College of Computing

Georgia Institute of Technology

CS 6250: Computer Networking: Spring 2014

Quiz III

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**.

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! You may want to look through the whole quiz to identify which questions you can complete most quickly for the most points.

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 "CLOSED BOOK" QUIZ.
YOU ARE PERMITTED ONE DOUBLE-SIDED SHEET OF PAPER FOR NOTES.
ABSOLUTELY NO EMAIL OR MESSAGING OF ANY KIND!
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:

Do not write in the boxes below

1-5 (xx/20)	6-9 (xx/20)	10-12 (xx/40)	13-14 (xx/20)	Total (xx/100)

Name:

I Warmup

1. [4 points]: What are some advantages of separating the data and control planes, as in a software defined network (SDN)?

(Circle ALL that apply)

A. Independent evolution of data and control plane.

B. Less likelihood of failure.

C. Network-wide view of the state of forwarding elements.

D. Ability to control a network from a single, centralized software program.

E. None of the above.

2. [4 points]: What is the meaning of "parallel composition", in terms of Pyretic policies?

(Circle ALL that apply)

A. Apply each policy to the same copy of the packet concurrently.

B. Apply multiple policies to packets in sequence.

C. Make a copy of the original packet, then apply each policy to an independent copy of the packet.

D. Apply exactly one of the parallel policies to a copy of the packet, depending on which policy matches.

E. All of the above.

3. [4 points]: What does the Pyretic policy `match(srcip=A) >> fwd(2)` do?

(Circle ALL that apply)

A. For all packets that will be forwarded via output port 2, rewrite the source IP address to A.

B. Forward packets matching source IP address A via output port 2.

C. Rewrite packets matching source IP address A so that the virtual packet header for `outport` has the value 2.

D. Drop packets whose source IP address is not A.

E. All of the above

Name:

4. [4 points]: Which of the following are true about BGP routing security?
(Circle ALL that apply)

A. An AS can defend against route hijack attacks by filtering route advertisements for IP prefixes that neighbors do not own.

B. An AS can defend against AS path shortening attacks by filtering route advertisements for AS paths that it does not own.

C. In Secure BGP (S-BGP), an AS that advertises a route signs a version of the AS path that includes the next AS along the path (i.e., the AS to whom it is advertising the route).

D. Attackers can use short-lived BGP routing announcements to make it more difficult to trace certain types of attacks (e.g., spam, DoS).

E. None of the above

5. [4 points]: What are some mechanisms that can be used to implement censorship?
(Circle ALL that apply)

A. Blocking DNS requests.

B. Blocking TCP connections.

C. Redirecting URLs to a block page.

D. Withdrawing BGP routes.

E. None of the above.

Name:

II Potpourri

6. [5 points]: Define *origin authentication* and *path authentication*, in the context of interdomain routing security. Describe an attack that is possible without origin authentication, and describe an attack that is possible without path authentication.

(Answer legibly in the space below.)

7. [5 points]: Mininet uses virtual "containers" to create each virtual node in an emulated virtual network. Explain the difference between a virtual container and a virtual machine, and describe one advantage of using virtual containers over virtual machines for network emulation (as in Mininet).

(Answer legibly in the space below.)

8. [5 points]: One problem that software defined networks face is that of *consistent updates*. Define per-packet consistency and per-flow consistency. Give an example of incorrect behavior that can result if the network does not provide per-packet consistency, and an example of incorrect behavior that can result if the network does not provide per-flow consistency.

(Answer legibly in the space below.)

9. [5 points]: Explain what equal cost multipath (ECMP) is, and how it can be used in a data center to balance load across servers in a data center. (You may wish to draw a picture of a standard data center topology an explain where ECMP can be used to balance load across certain links.)

(Answer legibly in the space below.)

Name:

III Programming SDNs

10. [20 points]: In this problem, you will explore a few simple programs in Pyretic and PyResonance, applying what you learned in the lecture videos and problem sets. Consider the code sample below from the Pyretic examples, which performs simple MAC learning:

```
1  def learn(self):
2
3      def update_policy():
4          self.policy = self.forward + self.query
5      self.update_policy = update_policy
6
7      def learn_new_MAC(pkt):
8          self.forward = if_(match(dstmac=pkt['srcmac'],
9                                   switch=pkt['switch']),
10                            fwd(pkt['inport']),
11                            self.forward)
12         self.update_policy()
13
14     def set_initial_state():
15         self.query = packets(1,['srcmac','switch'])
16         self.query.register_callback(learn_new_MAC)
17         self.forward = self.flood
18         self.update_policy()
19
20     self.flood = flood()
21     set_initial_state()
22
23
24 def mac_learner():
25     return dynamic(learn)()
26
27 def main():
28     return mac_learner()
```

A. Explain the meaning of the `packets` statement (line 15).

B. Explain what line 4 does.

C. Explain why the `match` statement on lines 8–9 matches on a the `switch` field.

D. According to line 17, the initial `self.forward` policy is `flood()`. Upon the first callback to `learn_new_MAC`, `self.forward` is reassigned.

- Explain when this callback takes place.
- Suppose that a packet with source MAC address `ab:cd:ef:ab:cd:ef` arrives on input port `1` on switch `A`. Write the forwarding policy in terms of `match`, `fwd`, and `flood`, and explain how new packet arrivals cause the program to "learn" new forwarding behavior.

(Answer legibly in the space below.)
(You can use the back of the page as well.)

Name:

11. [10 points]: George Burdell wants to modify the learning switch to create a firewall, as you have done in the assignments. He adds the following functions:

```
1  def firewall(self):
2
3    def update_policy():
4      self.policy = self.policy + self.query
5    self.update_policy = update_policy
6
7    def initialize():
8
9      self.AddRule(1,'00:00:00:00:00:01')
10     self.AddRule(1,'00:00:00:00:00:02')
11
12     self.query = packets(None, ['srcmac'])
13     self.query.register_callback(check_rules)
14
15     self.policy = drop
16     self.update_policy()
17
18   def check_rules(pkt):
19     filter_on_mac(pkt)
20
21   def filter_on_mac(pkt):
22     if self.CheckRule(pkt['switch'], pkt['srcmac']) == True:
23         self.policy = passthrough
24     else:
25         self.policy = drop
26     self.update_policy()
27
28   initialize()
29
30 def main():
31     return dynamic(firewall)() >> dynamic(learn)()
```

Assume that `AddRule` adds a rule to firewall with ID `1` that permits packets with the source MAC address provided, that `CheckRule` checks for the presence of a permit rule at a switch for frames with the corresponding source MAC address, and that `learn` implements a simple MAC learner.

A. George starts his control program and begins to send pings between host 1 and host 2. The firewall passes traffic between these two hosts just fine. However, when he sends pings between host 1 and host 3, he notices that some traffic actually passes between these two hosts, even though there is no rule in the table for the host with MAC address 3. Why?

B. Briefly explain how you would fix the problem that George observes. (You don't have to write any code to receive credit, although you are welcome to if it makes your answer more clear.)

(Answer legibly in the space below.)
(You can use the back of the page as well.)

Name:

12. [10 points]: In a common SDN control program, if a packet arrives at the switch and the switch has no matching flow table entry for the packet, the switch must send the packet to the controller.

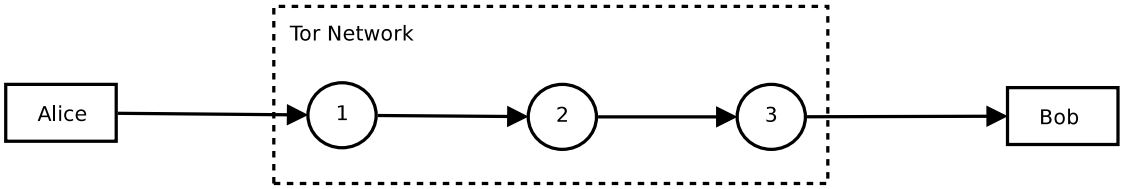
- Explain why sending data packets to the controller is not desirable.
- With advance knowledge of traffic patterns, it might be possible to avoid sending traffic to the controller. Describe a mechanism for handling as much traffic as possible in the data path. Mention possible scalability concerns with your approach, and possible ways to address them.

(Answer legibly in the space below.)

Name:

IV Censorship

13. [10 points]: Consider the figure below, which shows a Tor network, including a guard node, a relay node, and an exit node.



A. Which of the links in the diagram are encrypted?

B. Above each link in the diagram, write down the onion encryption for a Tor packet as it traverses the path from Alice to Bob, using the notation $\{M\}_{k_1}$ to indicate that the message M is encrypted with the public key of node 1. You can (and should) use nested encryption.

C. Explain how this mode of onion encryption makes it impossible for an intermediate relay in the Tor network to know either the sender or recipient of traffic.

D. Suppose that an attacker could observe traffic both entering and exiting the Tor network. What types of attacks could an attacker mount, in this case?

(Answer legibly in the space below.)

Name:

14. [10 points]: George Burdell notes that, with knowledge of the Tor relays, a censor could simply add firewall rules to block traffic to all of the IP addresses of Tor relays. Explain how you might design a client lookup service such that no single client can discover all Tor relay nodes.

(Answer legibly in the space below.)

Name: