What are some benefits to using a layer-2 MAC topology for an entire data center?



Forwarding on physical MAC addresses is simpler, since both the data center network topology and hosts' physical MAC addresses are hierarchical.



**IP routing does not need to be reconfigured when physical or virtual machines move from one part of the network to another.**

****

**Host configuration is simpler, since all hosts are visible from a single large Ethernet topology.**



Scaling problems are simpler, since all hosts are configured on a single, flat topology.



Load balancing is easier on a layer-2 topology than on a layer 3 topology.

1 point

2.Question 2

In PortLand, what are the reasons for assigning hosts pseudo-MAC addresses, as opposed to simply forwarding traffic on physical MAC addresses?



**Without pseudo-MAC addresses, switches would have to update forwarding state whenever hosts with a particular MAC address moved from one portion of the topology to another**.



Forwarding loops are be more common in a flat layer-2 topology than they are in a topology with hierarchical pseudo MAC addresses.



Hosts in the data-center network topology are more vulnerable to attack if they expose their actual physical MAC addresses, rather than having a layer of indirection.



It is very difficult to load balance traffic using physical MAC addresses; pseudo MAC addresses make it possible to assign traffic to destination IP addresses.



**In a flat layer-2 topology, switches cannot know on which port to forward traffic without maintaining switch tables for each MAC address, since MAC addresses are flat, not hierarchical**.

1 point

3.Question 3

What are the steps involved in the Proxy ARP process that PortLand's Fabric Manager runs?



Host sends ARP query, fabric manager intercepts ARP query, consults PMAC mapping table and returns PMAC to end host.



**Host sends ARP query, edge switch intercepts query and redirects to the fabric manager, fabric manager consults PMAC mapping table and returns PMAC to edge switch, edge switch returns PMAC to end host.**



Host sends ARP query, edge switch intercepts query, consults PMAC mapping table and returns PMAC to the host.



Edge switch sends ARP query to fabric manager, fabric manager consults PMAC mapping table and returns PMAC to edge switch, edge switch updates its local PMAC mapping table.



Host sends ARP query, edge switch intercepts query and redirects to the fabric manager, fabric manager consults PMAC mapping table and returns returns PMAC directly to the end host.

1 point

4.Question 4

What are some of the disadvantages of today's interdomain routing protocol, BGP?



ISPs cannot express preference of one route over another, given multiple routes to a destination.



ISPs cannot load-balance traffic across multiple routes to the same destination IP prefix.



**ISPs can only influence the routing decisions of their immediate neighbor, not the entire end-to-end path.**



**ISPs can only influence route selection through indirect mechanisms (e.g., prepending), rather than directly manipulating the forwarding table entries in switches.**



**Routing and forwarding decisions are only based on IP prefix, not on a broader range of traffic flow attributes.**

1 point

5.Question 5

Which of the following statements are true about the virtual SDX abstraction?



The virtual SDX abstraction makes it more difficult to implement BGP-based load balancing at the exchange, since all traffic is being exchanged using layer-2 forwarding.



**An ISP will not see another ISP in its virtual SDX topology unless it has some business relationship with that ISP.**



Each AS at the exchange sees the same virtual SDX abstraction.



**The virtual SDX abstraction allows an AS to express policies at the exchange, even if it has no physical presence at that exchange and carries no traffic to or from the exchange.**

****

**The virtual SDX abstraction is implemented using symbolic execution and attaching "states" to IP packets as they arrive on physical ports at the exchange**.

1 point

6.Question 6

From the discussion of both SDX and B4, what are some of the claimed benefits of deploying SDN to handle wide-area traffic?



Better security, since only one controller needs to be protected from attack, as opposed to control software on all routers.



Better reliability, since the SDN software undergoes a more rigorous testing process than hardware routers.



**Faster failure convergence, since iteration through intermediate, non-functional paths can be avoided.**



**Better debugging and testability, since production control systems are separate from the data plane and hence can be emulated more easily.**



**Better load balance properties, since a single controller can see the complete view of the traffic matrix and topology.**

1 point

7.Question 7

What are some of the features that an SDX enables that today's IXPs cannot support?



Wide-area load balancing using DNS-based redirection



**Application-specific peering**

****

**On-the-fly redirection to middleboxes**

****

**Wide-area load balancing using IP packet rewriting**



Application of different business relationships across different regions of the world (e.g., peering only in a specific geographic region).

1 point

8.Question 8

Suppose that the SDX has 10 AS participants. What is the minimum number of times that sequential composition needs to be applied to create the resulting policy for the entire SDX?



10



1



100



1000



3 not Answer

1 point

9.Question 9

What are some of the motivations for applying software defined networking in home networks?



**Ability to better user interfaces to control home network behavior, independent of the interfaces that ship with home router devices.**

****

**Outsourcing control and management of the home network to a third party.**

****

**Ability to allow multiple service providers access to the home network infrastructure for different applications and services.**

****

**More fine-grained control over the forwarding behavior of individual devices as conditions in the network change (e.g., a device uses too much bandwidth or data).**



Better performance, since control decisions can be made from a well-provisioned server, as opposed to an under-provisioned router.

1 point

10.Question 10

Suppose that an operator of a home network wants to write the following policy:

1. Block all traffic to Facebook from my child's computer.

2. Rate limit BitTorrent traffic from my child's computer if the VoIP client on my desktop is active.

Which of the following most closely approximates the policy? Assume that "facebook" represents Facebook IP addresses, that "bittorrent" represents BitTorrent ports, and that "limitifVOIP" is a dynamic policy that checks a Resonance-like state machine to determine whether VOIP traffic has recently been observed.



(match(srcip=child, dstip=facebook) + drop) + (match(srcip=child, dstport=bittorrent) + dynamic(limitIfVOIP))



**(match(srcip=child, dstip=facebook) >> drop) + (match(srcip=child, dstport=bittorrent) >> dynamic(limitIfVOIP))**



(match(srcip=child, dstip=facebook) >> drop) >> (match(srcip=child, dstport=bittorrent) >> dynamic(limitIfVOIP**))**



(match(srcip=child, dstip=facebook) + drop) >> (match(srcip=child, dstport=bittorrent) + dynamic(limitIfVOIP))

1 point