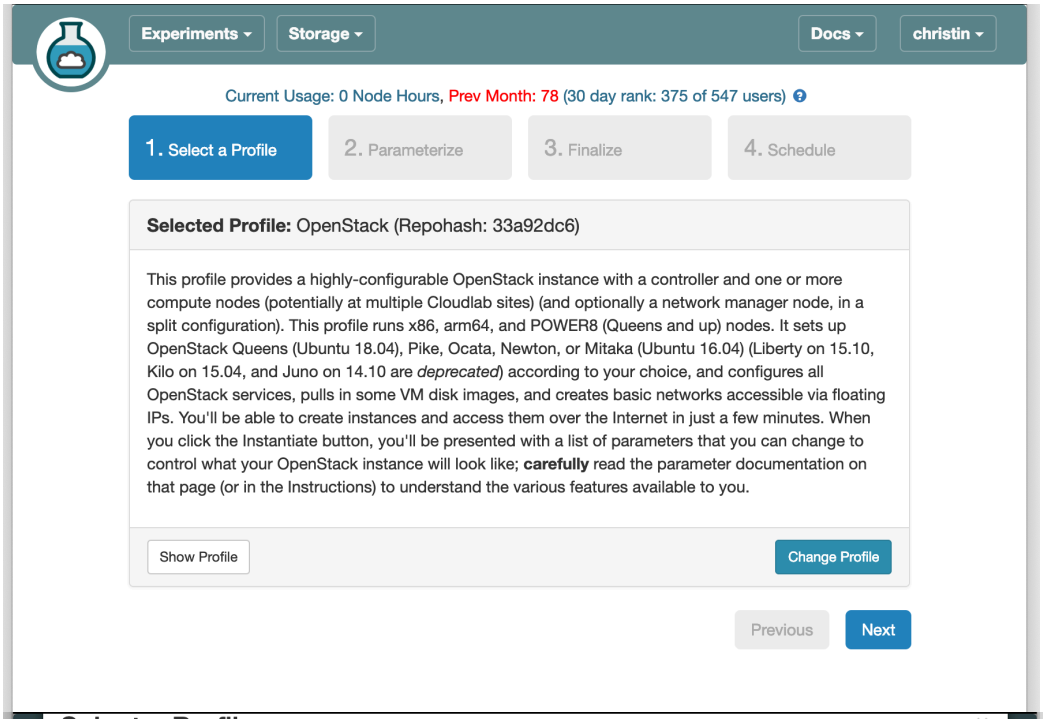
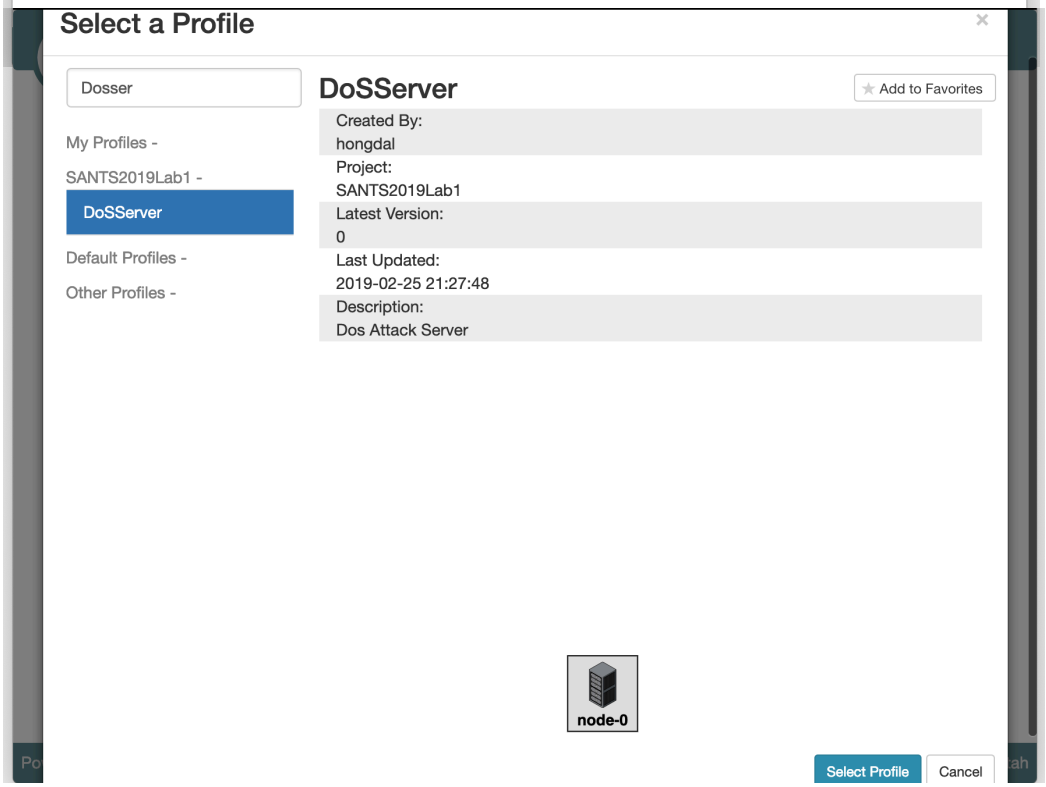
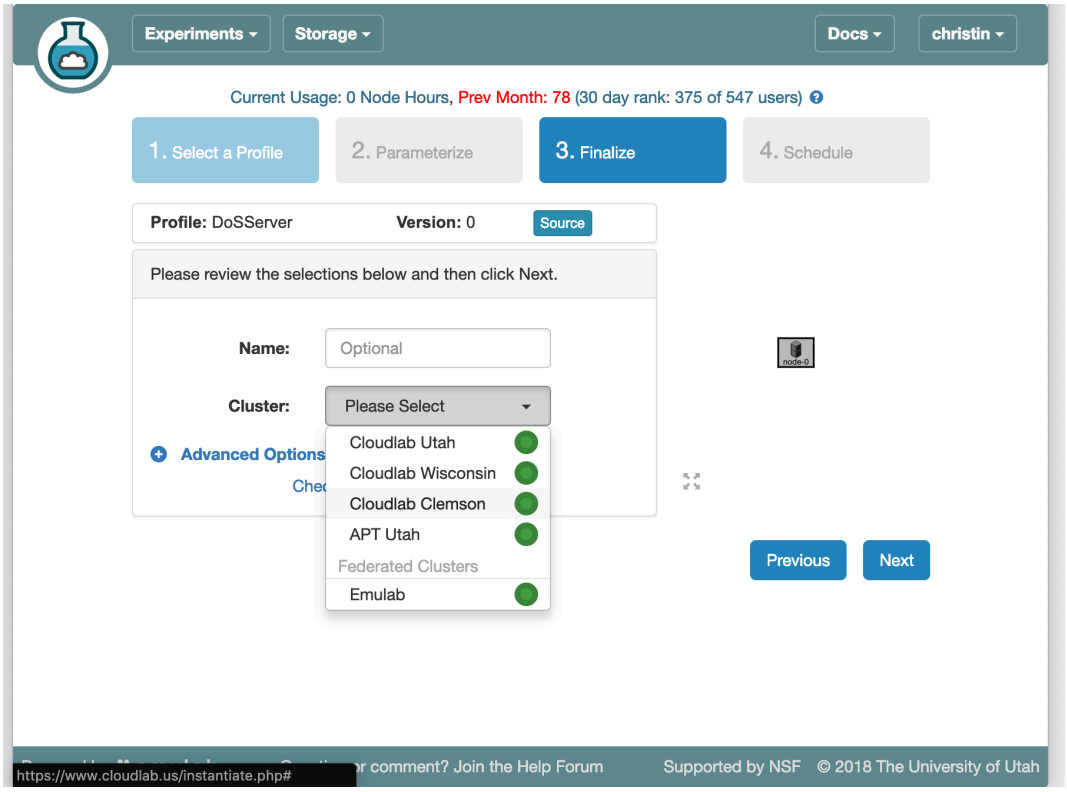
Project 2: Flooding Attacks to the SDN Data Plane

Submitted by Christin Wilson

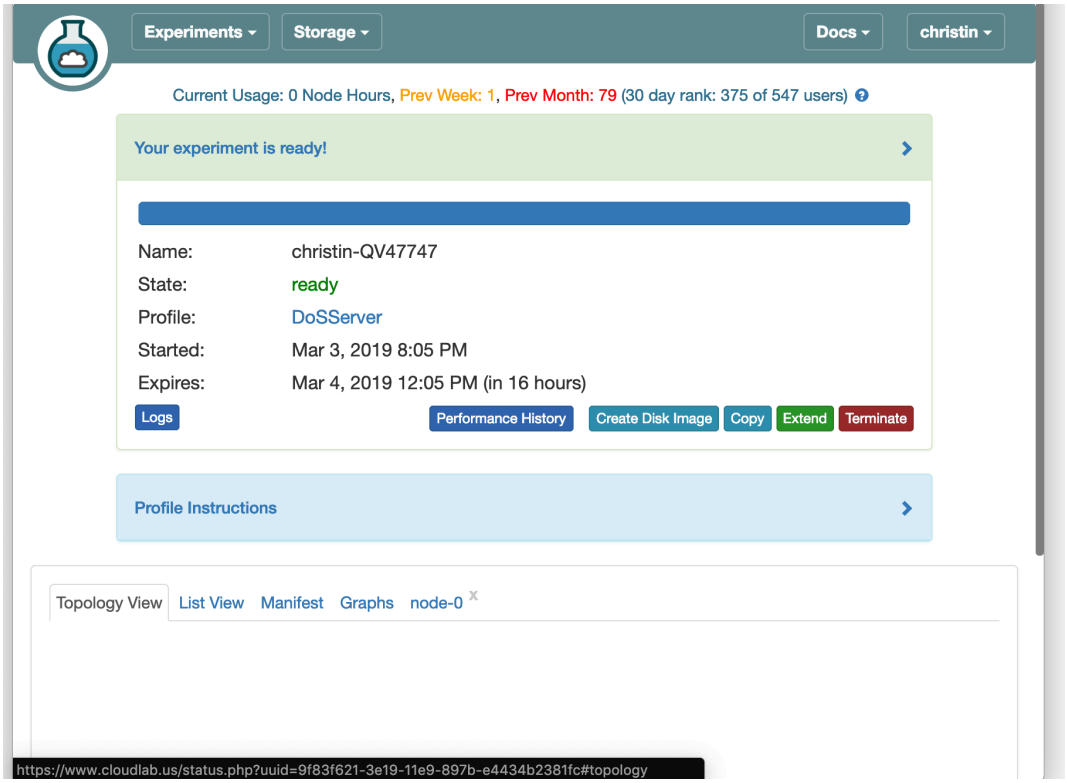
1. Started a new experiment and the profile used is “DoSServer” and instantiated it on the clemson cluster.



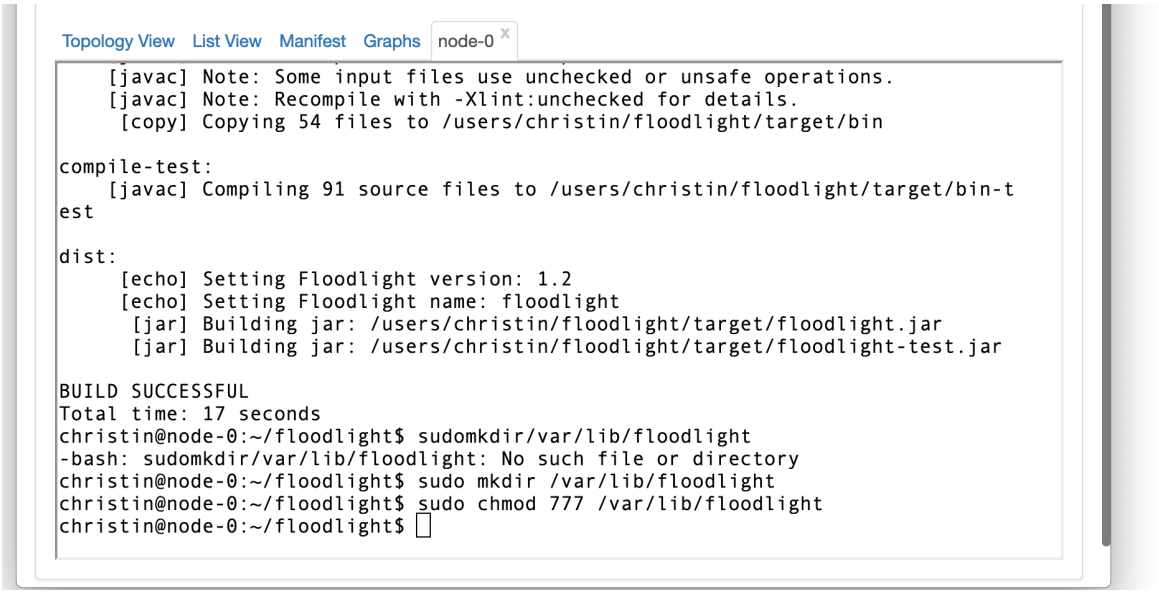


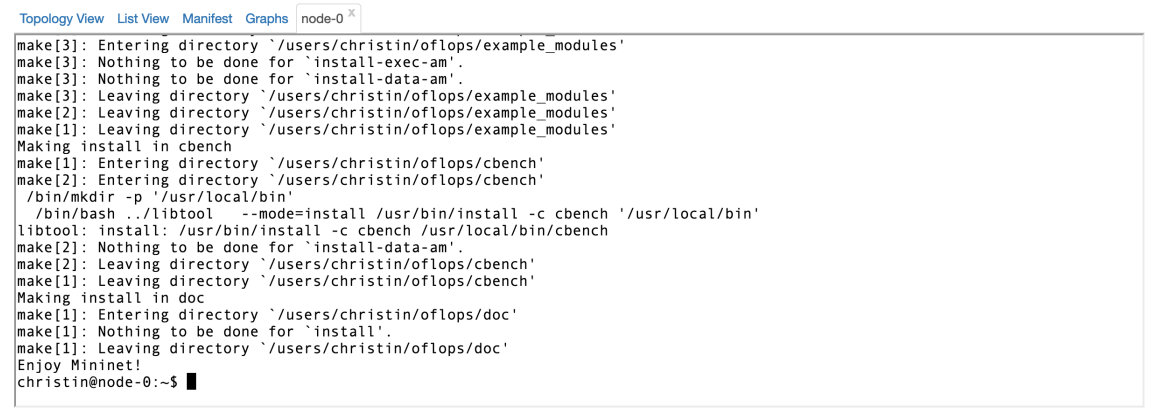


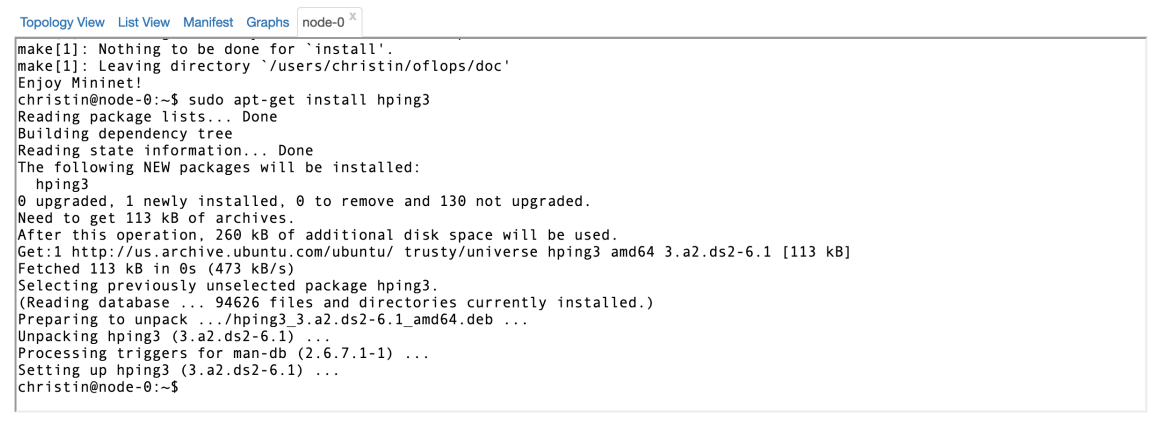
2. The experiment booted up and started running in some time.



3. Installed the dependencies on the node-0 of the experiment. The dependencies are mininet, floodlight and hping3.

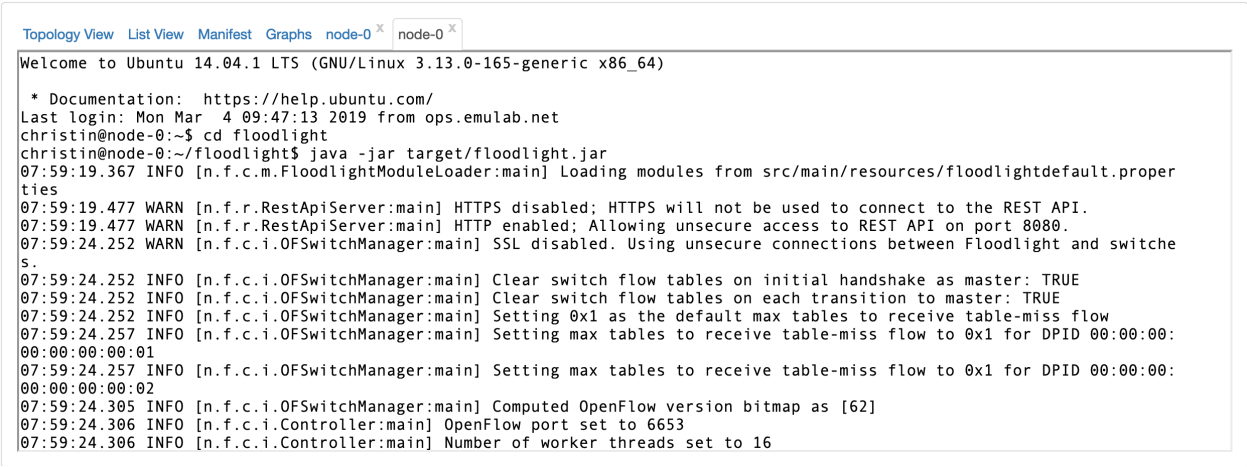




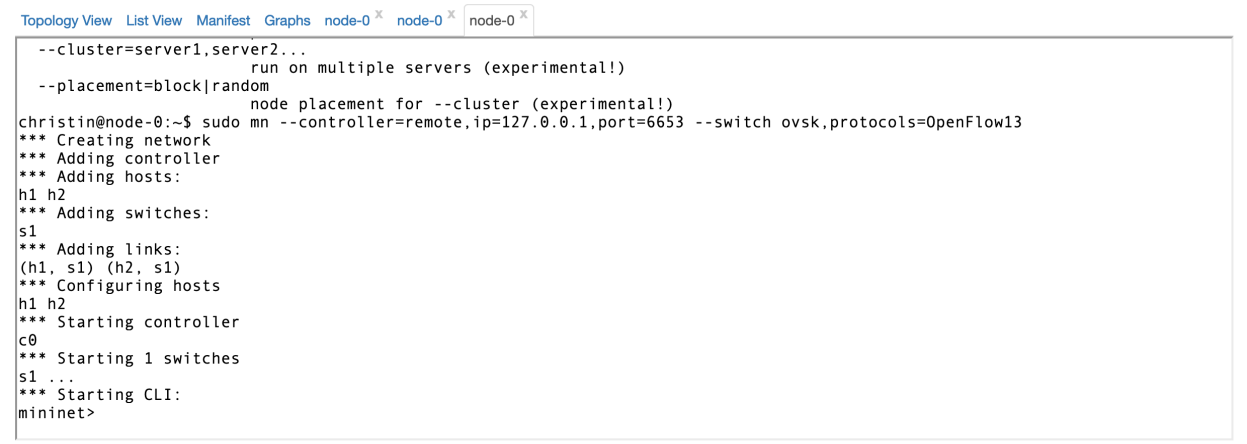


I used the set of commands and not the script to install the dependencies.

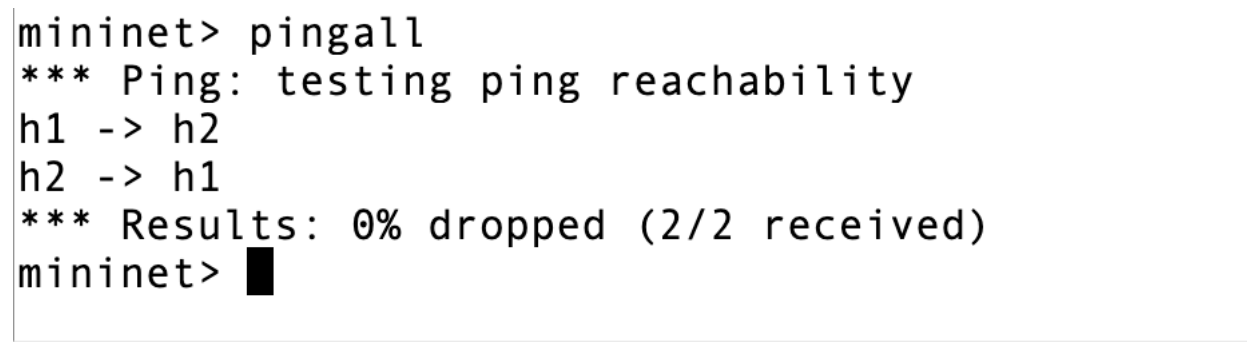
4. Opened a new shell for node-0 and started running the floodlight using ‘java -jar target/ floodlight.jar’



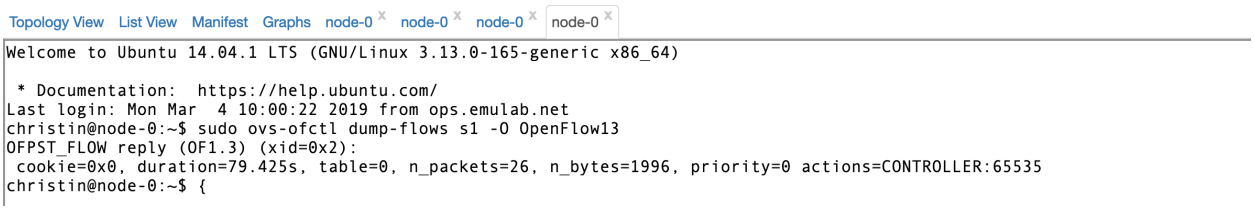
5. Opened another shell terminal for node-0 and I run a Mininet topology with 2 hosts that are connected by an OVS bridge switch and the bridge is connected to controller based on the IP address 127.0.0.1 and using port 6653 using
‘sudo mn —controller=remote,ip=127.0.0.1,port=6653 --switch ovsk,protocols=OpenFlow13’



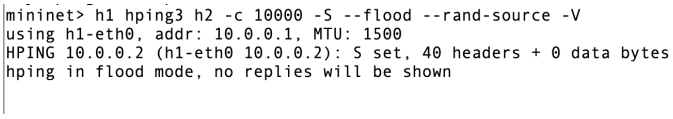
6. Confirmed that the hosts are reachable to each other using ‘pingall’



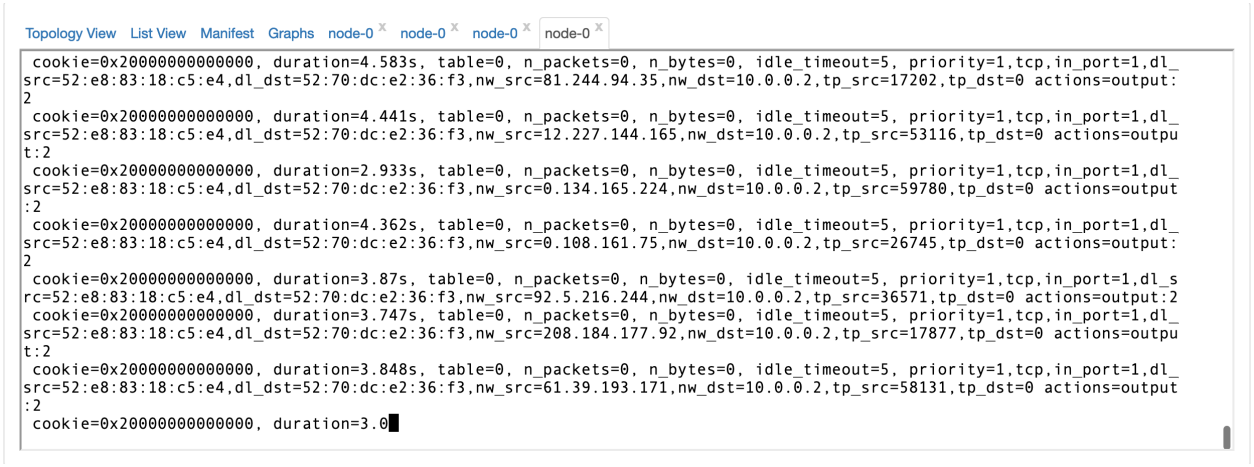
7. Opened a new shell terminal for node-0 and printed the current flow-rules inside switch using “sudo ovs-ofctl dump-flows s1 -O OpenFlow13’. We got just one rule now.



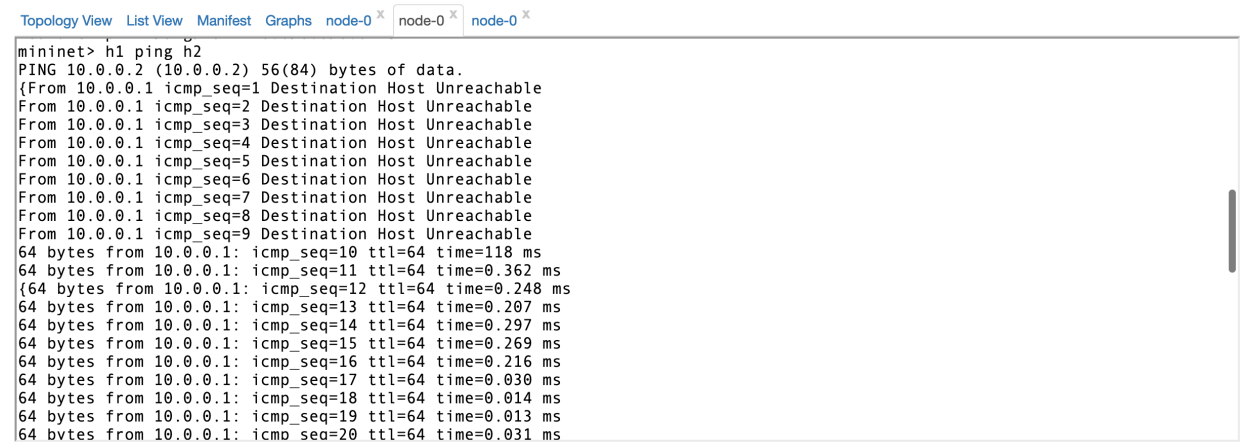
8. Opened the mininet terminal and flooded a lot of packets to h2 using ‘h1 hping3 h2 -c 10000 -S –flood –rand-source -V’



Now, the output obtained while checking the flow entries in the switch s1 is:



9. hping3 is stopped on the Mininet terminal. We Ping h1 from h2. We experience that it fails initially and then later the time taken is very high and then the time decreases drastically afterwards.



10. Now once again we check the flow table rules of OVS Switch S1

Thus a denial of service attack is being exhibited here. This happens due to the resource exhaustion which results in the switch not being able to receive instructions to install a flow entry.
So when the flow table of OVS switches is full, additional flow-rule installations will fail due to insufficient space in the flow table.