Exam - Final

Due: 4pm, 21 Dec 2014

Closed Book. Maximum points: 100

NAME:

You MUST to select 1 of the 5 questions to NOT be graded,
*****by marking it with an X by the question number*****

1. DNS [25 pts] Consider the following DNS resolution response:

```
; <<>> DiG 9.8.3-P1 <<>> www.bestbuy.com
...
;; ANSWER SECTION:
www.bestbuy.com. 2928  IN CNAME www.bestbuy.com.edgesuite.net.
www.bestbuy.com.edgesuite.net. 13689 IN CNAME a1105.b.akamai.net.
a1105.b.akamai.net.  18 IN A 23.67.244.115
a1105.b.akamai.net.  18 IN A 23.67.244.91
```

a. BestBuy is using Akamai to select servers that it *thinks* are close to you. According to the resolution above, this decision happens by the Akamai DNS server for `b.akamai.net`. **What does** `b.akamai.net` **assume to make this decision? When can it be wrong?** [7 pts]

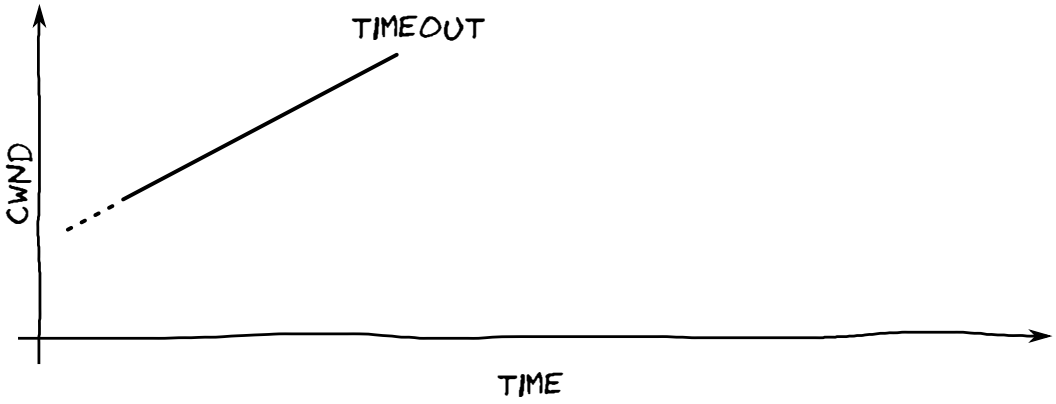
b. The number next to the names is the TTL of the DNS entries. **Why is the time for the bottom answers so small?** [8 pts]

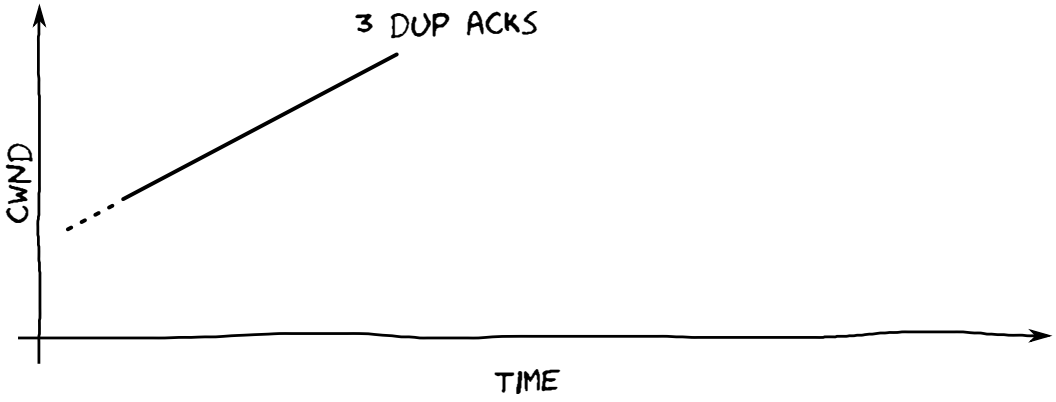
c. Dr. Evil wants to write a virus to attack the DNS infrastructure by altering DNS queries. He considers two options: the first option will randomly change the top level domain of any query: `www.facebook.com -> www.facebook.wx7p`. The second option will change the first subdomain of a query: `www.cnn.com -> 4rxrpt.cnn.com`. Suppose he infects a very large number of computers. Notwithstanding that this is a pretty lame virus, **which version of the virus is more effective in affecting the global DNS *infrastructure*?** Explain your reasoning in terms of the load imposed on different DNS servers. [10 pts]

2. TCP Congestion Control [25 pts]

a. TCP Reno introduced fast retransmit and fast recovery to TCP when the sender detects three duplicate acknowledgments. **Why are 3 duplicate acknowledgments a good indication that there has been a packet loss? Why is it a less severe type of loss than the one indicated by a timeout?**

b. Complete the diagrams for the window size behavior over time for TCP Reno when there is a timeout, and when the sender receives 3 duplicate acks. **Draw the line until the point at which the window size returns to the original size.** Indicate, if needed, whether you are in slow start or congestion avoidance mode, and what `ssthresh` is.





3. Eliminating Ethernet Broadcasts [25 pts] One of the main impediments for scaling Ethernet is the prevalence of broadcasts. MAC learning, ARP, and DHCP, which we have talked about, use broadcast messages for different purposes, but all due to lack of information about the network.

Your task is to eliminate such broadcasts from Ethernet using a distributed hash table. Assume that each switch in a large LAN has a unique id, and that the switches run a form of link state, such that each switch learns the ids of all other switches, and how to reach each one. Also assume that we are defining the program that runs on the switches (e.g., you can say that the switches will perform a lookup before forwarding a packet).

a. Describe how the switches can form a Consistent Hashing ring where we can store [key, value] pairs. (This is not Chord, as we can make the simplifying assumption that each switch knows about all others, and can reach any other switch through a shortest path.) Describe how to determine the switch responsible for a given key. [7 pts]

b. What are the keys and values we need to replace MAC learning and broadcast Ethernet messages destined to a single MAC address by the switches (i.e., the broadcasts switches do before they do MAC learning)? When are they read and written? [6 pts]

c. What are the keys and values we need to replace ARP broadcast messages? When are they read and written? [6 pts]

d. What are the keys and values we need to replace DHCP broadcast messages? When are they read and written? [6 pts]

(Curiosity: Note that this solution is cool, but requires the switches to be quite smart. In your SDN assignment you also pretty much eliminated broadcast, but the hash table (such as ARP and MAC learning) was implemented centrally in the controller, and the switches did even less!)

4. DNS Poisoning, a True Story[25 pts] A friend of mine called me the other day because she was a victim of a bank fraud in Brazil that caused her to lose some decent amount of money. To make a long story short, she visited a bank's web page (`www.bb.com.br`) and it presented her with a form that was actually coming from a malicious server, while embedded in the true bank's page. But it gets more interesting: this only happened when she used her home connection. When she accessed the bank's page on the same computer, but using a shared connection from her phone, she got the correct form.

The core of the problem was that the bank's main page was requesting a javascript program from `www56.bb.com.br`, which is in the same domain as the bank, but on a different server. Because of javascript's security policies, any script coming from a `*.bb.com.br` domain would be trusted to run on the `www.bb.com.br` page. The browser placed all trust on the fact that the IP address returned by the DNS resolution of `www56.bb.com.br` belonged to `bb.com.br`, which was not true.

She ran `dig www56.bb.com.br` on her computer while connected through her ISP and through her phone's shared connection, and indeed the IP addresses were different, the former not belonging to the bank. The fact that it was correct on the phone's network means that the problem was not in my friend's computer.

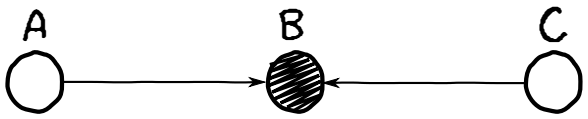
When connecting through the ISP, DHCP returned the cable modem as the DNS server for the computer to use, and usually the cable modem uses another DNS resolver in the ISP to do the resolution on its behalf.

a. How do you explain that the same domain was resolving to the wrong IP address only when connecting through her cable modem and ISP? Give two different ways in which the attacker could have caused the resolution to return the wrong answer. [9 pts]

b. Explain how if the bank had used DNSSEC it would have prevented this attack. What does DNSSEC allow us to say about a DNS response? [8 pts]

c. Explain how using HTTPS would have prevented this attack, i.e., what property of an HTTPS session would allow the browser to detect the attack? [8 pts]

5. Wireless [25 pts] Consider the wireless network in the diagram below, where the adjacent nodes can hear each other.



a. Describe what the hidden terminal problem is and how it manifests itself in this scenario. [9 pts]

b. How does RTS/CTS work to address the problem?[8 pts]

c. Why does RTS/CTS not completely solve the problem in all cases?[8 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!)