College of Computing

Georgia Institute of Technology

CS 6250: Computer Networking: Fall 2010

Quiz II

There are 14 questions and 10 pages in this quiz booklet (including this page). Answer each question according to the instructions given. You have **85 minutes** to answer the questions.

If you find a question ambiguous, write down any assumptions you make. **Be neat and legible.** If I can't understand your answer, I can't give you credit! There are three pretty challenging questions (clearly marked); you may want to look through the whole quiz and save those for last.

Use the empty sides of this booklet if you need scratch space. You may also use them for answers, although you shouldn't need to. *If you do use the blank sides for answers, make sure to clearly say so!*

Note well: Write your name in the space below AND your initials at the bottom of each page of this booklet.

THIS IS AN "OPEN NOTES, OPEN PAPERS" QUIZ.
NO OTHER MATERIALS, NO PHONES, NO COMPUTERS, NO LAPTOPS, NO PDAS.
MAKE SURE YOU'VE READ ALL THE INSTRUCTIONS ABOVE!

Initial here to indicate that (1) you've read the instructions and (2) you agree to abide by the Georgia Tech Honor Code:

The last page has easy bonus questions, *which you can answer outside of the allotted time*. Rip the last page off of your quiz for five bonus points. Turn it in anonymously if you like (feel free to fill it out after the quiz and give it to a TA, or take it with you). You won't get the five points if you don't tear off the page (this is to make certain you've read this far ;).

Do not write in the boxes below

1-5 (xx/20)	6-10 (xx/28)	11-13 (xx/13)	Bonus (xx/9)	Total (xx/70)

Name:

I Warmup

1. **[4 points]:** Which of the following is true about various measurement techniques?
(Circle ALL that apply)

   A. From a flow-level trace, one cannot compute the jitter experienced by the flow.
   B. Collecting flow statistics from a sampled packet trace may result in no statistics being gathered about small flows.
   C. From a flow-level trace, one cannot compute the average packet size for each flow in the trace.
   D. The ability to compute the round-trip time perceived by a client on one end of a TCP connection from a packet trace depends on where the packet trace was captured.
   E. All of the above.

Answer 1 The answer is: (A), (B). ■

2. **[4 points]:** Which of the following are true about spam filtering techniques?
(Circle ALL that apply)

   A. DNS-based blacklists are difficult to keep up-to-date because IP addresses of spammers keep changing.
   B. It is possible to send spam from a "spoofed" IP address.
   C. Most spam is sent from "spoofed" IP addresses.
   D. Most spam comes from botnets.
   E. None of the above.

Answer 2 The answer is : (A), (B), (D). (Some folks may not circle B, but it is technically possible with BGP route hijacking.) ■

3. **[4 points]:** Which of the following is true about data-center network architectures?
(Circle ALL that apply)

   A. The current Yahoo data center network design uses no IP routing.
   B. The VL2 design requires modifications to the host network stack.
   C. The VL2 design relies on Valiant load balancing to spread traffic across the aggregation switches.
   D. In Seattle, a host can discover the MAC address for a certain IP address by sending an ARP request.
   E. All of the above.

Answer 3 The answer is: (B), (C), (D). ■

Initials:

4. [4 points]: Which of the following is true about programmable network software and hardware?
(Circle ALL that apply)

A. Running a Click program in the kernel can speed up packet forwarding from running them in user space.

B. A RouteBricks cluster can achieve faster forwarding performance because packets never need to be forwarded across the PCI bus.

C. One of the major disadvantages of programming a custom data plane for the NetFPGA is that it is difficult to program.

D. One of the major disadvantages of programming a custom data plane for a Click software router is that the developer can only use the elements that the Click software distribution provides.

E. All of the above.

Answer 4 The answer is (A), (C). ■

5. [4 points]: Which of the following is true about BGP security and route hijacking?
(Circle ALL that apply)

A. If a route is hijacked, one can determine the party that is responsible for the hijack by looking at the origin AS in the AS path (i.e., the last AS in the AS path).

B. An attacker who hijacks a route can always be discovered using traceroute.

C. One of the main reasons S-BGP has not been deployed is that deploying it slows packet forwarding rates considerably.

D. One of the main reasons S-BGP has not been deployed is that it requires everyone to deploy it before any AS sees any benefits.

E. None of the above

Answer 5 The answer is (D). ■

Initials:

II Potpourri

6. [5 points]: Give a simple example where network tomography using end-to-end packet probes from multiple locations can isolate a link failure. Give *two* possible reasons why binary tomography might be inaccurate in practice.

(Answer legibly in the space below.)

Answer 6 A simple example here would illustrate something as in the binary tomography slides: For example, two end-to-end probes starting from the same source but going to two different destinations. If one end-to-end probe succeeded, but the other failed, you would know that the failure was on the link that corresponded to the failed probe, but not the other. (A picture here would be most illustrative.)
Binary tomography might be inaccurate in practice because failures might be mistaken for congestion, or because measurements of the reachability matrix may be inconsistent (e.g., due to re-routing during a failure event). ■

7. [4 points]: Give an example of an *intra-firewall inconsistency* where a subset of packets matched to the current rule would have been matched by a preceding rule that took a different action. How might such an inconsistency arise in practice?

(Answer legibly in the space below.)

Answer 7 One example of an intra-firewall inconsistency would be a rule that denied all packets from a $/16$ subnet, but then a later rule in the chain that allowed all packets from a $/24$ subnet contained inside of that original $/16$ (any such subnetting inconsistency where the smaller subnet contradicted the actions from the earlier subnet would be acceptable here). ■

Initials:

8. [6 points]: Consider the BGP routing table shown below like the one you saw in Problem Set 2, which contains a single route per prefix.

```
*> 8.14.0.0/19      143.215.254.25          0 2637 209 3356 46164 i
*> 8.14.0.0/20      143.215.254.25          0 2637 174 7018 46164 i
*> 8.14.16.0/20     143.215.254.25          0 2637 174 7018 46164 i
*> 8.14.38.0/24     143.215.254.25          0 2637 209 3356 53317 53317 i
*> 8.14.52.0/24     143.215.254.25          0 2637 209 3356 30016 i
*> 8.14.53.0/24     143.215.254.25          0 2637 209 3356 30016 i
*> 8.14.57.0/24     143.215.254.25          0 2637 174 33012 i
```

A. List two *contiguous* IP prefixes in the table that are advertised by the same origin AS.

B. What might be a reason that an AS advertises two contiguous prefixes?

C. List two *overlapping* IP prefixes advertised by the same AS.

D. What might be a reason that an AS advertises two overlapping IP prefixes?

E. List an AS path that uses *AS Path Prepending* in this table.

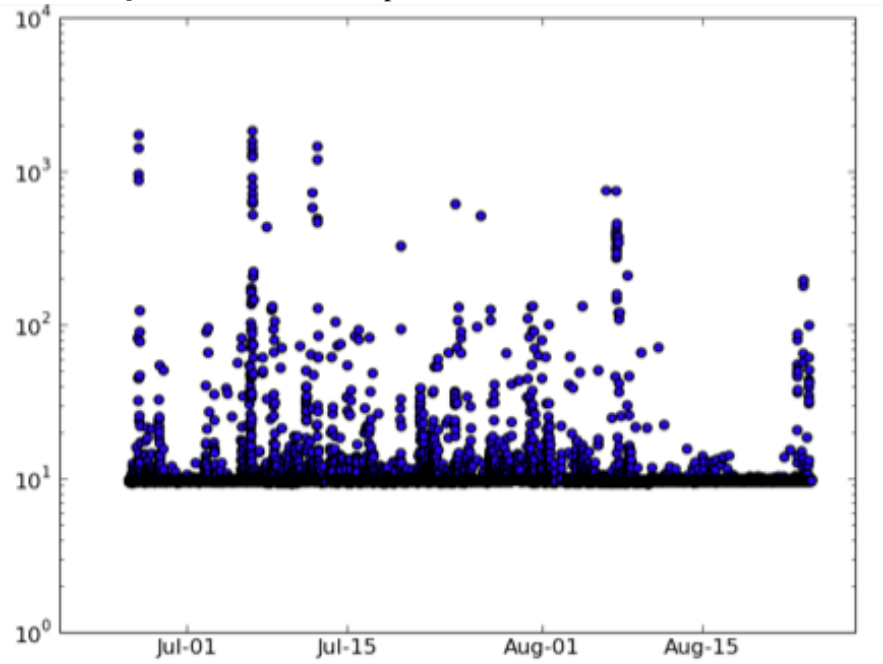
F. Each IP prefix in this table has only one route. Does that imply that AS path prepending did not have any effect on traffic flow along that path? Why or why not?

(Answer legibly in the space below.)

Answer 8 Two contiguous prefixes advertised by the same AS are 8.14.52.0/24 and 8.14.53.0/24. One reason that an AS advertises two contiguous prefixes would be for inbound traffic control for traffic engineering. Two overlapping IP prefixes advertised by the same AS are 8.14.0.0/19 and 8.14.0.0/24. One reason that an AS might advertise two overlapping prefixes is, again, for inbound traffic engineering. Another possible reason would be provider-based addressing (perhaps the AS has a downstream customer that is advertising this prefix via both this upstream AS, and another upstream). This second answer should likely only get half credit, since it is not quite feasible. An AS that uses AS path prepending is 53317. AS path prepending could have had an effect on the router that is directly upstream of this router, for example, so it is not correct to say that AS path prepending did not have any effect, even in this case. ■

Initials:

9. [5 points]: Consider the graph below, as seen in lecture, which shows samples of round-trip time latency for several months between an apartment in Atlanta and Georgia Tech, over a DSL link. The y axis shows round-trip time latencies in milliseconds.



A. Give *two* reasons why the latencies might vary drastically over time.

B. Assume that, when latency gets very high, uploads are inducing congestion on the access link that is causing the additional latency. Also assume that the uplink speed is 1 Mega*bit* per second. Suppose also that buffering at the first hop is imposing the delay, and that no packets are dropped. How large must the buffer on this first hop be, if packets are experiencing round-trip times of one second?

C. Why might access links use large buffers?

D. What is a disadvantage of using large buffers on the access link?

(Answer legibly in the space below.)

Answer 9 Latencies could vary over time due to congestion on the access link introduced by the user's own traffic (either uploads or downloads could cause buffering at the access link). Latencies might also vary due to congestion at otehr bottlenecks along the end-to-end path.

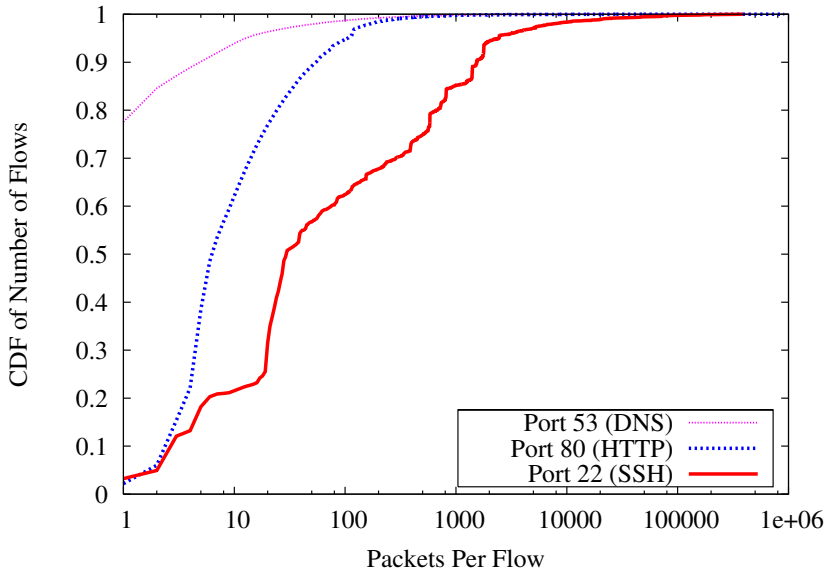
The buffer must be large enough to cause a one-second delay for some packets on a 1 Mbps link. So, that would be 1 Mbps times 1 second = 1 Mb.

Access links might use large buffers to help reduce packet loss. The disadvantage of such large buffering is that it can make it difficult to use interactive applications, since large variances in latencies could be introduced. An interesting recent discussion of this phenomenon is available here: `https://gettys.wordpress.com/2010/12/06/whose-house-is-of-glasse-must-not-throw-stones-at-another`

■

Initials:

10. [8 points]: Consider the following graph, which shows the flow-size distribution for flows captured on the Georgia Tech campus network in 2007.



A. Which protocol has the smallest median number of packets per flow?

B. What is the median number of packets for the protocol you named in part (a)?

C. Why are the flows for that protocol so small?

D. Which protocol has the largest number of median packets per flow?

E. Assume that this graph was generated directly from flow records "dumped" from a Cisco router, with no post processing of the flow records. From the lecture on flow monitoring, list *two* potential sources of inaccuracy that this graph might have. (In other words, why might the flow sizes be inaccurate?)

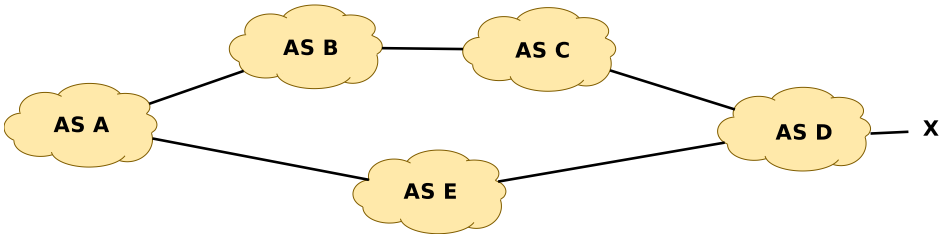
(Answer legibly in the space below.)

Answer 10 DNS has the smallest number of median packets per flow (one packet). The flows are likely small for that protocol because most DNS lookups can fit into a single packet. ssh, on the other hand, has a larger number of median packets per flow. Flow sizes might be inaccurate, particularly for ssh, because flow monitoring automatically "dumps" the flow records after (1) a period of "silence" (i.e., no packets); (2) after a fixed period of time, on a regular basis (i.e., once every 30 minutes). These can cause longer flows to be inadvertently broken up into smaller flows. ■

Initials:

III Design Question: Routing Security

For this problem, consider the AS diagram shown below. To indicate that message M is signed with the private key belonging to AS i, you may use the notation $\{M\}_i$.



11. [4 points]: Suppose that AS D advertises a route for IP prefix y to both AS C and AS E. Given equal local preference settings, AS A would select the route through AS E. Describe an attack that AS B could mount to try to "attract" traffic destined for IP prefix y.

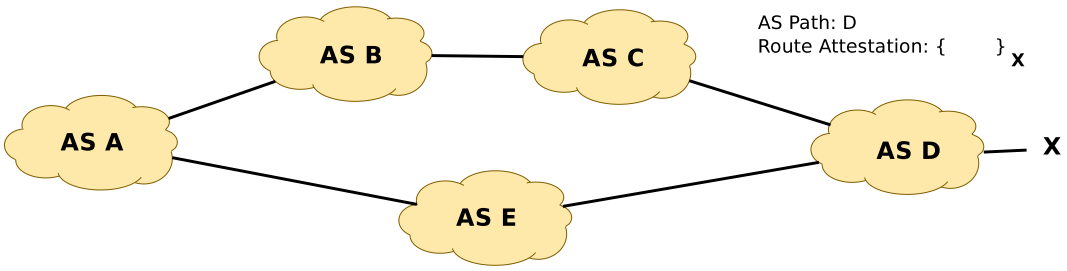
(Answer legibly in the space below.)

Answer 11 AS B could remove AS C from the AS path that it advertises to AS A for destination x, effectively having AS A see two AS paths of equal length—AED and ABD. If it treated routes from B and E with equal local preference, there is some chance that AS A might start sending more traffic through AS B as a result of this "path shortening" attack. ■

12. [4 points]: Suppose now that these ASes all deploy Secure BGP (S-BGP). Annotate the edges of the graph below to indicate *all* of the signed route attestations that each AS advertises along with the route. Use the notation recommended above: for example, $\{XYZ\}_W$ would indicate that AS W signed the AS path XYZ with its private key. *Hint: Be careful to sign the correct AS path; be careful*

Initials:

to defend against route shortening attacks.



Answer 12 Between AS D and AS C: AS Path: D, Route Attestation: $\{CD\}_D$
Between AS C and AS B: AS Path: D, Route Attestation: $\{CD\}_D$, $\{BCD\}_C$
Between AS B and AS A: AS Path: D, Route Attestation: $\{CD\}_D$, $\{BCD\}_C$, $\{ABCD\}_A$
Between AS C and AS D: AS Path: D, Route Attestation: $\{ED\}_D$
Between AS C and AS D: AS Path: D, Route Attestation: $\{ED\}_D$, $\{AED\}_E$

■

Initials:

13. [5 points]: George Burdell notes that, if a router should happen to reboot, it would have to sign hundreds of thousands of routes before advertising a full routing table to its neighbor AS, and the neighbor AS would have to verify the signatures on all of these routes. How might you design a scheme to speed up the process of signing and verifying advertisements for a full routing table's worth of route advertisements? (*Hint:* Think about some things that are common across routing advertisements.)

(Answer legibly in the space below.)

Answer 13 One possibility might be to have a *cache* of route signatures for each route attestation. You could, for example, cache the result of each signed route attestation, since the AS paths for the routes coming from a neighbor would likely be the same as they were before the reboot occurred.
One additional consideration with this approach is that caching old signatures could make the router vulnerable to a replay attack. So, a more robust solution would be to also include a timestamp with the route attestation, to prevent replay. (In fact, S-BGP's route attestations already include such a timestamp.) ■

14. [9 points]: *Bonus.* George also notes that S-BGP provides no mechanism for guaranteeing the authenticity of a BGP withdrawal message. Design a scheme that prevents at attacker from forging a BGP withdrawal message. Your solution need not be cryptographic. (Feel free to use cryptography, of course, but you could take other approaches; for example, you could use views of the Internet routing table from multiple vantage points.)

(Answer legibly in the space below.)

Answer 14 One simple approach would be to have the neighbor AS sign the BGP withdrawal messages, but that doesn't completely work, since the neighbor AS could actually withdraw a prefix for a network that is downstream. Really, you would need a scheme that allows the AS to determine *who initiated the withdrawal*, and that the *withdrawal was initiated by someone who has the right to initiate that withdrawal*. There's actually no good answer to this, because anyone could initiate the withdrawal of any prefix, for a variety of reasons (*e.g.*, an AS might withdraw a more specific route for traffic engineering reasons).
Two parts to the solution that should get credit are: (1) recognizing that a withdrawal could be originated from anywhere, not just the immediate AS neighbor; (2) somehow developing a scheme that attributes the BGP withdrawal to a particular AS (*not only the neighbor*). ■

Initials: