Exam - Final

Due: 2pm, 19 Dec 2016

Closed Book. Maximum points: 100

NAME:

There is a bonus item on question 2. Your grade will be min(100,total points).

1. Means to an end [16 pts]

When designing layered networked systems, we discussed a few principles to guide the placement of functionality (say, encryption, reliability, or ordering).

a. **Explain one reason why you would want to place functionality in a lower layer**. [4 pts]

b. **Explain one reason why you would want to place functionality in a higher layer**. [4 pts]

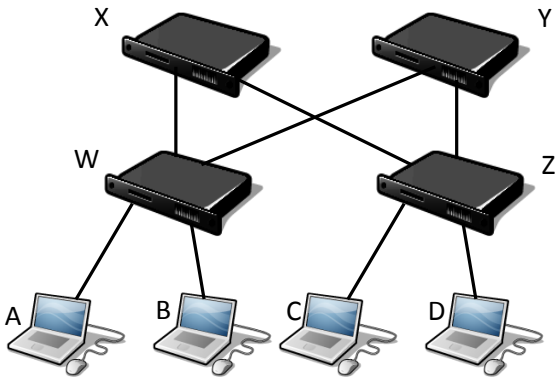
BitTorrent uses (i) hashes to verify the integrity of the entire file, and (ii) hashes to verify the integrity of each piece. BitTorrent can run on top of TCP, (iii) offers reliability as well.

c. **Which one of these mechanisms is strictly necessary?**[4 pts]

d. **Why then are the others there? Do they run counter to the end-to-end principle?**[4 pts]

2. Packet Spraying [24 + 8 (bonus) pts]

Suppose you have the following topology, where A, B, C, and D are switches, and all links are 10Gbps.



a. The spanning tree protocol is used in Ethernet to avoid broadcast storms. One problem with the STP is that we cannot use all of the possible bandwidth. After running the STP, if A wants to send to C, and B to D, simultaneously, **what is the maximum throughput each pair will get and why**? [8 pts]

b. To solve this, we can be smarter and not disable any links. One way is to introduce rules in switches W and Z to never broadcast packets that are coming "down" (from X or Y) back "up" (to Y or X). Assume we get all the details right (like suppressing duplicate broadcast packets), and can send packets on either path now: e.g., a packet from A to C can go through either switches X or Y.

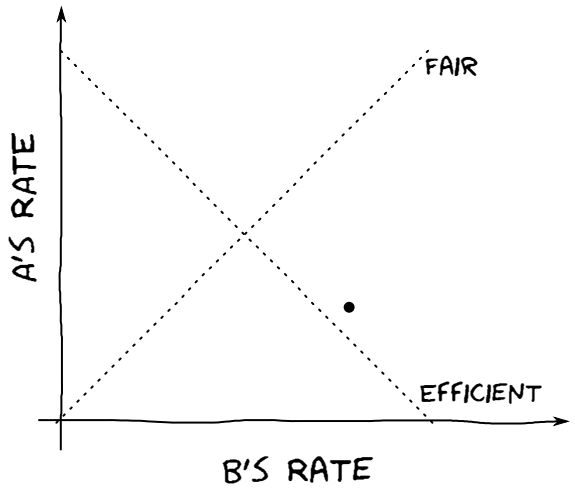
Suppose you change the switches to do this: for *every packet* it receives to the other rack, it *randomly* picks X or Y, and sends it through that switch. (This is called packet spraying.) By doing this, **what is the maximum throughput that each pair A/C and B/D can get and why**? [8 pts]

c. This strategy can have an adverse effect on TCP. Suppose that A and C have a TCP connection going on, and there is also traffic from other hosts. **Give a (perhaps unlucky) scenario in which TCP Reno halves its window without an actual loss, because of packet spraying.** [8 pts]

Bonus **Propose a scheme where, by changing the way the switch picks a top switch, the problem in part (c) does not happen.** Your scheme should work for any set of flows that any set of hosts on either side decide to send over the topology. Are there any downsides to your scheme? [8 pts]

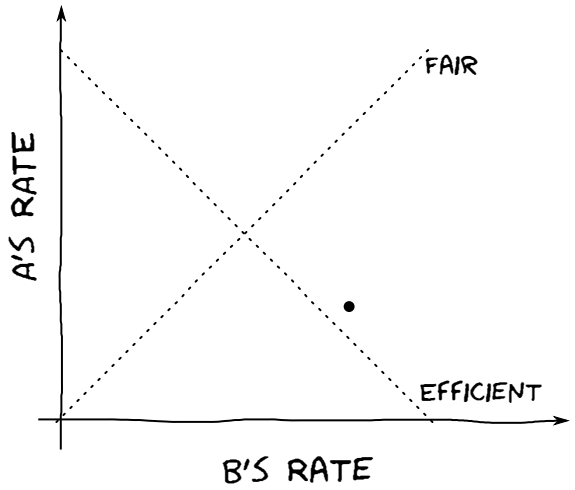
3. TCP Fairness [16 pts]

a. The figure below is the Chiu-Jain phase plot for two idealized TCP connections sharing a bottleneck link. **Draw what happens when A and B's rate start at the indicated dot** and both adjust their rates according to an identical and synchronized additive increase, multiplicative decrease (AIMD) scheme. [8 pts]



b. Briefly **describe one way (we discussed a few) in which A can get more bandwidth than B** and **draw the (approximate) corresponding diagram.** [8 pts]

Description:



4. Eavesdropping [24 pts]

Suppose Eve wants to eavesdrop on the communication between Alice and Sofia, where Alice is running a web browser and Sofia, a web server. Sofia serves her website over HTTPS, and Alice's browser happily accepts Sofia's certificate. Eve has access to all messages exchanged between Alice and Sofia, and can inject, change, or drop packets in either direction. She cannot, however, break encryption algorithms she doesn't have the key for.

a. **What is the condition on the signer of a TLS certificate for it to be accepted by a browser**? [4 pts]

b. For the items below, **say whether a TLS certificate contains the item, and why (what for) or why not**. [4 pts]

- Server's public key
- Server's private key
- Domain name of the server
- Revocation URL

Now Recall how a TLS connection is established, and answer the following questions:

c. Assume initially that Eve does not have access to any private keys or to certificates of her own. **What step of the TLS negotiation prevents Eve from eavesdropping on the communication?** (By eavesdropping we mean not only seeing the bytes of the communication, but understanding them.) [8 pts]

d. Now assume that Eve has stolen Sofia's private key, the one corresponding to the public key in Sofia's certificate. **Explain how Eve can read all of the communication between Alice and Sofia, by relaying the messages between the two**. [8 pts]

5. NAT Traversal [20 pts]

Suppose you are creating an simple chat client that works over UDP. In your design, there is a centralized, well known chat coordinator that maps your friends' names to their IP address and port number, and you can then directly connect to them. The server has an API that clients can use upon starting, to register their presence: `register(Name, IP, port)`. Before talking to a friend, a client looks up the name, gets the IP address and port, and proceeds to connect directly to the friend.

a. Now suppose Alice is behind a NAT, while Bob is not. They both register their IP addresses and desired port number with the server, and find that while Alice can connect to Bob, Bob cannot connect to Alice. **Why can't Bob connect to Alice?** (hint: just saying because Alice is behind a NAT isn't enough.) [4 pts]

b. After taking CSCI-1680, you solve this problem. **Describe a change in the original protocol that enables clients to talk to a friend behind a NAT**. List any changes to the API, the semantics of the call(s), and/or when they are made, to enable Bob to talk to Alice. [8 pts]

One issue when designing directories like your central server is that, to avoid many connections to the database, clients cache the responses. There are different approaches to handle this cached state: hard state (with cache invalidations by the server), and soft-state (with expirations, or TTL).

c. Like most Internet protocols (e.g., DNS, HTTP), you decide to go with a soft-state approach for your protocol. **Give one advantage and one disadvantage of using hard state**. [4 pts]

d. For your protocol, **what main factor(s) would you take into account to set the TTL?** [4 pts]

6. Feedback [0 pts] *These are optional, confidential, and not graded.*

a. What was the most useful concept you learned in this course?

b. What was the least useful concept you learned in this course?

c. What do you wish you had learned that we didn't cover?

d. Give one way in which we could improve the course in the future.

Thank you and have a great break (starting now!)