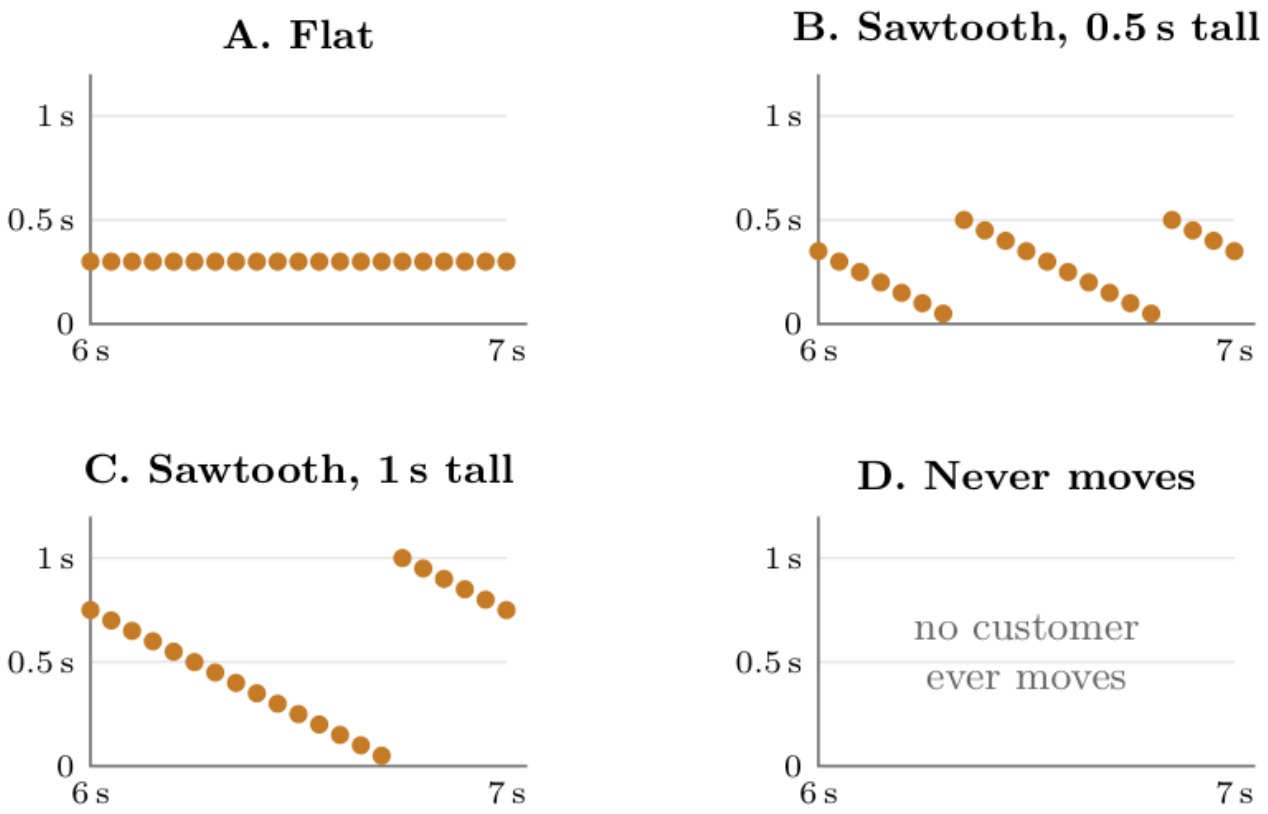
We run your team's A2 program on every switch below. Netflix sends from S0 to S4 the whole time. Amazon starts a **burst** from S1 to S5 about 6 s into the run. Both pass S2, and from S2 to S3 there are two roads: the **highway**, one link, and the **side road**, through S6 and S7. Every link on both roads runs at **4 Mbit/s**; every other link at 10 Mbit/s.



Customer	Rule	Asks for	Sends
Netflix	rate matching	2.5 Mbit/s	the whole time
Amazon	AIMD	3.0 Mbit/s	from the burst start

A customer is **on the side road** once almost all of its packets leaving S2 take the side road.

Your program doesn’t know when the burst starts, so it can start anywhere in your program’s timer cycle. We run your program many times, starting the burst at a different moment each time between 6 s and 7 s, and in each run measure the time from the burst start until a customer is on the side road. The graphs below plot that time against when the burst starts.



Each dot is one run. x-axis: when the burst starts in that run. y-axis: time from the burst start until a customer is on the side road. The dots can sit higher or lower than drawn; their pattern is what counts.

15 Essay 2 points

Which customer does your network most often move to the side road first?

A. Netflix
B. Amazon
C. Neither: both stay on the highway
IDK. I don't know (earns 0.25 points)

Type one letter: A, B, C, D or IDK.

3 max (word limit)

16 Essay 4 points

Which graph above is your program's?

A. Flat
B. Sawtooth, 0.5 s tall
C. Sawtooth, 1 s tall
D. Never moves
IDK. I don't know (earns 0.25 points)

Type one letter: A, B, C, D or IDK.

3 max (word limit)

17 Essay 0 points

Reasoning box (not graded)

100 max (word limit)