CMPE210

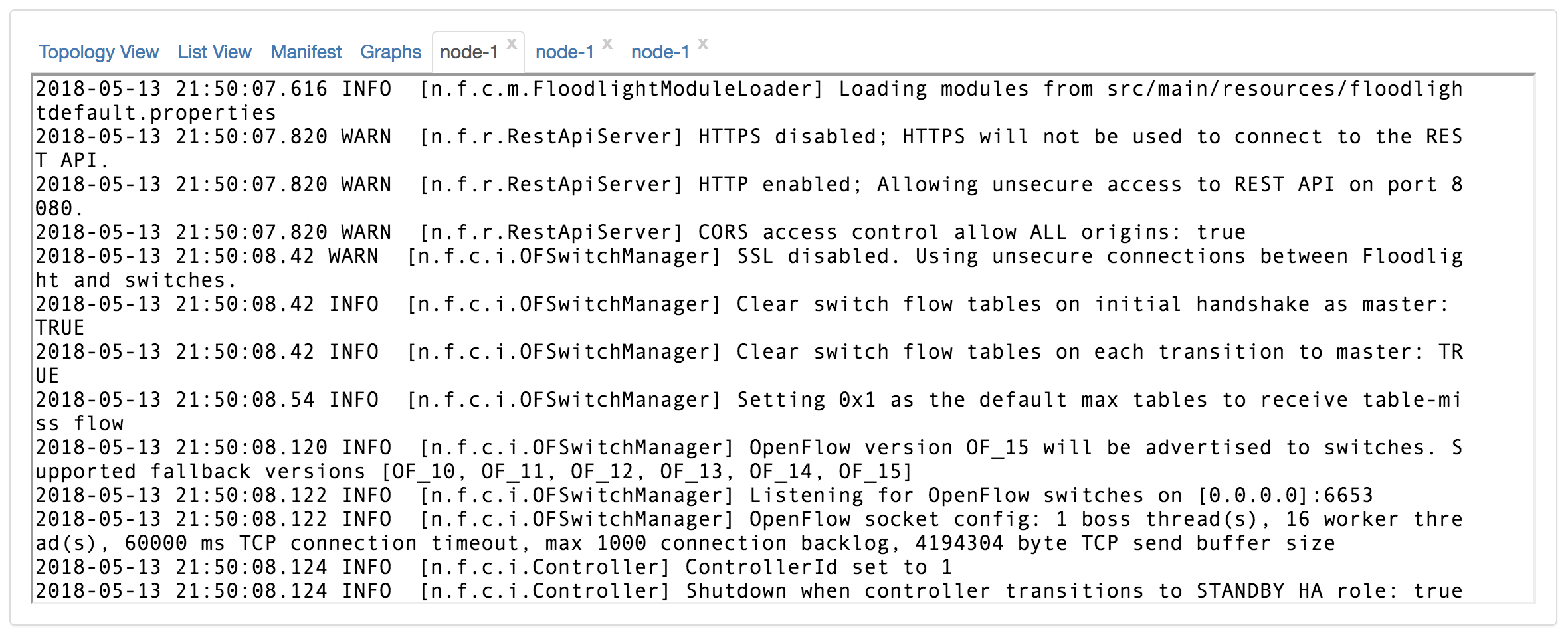
Harita Shroff

05/13/2018

**Homework-4**

1. [50 points] Please follow the DoS attack lab in SDN by using CloudLab. Please explain how DoS attack is launched in SDN.

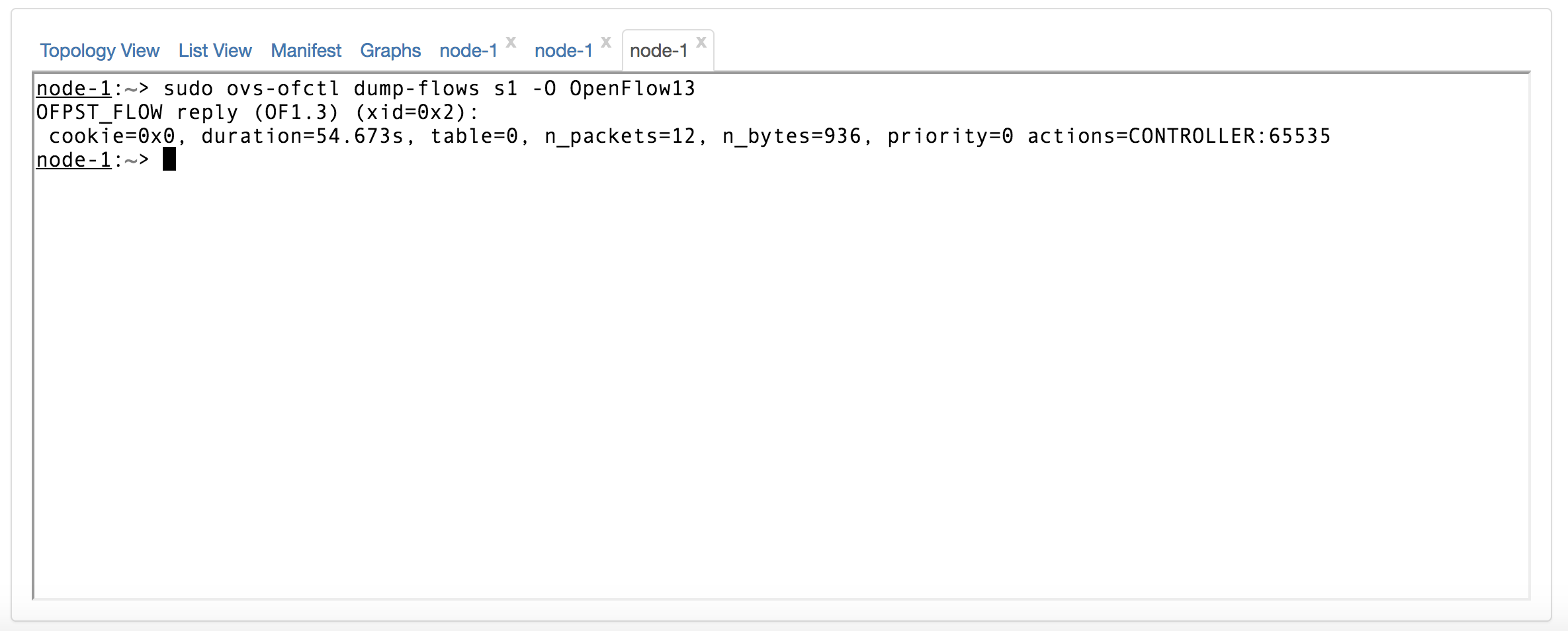
* We have started the floodlight controller in the below snapshot



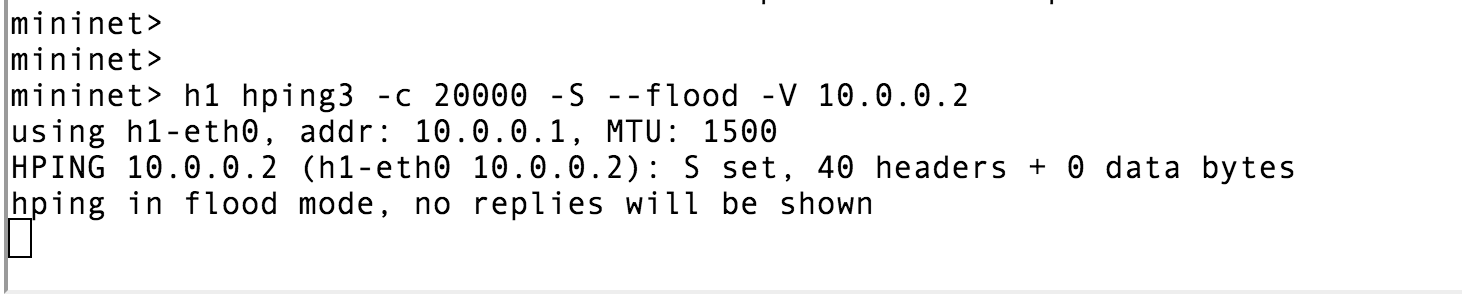
* Below we have created a simple mininet topology with 2 hosts and a switch.



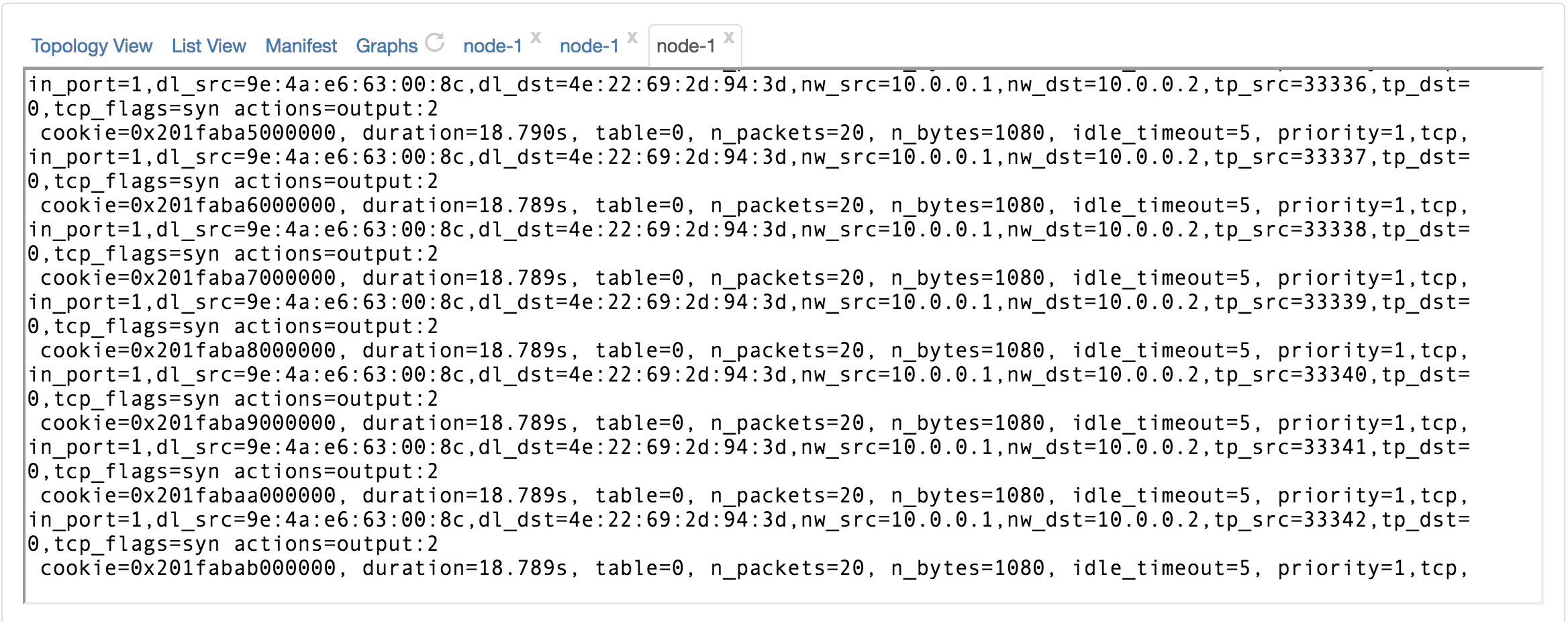
* Default flow rules are seen on the switch in below snapshot.



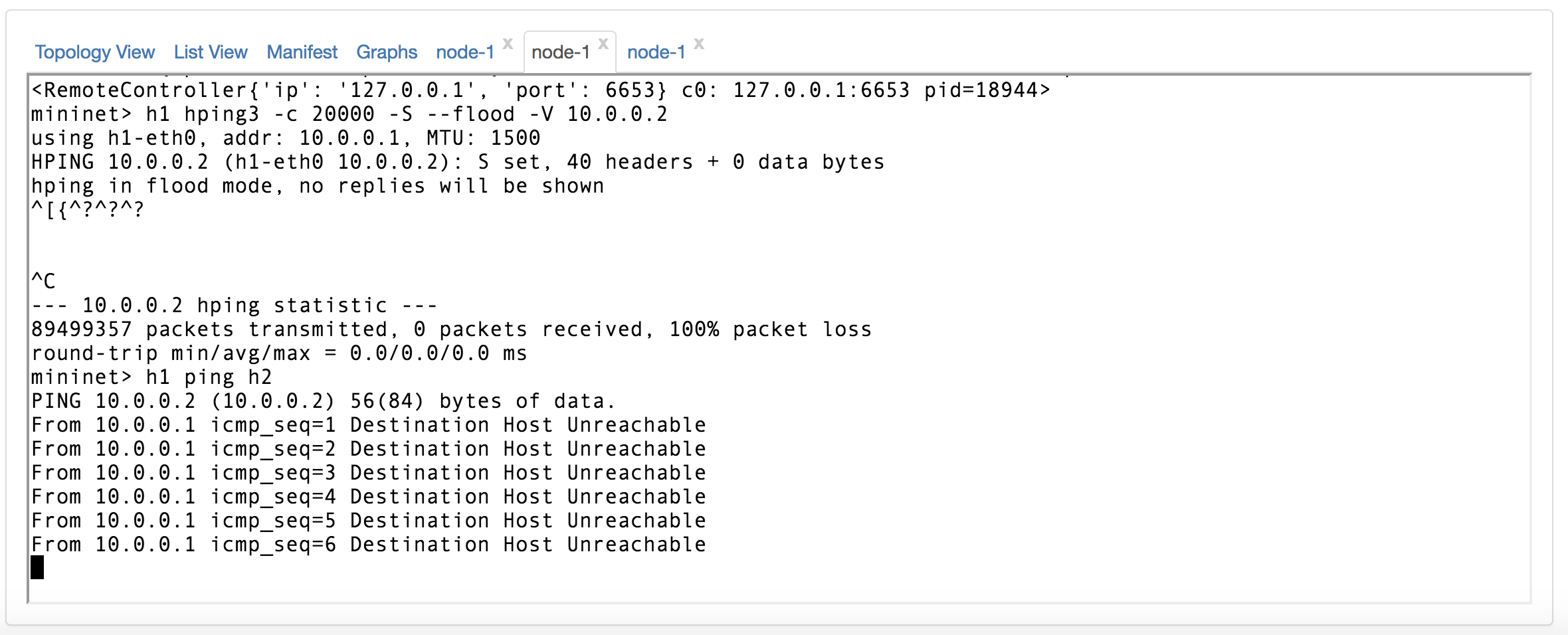
* From mininet terminal we used hping3 to send a packet flood to h2 from h1. We have used random-source option here. This will make sure that ping packet have different source address. Because of this, every packet results in the flow table miss and sent to controller. Controller in turn sends all the new flow rules to the switch.



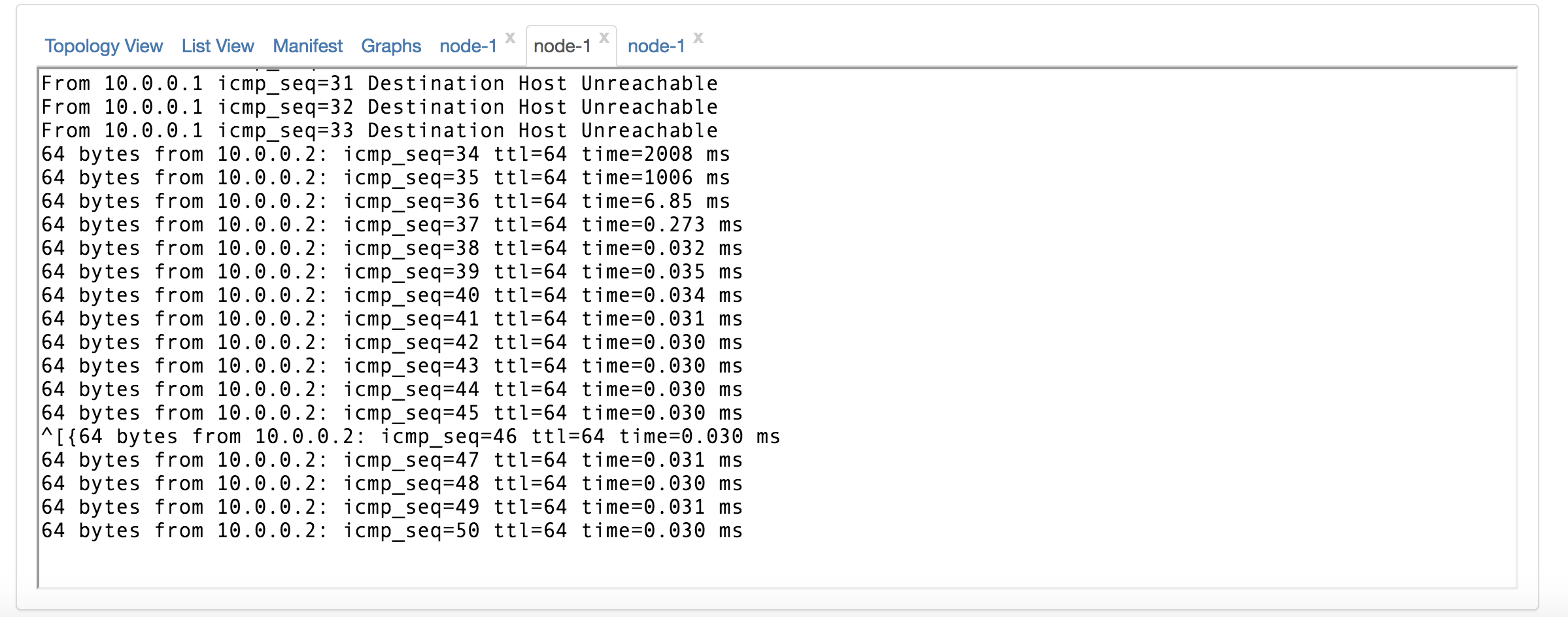
* Below is the snapshot capturing the large amount of flow rules. These flow rules are being sent from the controller to the switch.



* Once the flow rules have been completely printed, we can see below that ping does not work.



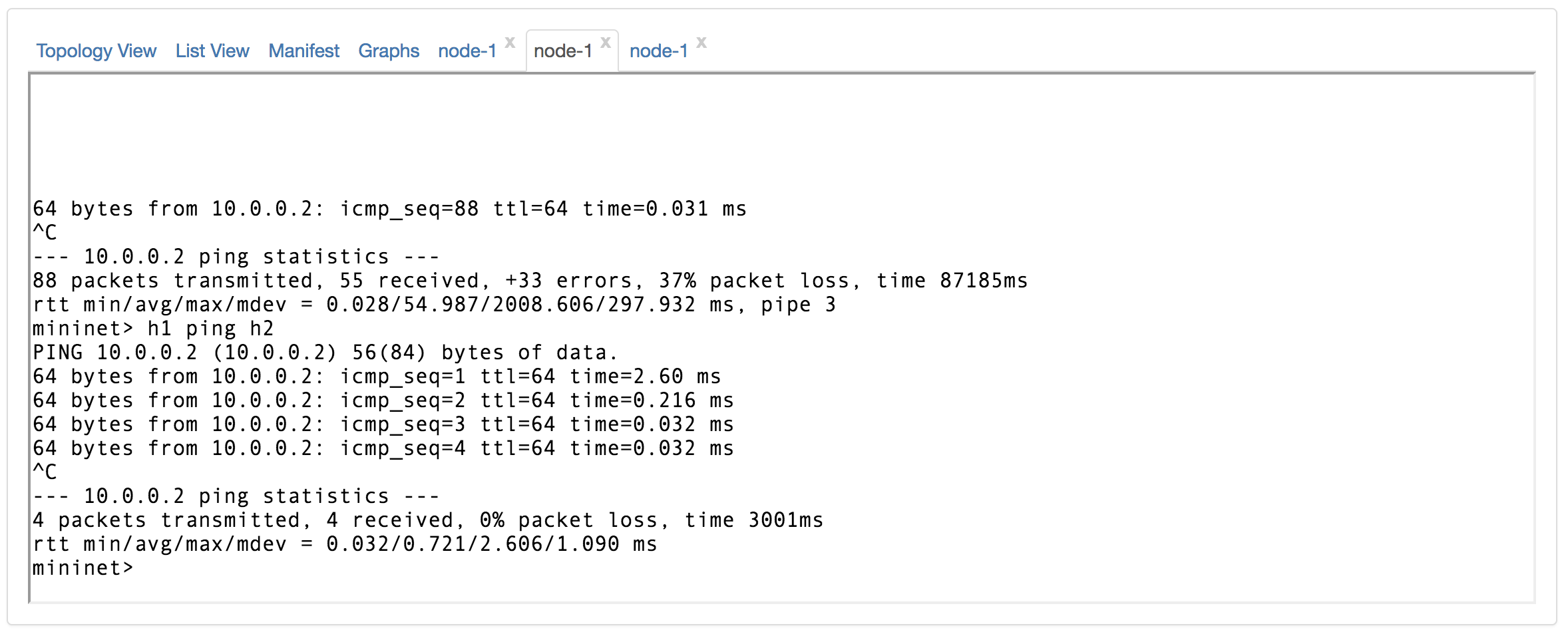
* After some time we can see that ping has started working again.



* All the flow rules have been deleted and only normal ping flow entries are present in the flow table.

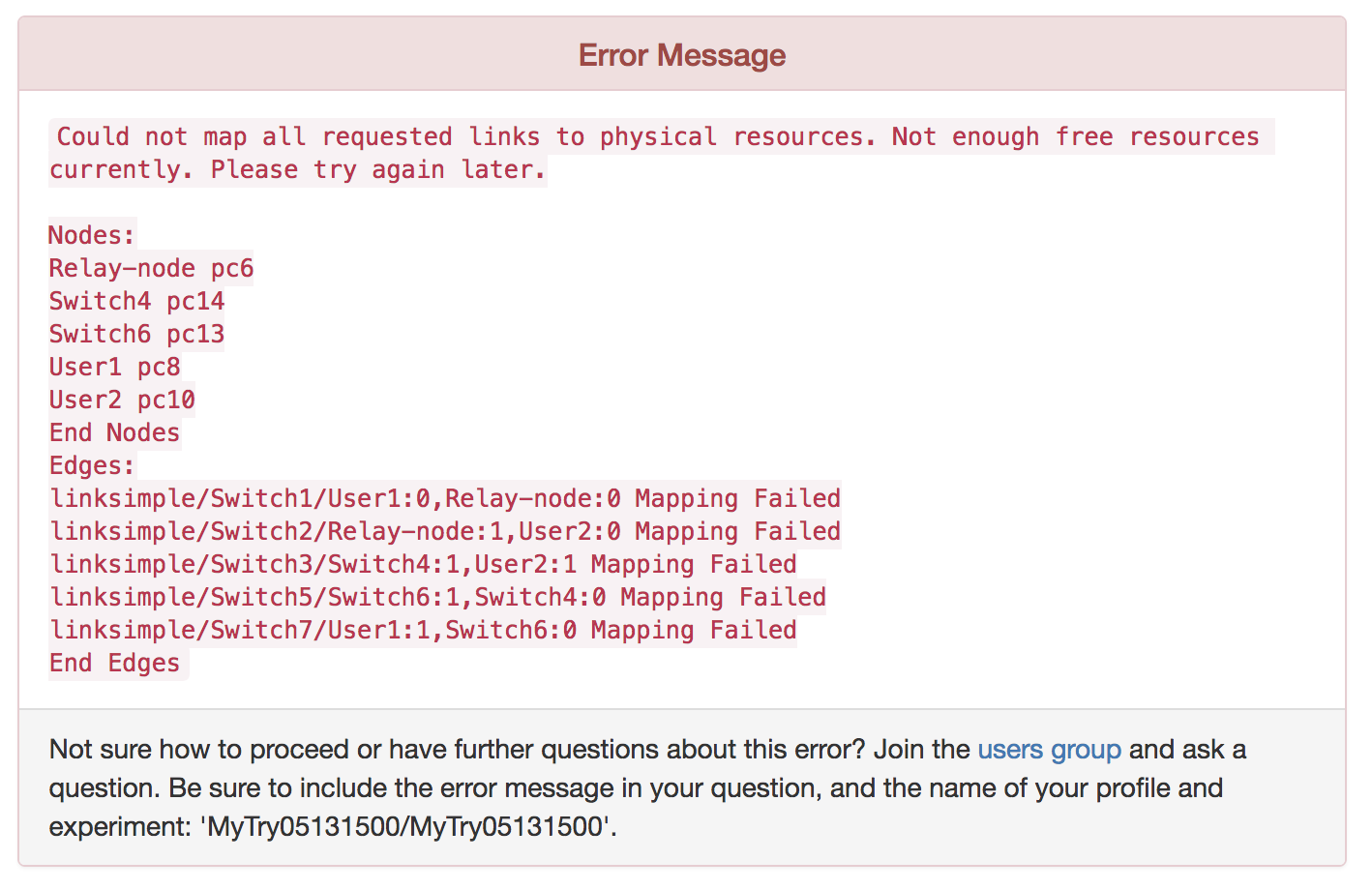
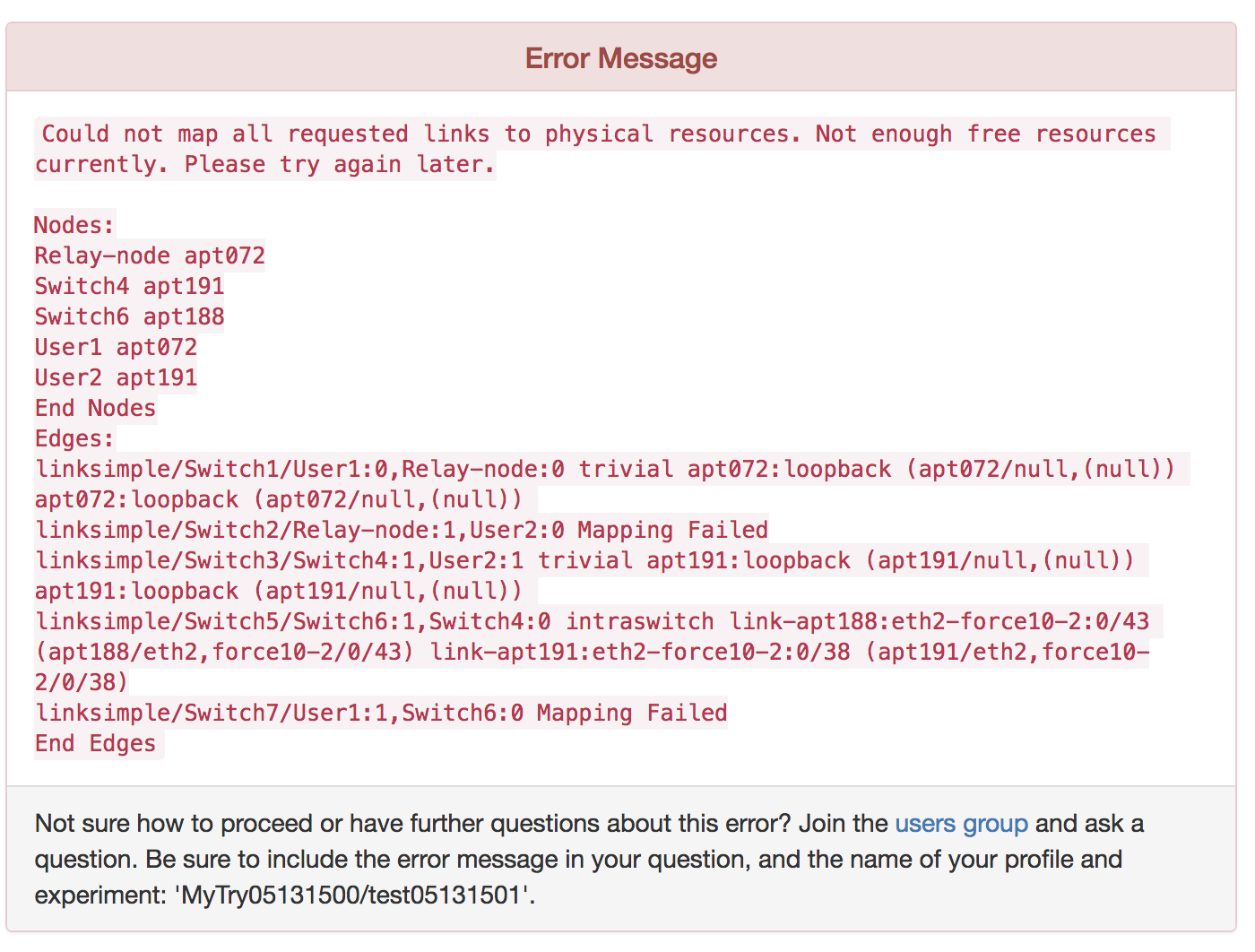


* A new ping command confirms that ping work as expected between two hosts.



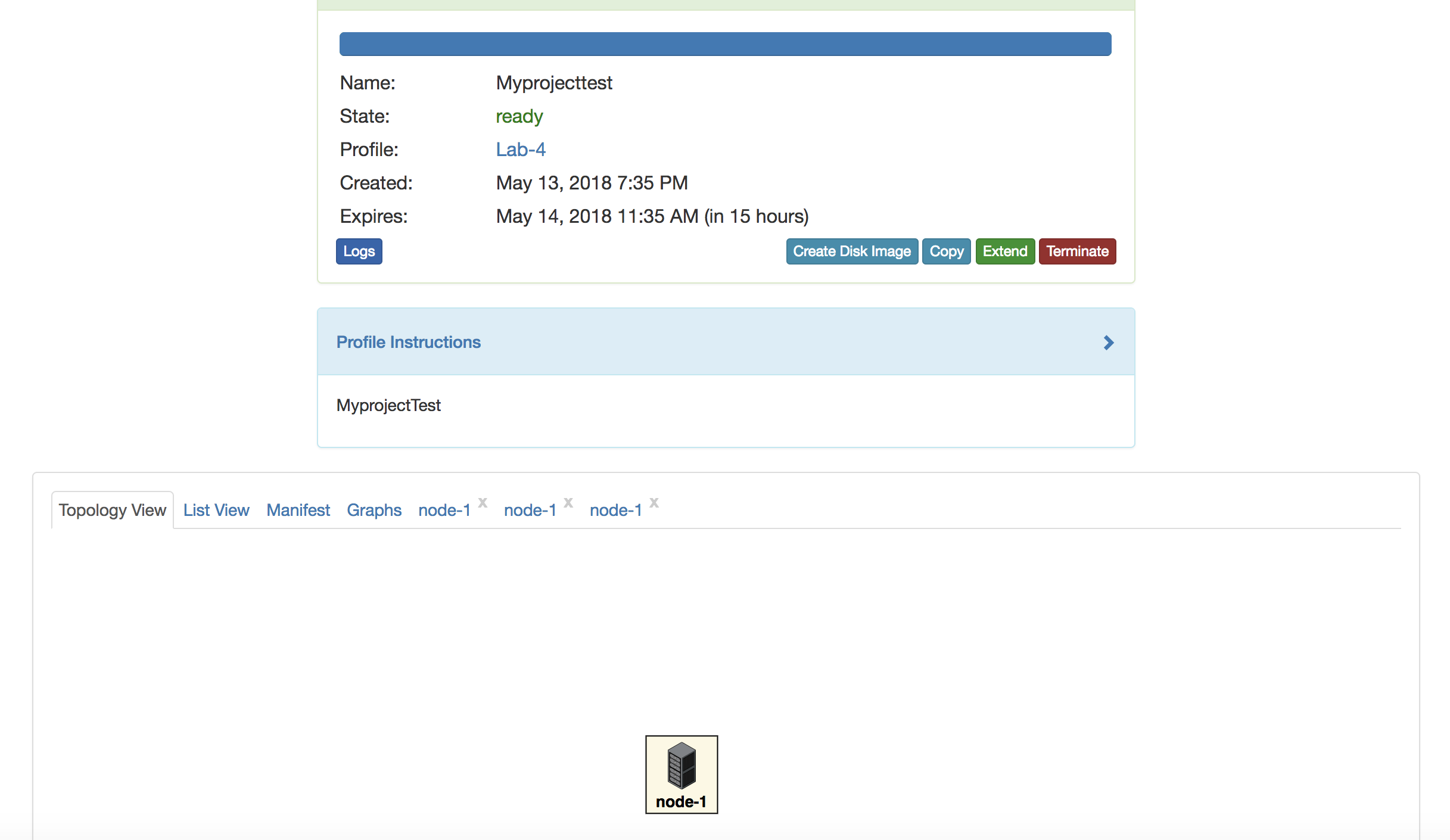
* When the switch has multiple flow rules due to hping3 utility, upon receiving an instruction to install a flow rules is rejected because of lack of space detected by the switch on the flow table. These rules are neglected and hence the ping does not work. Between switch and controller OFPT\_ERROR message with OFPFMFC\_TABLE\_FULL message is sent. The switch cannot forward the buffered packets until there is a space in the flow table to install new flow table rules from the ping command.

2. [50 points] Please follow the MiMT attack in SDN (in CloudLab). Please explain how the MiMT attack can be launched in SDN.

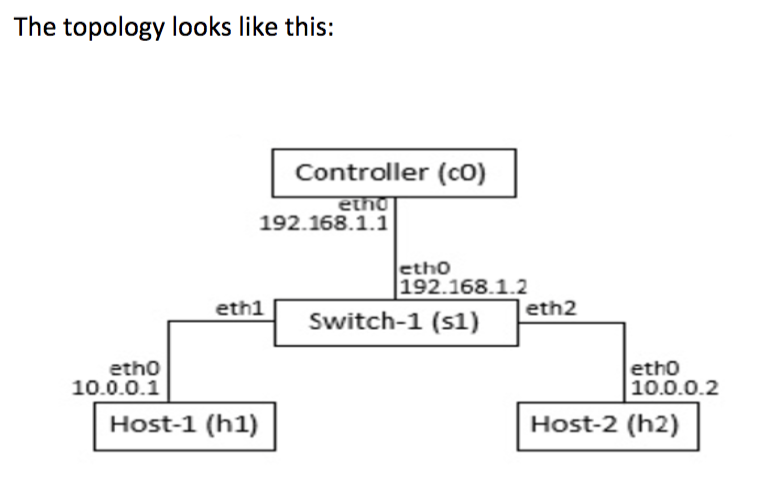


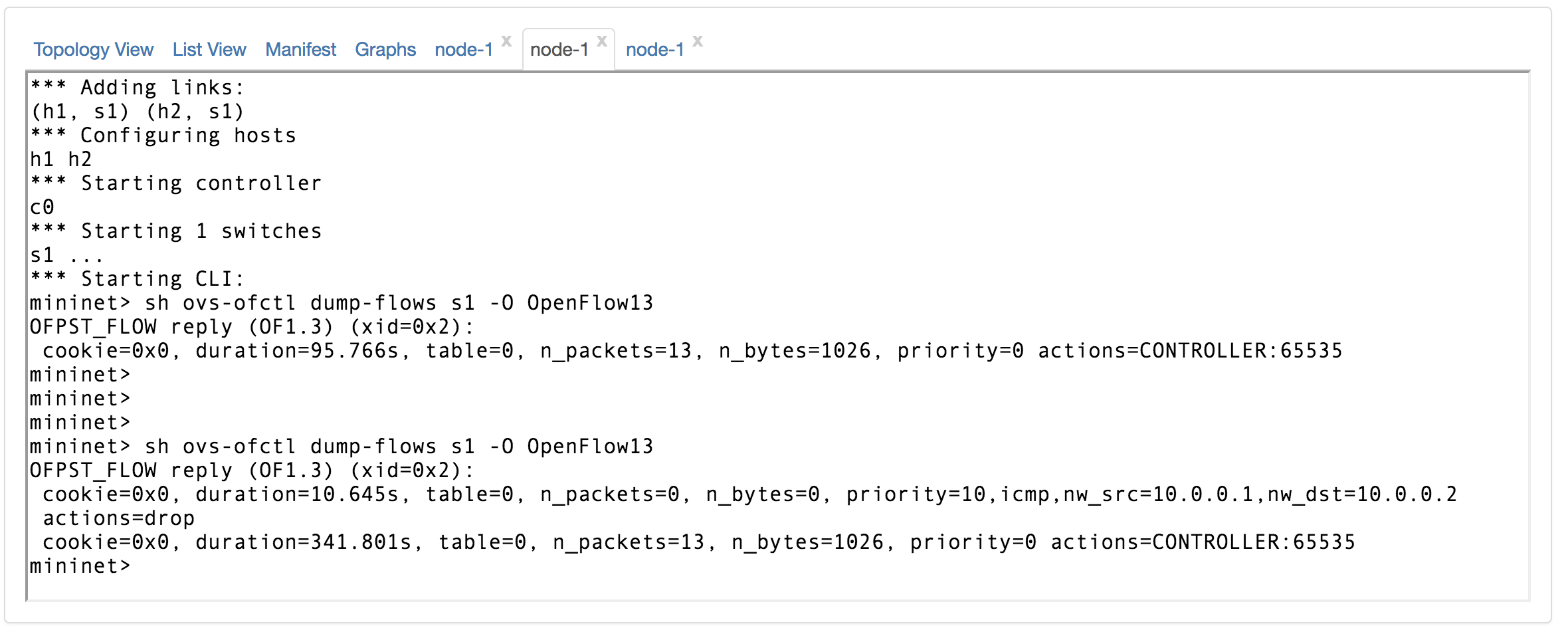
3. [100 points] Please test your course project in CloudLab and explain the result of your design experiment in CloudLab. You can use this result for your course project final report. Even though two students are the same team for your course project, the experiment result must be different. It is a sort of "design thinking".

* For the class project, we have designed the ip blacklist application which runs on the ryu controller. We designed the REST interface for this application using the inbuilt support for WSGI Application (Web Server Gateway Interface).
* Here in this experiment on the cloud lab, we create a node which will be used as a testbed for our application. Following tools were installed to achieve this result.
  + Mininet
  + Ryu controller
* Following snapshot shows that a single node was created in the cloud lab which is in READY state.

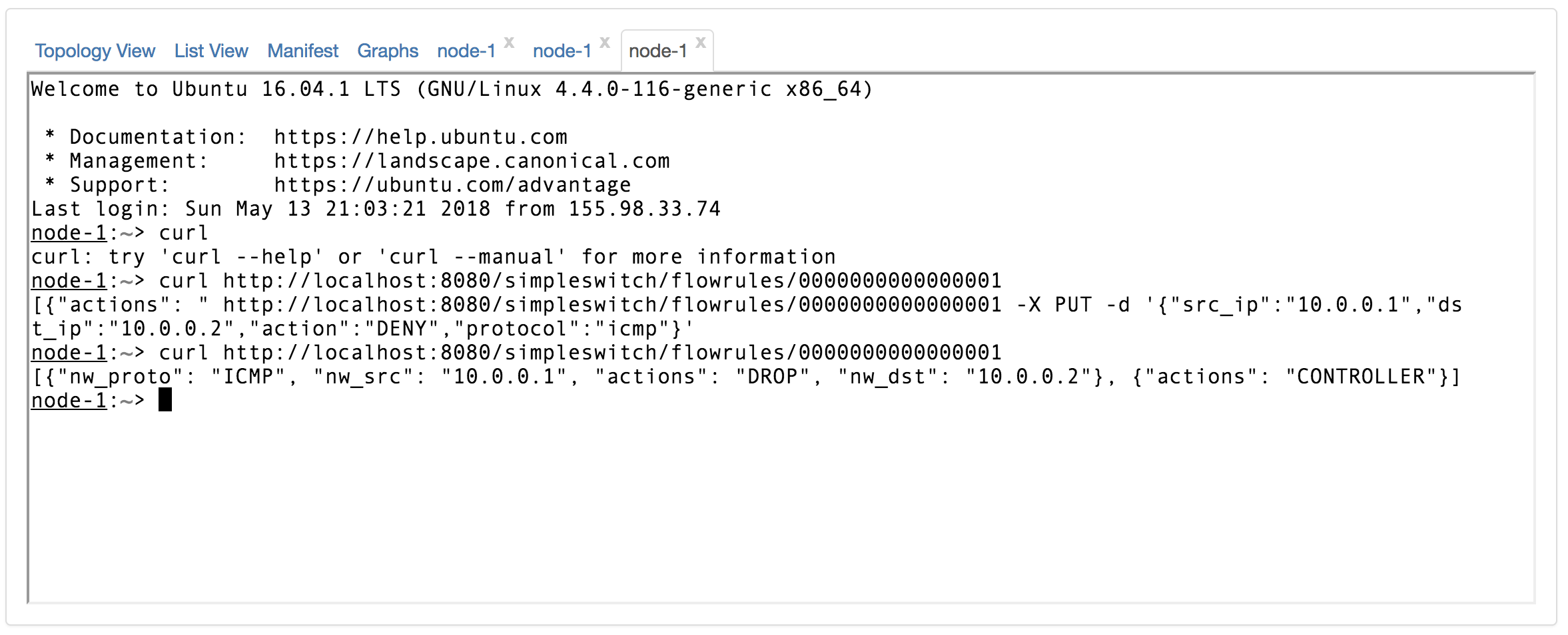


* As seen below, we have created a mininet topology with 2 hosts and a switch.



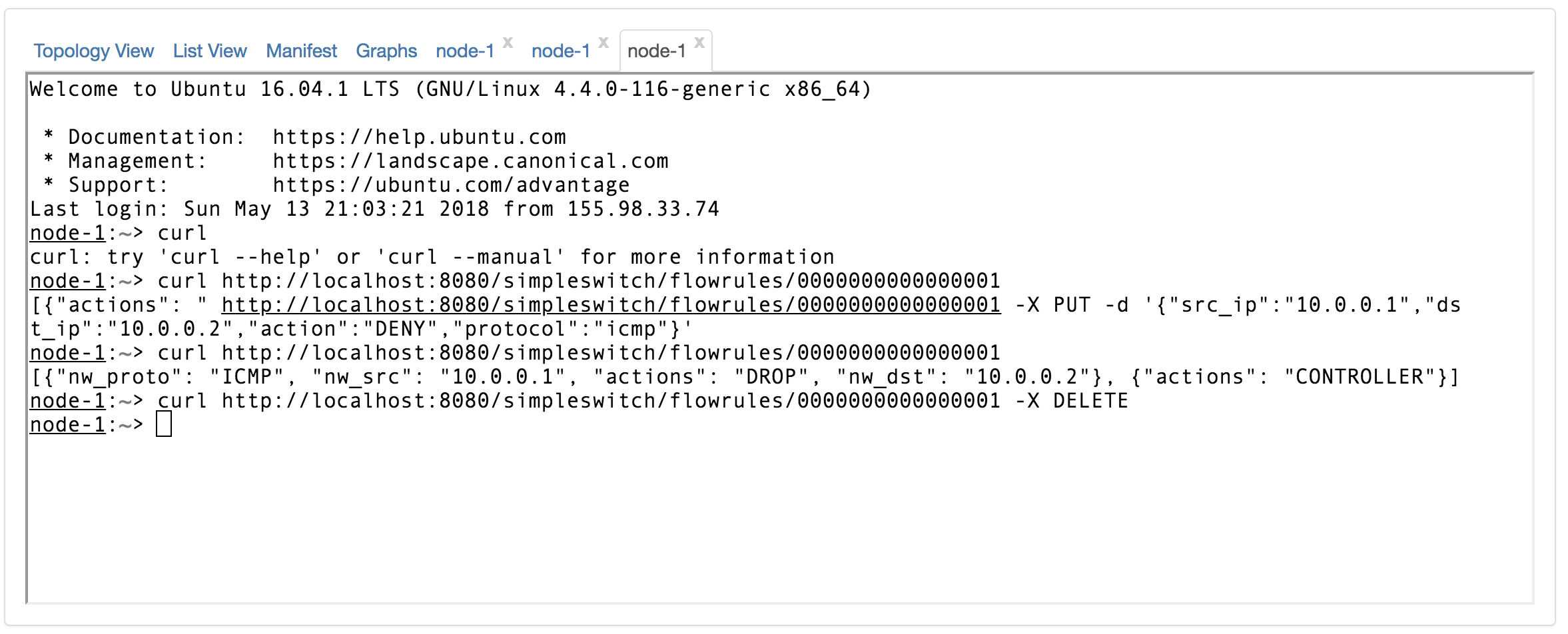


Snapshot-1



Snapshot-2

* As we can see in the above two snapshots, we have used a GET request and a PUT request to check and configure the flow rules through our application.
* The application update initialization, configures a basic CONTROLLER rule on the switch. This rule can be see in the snapshot-1.
* We used PUT request with data payload to configure a rule which can also be seen in the snapshot-1.



Snapshot-3



Snapshot-4

* Once the rule was configured successfully as we can see it in the snapshot-3, we used a DELETE all requests shown in snapshot-4.
* Upon receiving DELETE all, we can confirm on the mininet terminal that all the flow rules have been deleted.