Which of the following could be considered violations of route validity, as defined in the "rcc" lesson?



**Forwarding loops**

****

Network partitions



**Route hijacks**

****

**Blackholes**



Failed router hardware

1 point

2.Question 2

Which of the following could be considered violations of path visibility, as defined in the "rcc" lesson?



Forwarding loops



**Network partitions**



Blackholes



Router failures not answer



Route hijacks not answer

1 point

3.Question 3

Which of the following are true about configuration verification?



**Configuration verification cannot detect incorrect protocol behavior that may result from faulty hardware.**



**Configuration verification cannot detect incorrect protocol behavior that may result from buggy software**.



Configuration verification can only detect errors after the configuration is installed on production routers.



**Verifying the correctness of network behavior based on configuration requires a model of protocol behavior.**



Configuration verification requires a large-scale simulation of network protocols, complete with tests for different message orderings and timings.

1 point

4.Question 4

Which of the following assertions could be verified with configuration verification (i.e., of a snapshot of router and switch configuration)?



**A route learned from one peer will not be readvertised to another peer.**



Any time that an infection occurs, hosts are automatically quarantined.



**The configuration of route reflectors and clients ensures that any route learned from a neighboring AS will propagate to all routers in the topology.**

****

**The current settings of link weights will result in all routers being connected**.



There is no traffic pattern that would ever result in a stateful firewall dropping traffic.

5.Question 5

Which of the following are true about data-plane verification?



Data-plane verification requires accurate modeling of network protocols, including which bits are present in which part of the packet header.



Header-space analysis can only provide verification/analysis for specific packets; it cannot answer questions for general parts of flowspace.



**Data-plane verification techniques such as header-space analysis typically operate on a single "snapshot" of data-plane state.**

****

**Data-plane verification may detect errors that configuration analysis can miss in the cases of buggy control-plane software.**



Data plane verification can only operate on the forwarding table of a single router or switch; network-wide analysis is not possible.

1 point

6.Question 6

Which of the following assertions could be verified with data plane verification?



The network will remain connected, given the failure of at most two links.



**Two virtual network "slices" are not completely isolated: it is possible for traffic to travel from one slice to the other.**

****

**The rules installed on the firewalls in the network ensure that only port 80 traffic can ever reach the web server from the rest of the Internet.**

****

**The forwarding table state in the routers across the network will result in a forwarding loop.**



The configuration of the network's routing protocols will result in persistent oscillation (i.e., they will never settle on a stable set of routes).

1 point

7.Question 7

Which of the following is true about Kinetic policies?



The Kinetic controller can only process external events from routers and switches.



Kinetic's NuSMV verifier can verify that the data plane will never have loops.



**Pyretic's composition operators can help prevent state explosion.**

****

**State transitions can occur based on timing (e.g., a timeout).**

****

**State transitions can be exogenous or endogenous.**

1 point

8.Question 8

Which of the following policies could be implemented SDN dynamic control-plane verification (as in Kinetic)?



Ensure that no forwarding loops occur, even in the case of failure.



**If a host becomes infected, it should be redirected to a gardenwall.**

****

**If a host successfully authenticates, it should be allowed to send traffic to Internet destinations.**

****

**If a network experiences a surge in traffic volume to a primary web server, send flows from half of the incoming source IP addresses to the secondary web sever.**

****

**Ensure that forwarding table entries expire after a certain period of time.**

1 point

9.Question 9

Which of the following NuSMV expressions encodes the statement "It is always possible for the policy state to go to 'allow'."



SPEC AG (!authenticated -> AX policy=allow) not Answer



SPEC A [ policy=allow U authenticated ]



None of the above.



**SPEC AG (EF policy=allow)**



SPEC AG (authenticated -> AX policy=allow)

1 point

10.Question 10

Which of the following NuSMV expressions encodes the statement "The controller's policy should be 'allow' until 'infected' becomes true."?



FAIRNESS infected;Not Answer



**SPEC A [ policy=allow U infected ]**



SPEC ! AG (port=1 -> EX port=2)



SPEC ! AG A [ infected U allow ]



SPEC AG (!infected -> AX policy=allow) Not Answer