Exam - Final

Due: 5pm, 15 Dec 2018

Closed Book. Maximum points: 100

NAME:

1. IPv6 Deployment [14 pts]

One of the reasons it has taken so long to deploy IPv6 is that it requires widespread changes to a large part of the Internet infrastructure, protocols, and software. For each of the items below, say (i) whether or not they have/had to change to support IPv6, and (ii) why not, or what the change has/had to be.
To receive credit, you must provide an explanation. For all of the items, even if they support IPv6 today, consider change to mean change from their version prior to the existence of IPv6.

a. **Ethernet switch**: Would it change? ( ) yes ( ) no What change/why not?

b. **My laptop's operating system**: Would it change? ( ) yes ( ) no
What change/why not?

c. **An IP router in the middle of the network**: Would it change? ( ) yes ( ) no
What change/why not?

d. **The BGP protocol**: Would it change? ( ) yes ( ) no
What change/why not?

e. **The TCP protocol**: Would it change? ( ) yes ( ) no
What change/why not?

f. **A DNS nameserver**: Would it change? ( ) yes ( ) no
What change/why not?

g. **The HTTP protocol**: Would it change? ( ) yes ( ) no
What change/why not?

2. TCP / Congestion Control [22 pts]

a. In TCP, **what is the purpose of the three-way handshake**?

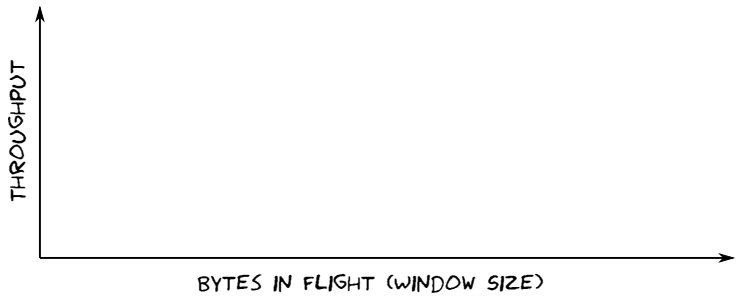
b. You have two applications, S and R, communicating over TCP. S has a lot of data to send to R. After they start, R stops reading from its socket. **Describe in detail how eventually S notices this, including what happens internally to TCP on both sides.**

c. Assume you have two TCP flows, A and B, sharing a bottleneck link. Both flows are in the congestion avoidance phase (AIMD). **Give three ways in which A could get more bandwidth than B, with a brief explanation for each.**

d. We looked in class at what happens to the RTT and the throughput of a TCP connection as the size of the window (bytes in flight) changes.

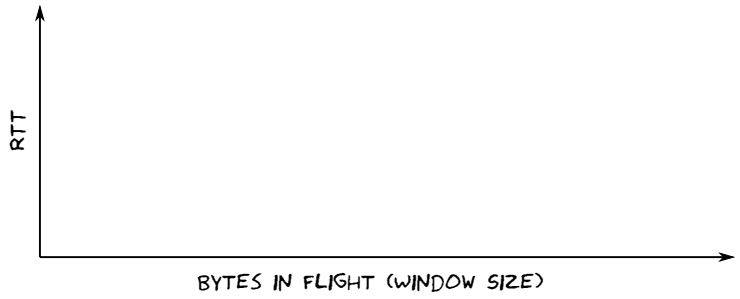
Draw the graphs of both quantities in the axes below. Indicate important values (such as constants), and inflection points. If there are linear slopes in the graphs, indicate the slopes.

Assume this is for a path with round trip time T and bandwidth B, and with a buffer before the bottleneck link of size Q bytes. Note that the x axis is **not** time!



PARAMETERS OF PATH:

NO-QUEUE RTT: T
BOTTLENECK BANDWIDTH: B
MAX BUFFER AT BOTTLENECK: Q



3. Party like its 1999 [22 pts]

You and a group of friends decided to celebrate the new year by playing the classic multiplayer game Unreal Tournament. The game uses a client-server architecture, in which players run clients, and the server coordinates the state of the game (such as the position of the players, the game map, location and status of objects, etc.) Clients connect to the server using UDP on a well-known port, hard coded to be 7777.

Since you took a networks class you were chosen to host the game server (it can't be harder than TCP, right?).

Each player (and your server) will be located in a different network, each one behind a NAT from their respective home routers. For this question, also assume that each one of you and your friends use different ISPs.

a. You start your server and look at the IP address in your machine, by running something like `ifconfig`. You tell them that your address is 192.168.1.14. They try to connect and it doesn't work. **Why not?**

b. You then remember some of your lectures from CS168 and see what was wrong. You connect to a(n honest) service `https://whatismyip.com` (not on your ISP) and it tells you a different (and correct) IP address. **How does this service know your IP address?**

c. The developers of the game understood that they can't expect the majority of players to know how to do what you just described, so they decided to build a system to allow players to connect to a server without knowing its IP address before hand. **If you were to design such a system, how would it work?**

d. The Unreal Tournament server listens on UDP port 7777. **Will regular hole punching work in this case? What do you need to do in your router to allow your friends to reach this port (assuming they know your IP address by c. above)?**

e. In 1999 there were estimated to be about 250M internet users, today there are over 4B users. Due to the large number of users, some ISPs have more customers than they have unique IP addresses, and deploy their own NATs. **If your ISP starts doing this, how can this affect your Unreal game?**

f. **If you were hired by the game manufacturer to make this work regardless of what the ISP were doing with respect to IP addresses, what would you do?**
State your assumptions, and assume you can do a lot, such as change the game software, run services on globally accessible servers, play with DNS, etc. Players *must* still run their servers and clients on their own home networks, and you can't tell ISPs what to do. (Be brief. We are just looking for an outline of your solution, not a complete protocol.)

4. DNS [22 pts]

a. Assume that you are writing your own DNS resolver (you don't like `dig`). **List the steps you have to take to resolve** `www.cs.brown.edu`, given that the only information you have is that on the root hints file (*e.g.* the address of a.root-servers.net.)

Assume the following information:

Name	IP Address	Zone	You have this already
a.root-servers.net.	198.41.0.4	.	✓
a.edu-servers.net.	192.5.6.30	edu.	✗
bru-ns1.brown.edu.	128.148.248.11	brown.edu.	✗
www.cs.brown.edu.	128.148.32.12	-	✗

Fill the first step below, and use the same format for the other steps. For each step, *query* is the main argument for the query (what you are asking); *server* is who you ask, which can be a name or an IP address. Each *answer* should have a type (NS or A) and the answer itself.

Step: 1
Query:
Server:
Answer Type: **Answer:**
…

b. Now let us sketch how a secure version of DNS would work. We are interested in signing answers we get from DNS, but not in encrypting them. In this design, keys will belong to a zone, not to a server (e.g., a key pair would belong to `edu.`, and all servers serving that zone would have the private key to sign for `edu.` For signing, any DNS server providing a response will have to sign the response with a private key, we know and trust the corresponding public key. Like in the TLS Public Key Infrastructure, we are going to have a chain of delegations, and assume that we have the public key for the '`.`' domain hard-coded (that is, we can verify and trust anything that the root server signs!) Unlike TLS, which creates its own hierarchy, we will leverage the DNS hierarchy instead: DNS servers will not have to change who they talk to when registering domains.

   For this to work, we will need to add some new information analogous to certificates to the DNS responses.

   For each of the responses in the DNS resolution to Brown in the previous question, describe what extra information has to be in the response, who is signing, and with what key.
   Recall that to trust a response (and, in particular our final response for www.cs.brown.edu), we need to have an unbroken chain of trust all the way back to the only public key we initially trust, the key for '`.`'.

   We are not worrying about invalidations, expirations, non-existent domains, or other details.

   Use the following notation for all steps:

   Step: 1
   Extra information:
   Who signs:
   What key:
   ...

5. TLS [20 pts]

a. **True or False**: In TLS, if a certificate authority in the authentication path between the server and the root CA is down during a request, the connection cannot proceed (ignore revocation checks).
True or False? Explain your reasoning.

b. What can an adversary do (who can they impersonate, and to whom) if they obtain one of the following: cnn.com's private key, the superfish private key (superfish is the Lenovo blunder we described in class where there was a program signing fake certificates of all sites), Verisign's private key (Verisign is a trusted root CA), or a friend working for a trusted CA from Molvania? **For each case, state the capabilities of an adversary in the table below.**

	Can impersonate	To Whom
cnn.com		
Superfish		
Verisign		
Friend at CA		

c. In TLS as we discussed, **how do we achieve bidirectional secure communication if there are only certificates for the servers**?

d. **What would we gain, if clients also had certificates that they would present to the server**?

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.