Exercise 3 – SDN and Virtualization

1. FlowVisor (65P)

Consider the network topology shown in the figure below. It connects two sites of a Wide Area Network (WAN), where each site represented by a single OpenFlow switch, s1 and s4, respectively. The sites, s1 and s4, have two paths between them:

a low bandwidth path via switch s2
a high bandwidth path via switch s3

s1 has two hosts attached: h1 and h2. s2 has two hosts attached: h3 and h4.
The provider of the WAN now wants to dedicate certain links to certain applications within the network. In particular, the provider wants to create a *video slice* that handles the video traffic, and a *non-video* slice that handles the remaining, non-video traffic. Each slice will be controlled by a different controller (non-video by controller c1, video by controller c2). The video traffic (sent over TCP port 1234) should be forwarded over the high-bandwidth links, while the non-video traffic (all other ports) should be forwarded over the low-bandwidth links. A visualization of such a slicing is shown in the figure on the next page.

a. (20P) Please indicate the flows paces that FlowVisor will set up to realize these slices.

Consider h1 to h4 non-video traffic, s1 will ask controller where to go, FlowVisor will check the policy, then send this message to c1, then c1, will give s1 a rule that traffic from port 3 with port other than 1234 will be forwarded to port1. In s2, s2 will send message to controller, this message will be intercepted by FlowVisor, and check the policy, then send to c1. C1 will tell s2 forward all traffic from port1 to port2. When s4 receive that packet, it will ask controller, then this message will be intercepted by FlowVisor, after FlowVisor checked the policy, the message will be sent to c1. C1 will add a rule that traffic from port 1 with destination 10.0.0.4 will be forwarded to port 4.

In the same way, all messages will be intercepted by FlowVisor sent to the controller who has responsibility of that traffic. Controllers will add corresponding rules to the switches, and all the rules sent to switches also will be intercepted by FlowVisor to check the policy. If it not obeys to the policy, the message will be rejected.

b. (25P) Based on the slices created in a, which of the following statements are true? Give reasons for your answer.

a. (5P) Controller c1 is allowed to install the following rule in switch s2: Forward all incoming traffic on port 2 with TCP port 80 and source ip 10.0.0.3 (h3) via port 1

True, c1 in charge of s2 and can control all ports

b. (5P) Controller c1 is allowed to install the following rule in switch s3: Forward all incoming traffic on port 2 with TCP port 1234 via port 1.

False, the video traffic slice through s3 will not be affected by c1, c1 cannot see s3

c. (5P) If the link s1-s3 is down, video traffic with TCP port 1234 can no longer be forwarded from h1 to h4

True, TCP port 1234 only belongs to the video traffic slice, c1 does not have permission to add a rule for traffic from TCP port 1234, because the slices are not overlapped.

d. (5P) FlowVisor will return an error to controller c2 if c2 tries to setup the rule “forward all traffic with source-IP 10.0.04 (h4) via port 2” on switch s4.

True, because c2 only can control the packet with port 1234.

e. (5P) It is impossible to create such a virtualized network with traditional networking techniques.

True, because in traditional network, in data-link layer switches can only see the MAC address, switches do not know the TCP port number, and in transport layer, it cannot see the port in the switches.

c. (20P) FlowVisor has to process the so-called *new flow messages,* i.e., those messages that have to be forwarded to the controller in case of a table-miss at a OpenFlow switch. Here, FlowVisor has to determine the correct recipient controller of these messages before forwarding the new flow message to that controller.

In the figure below, we see that this operation incurs an additional 4 to 5 ms to the latency of these requests in FlowVisor, when compared to an OpenFlow network without FlowVisor. Do you think this amount of overhead is a criterion that could limit the usefulness of FlowVisor? Why?

It depends on the network application, if the application no need to divide virtual networks, and the traffic is complicated and changes a lot, then FlowVisor will only bring latency to that system.

If a network application has many virtual networks for different customers, the overhead is acceptable, and after the rules are installed the latency is as the same as OpenFlow.

2. CoVisor (35P)

a) (10P) Please explain the main difference between FlowVisor and CoVisor

FlowVisor allows controllers to work on disjoint slices of traffic only.

CoVisor allows combinations of parallel, sequential and override operators, and let multiple controllers work on the same traffic .

b) (10P) What is the main reasoning behind CoVisor’s incremental solution to policy computation?

Compare with decrement solution, for computation overhead it does not need to recomputed entire switch table. It only need to compose the new rules. For rule-update overhead, it does not need to change the priority of rules, when updating rules, it just add the new rules.

c) (15P) How does the incremental solution differ for the three composition modes of CoVisor?

Add priority for parallel composition.

Concatenate priorities for sequential composition

Stack priorities for override composition.