Group 7 – Malicious flows quarantine

Scenario: consider a network scenario wherein computing nodes (either clients or servers) are connected through an SDN-based network. A flow is identified by a pair client-IP server-IP. The network controller exposes a RESTful API allowing external users to mark/unmark a flow as malicious. When a flow is marked as malicious, the controller must reroute the traffic belonging to said flow, towards a dedicated switch, such as the red one in figure 1. The latter sends the packets of the malicious flows to the controller, which in turn buffers them up to a certain quantity, called *quarantine size*. When a malicious flow is unmarked, the controller configures the network to stop the rerouting and can be configured to either a) send the packet in the buffer towards their destination or b) drop all the packets in the buffer. These operations are called *buffer flush* and *buffer clear* respectively.

Detailed objectives:

1. Implement a Floodlight module that exposes a RESTful API allowing: 1) Marking a flow as malicious and configure the corresponding quarantine size, 2) unmark a flow and flush its buffer, 3) unmark a flow and clear its buffer, 4) request the total number of packets currently buffered for a given flow.
2. Implement a Floodlight module that implements the behavior above.
3. Test and demonstrate the overall system using mininet and Floodlight. The scenario of Figure 1 can be used as an example.

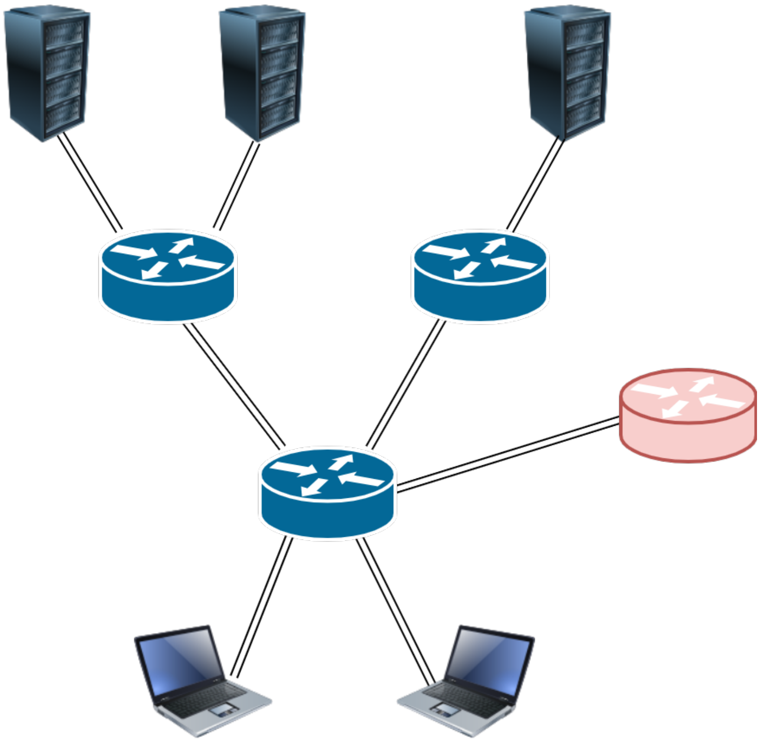

Figure 1