Lab 4. Man-in-the-middle Attacks in the SDN Data Plane

Contents

Objective

By using security protocols in the transport layer, students will learn how to establish a secure communication between the controller and switch. Students will understand OpenFlow protocol vulnerability.
Students will be able to launch the man-in-the-middle attack in SDN and understand how attackers can steal information. They will learn security protocols like TLS, IPSec, and SSH and their usage between the controller and the switches. They will learn authentication methods needed for all devices connected to the controller or switches to ensure secure communication.

Submission

Copy and modify the profile, then start the experiment using your modified profile. Get screenshots of the following two scenarios.

1) The ***Relay node*** did not conduct the MITM attack. Use TCPDUMP to capture packets in ***Switch6*** or ***Switch4***

2) The ***Relay node*** conducted the MITM attack. Use TCPDUMP to capture packets in the ***Relay node***.

CloudLab Login page: https://www.cloudlab.us/login.php

Prepare the Experiment

Prepare the Controller.

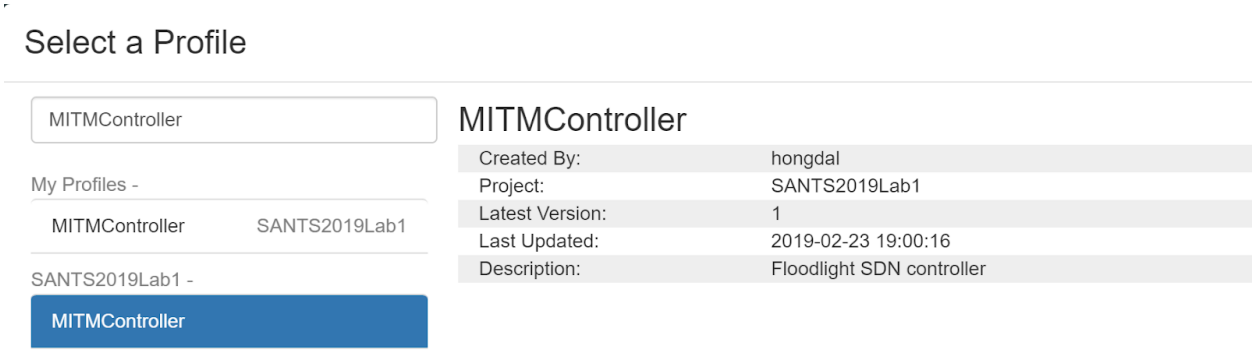


Figure 1: Start an experiment using the ***MITMController*** profile. Then Click “Select Profile” button to proceed.

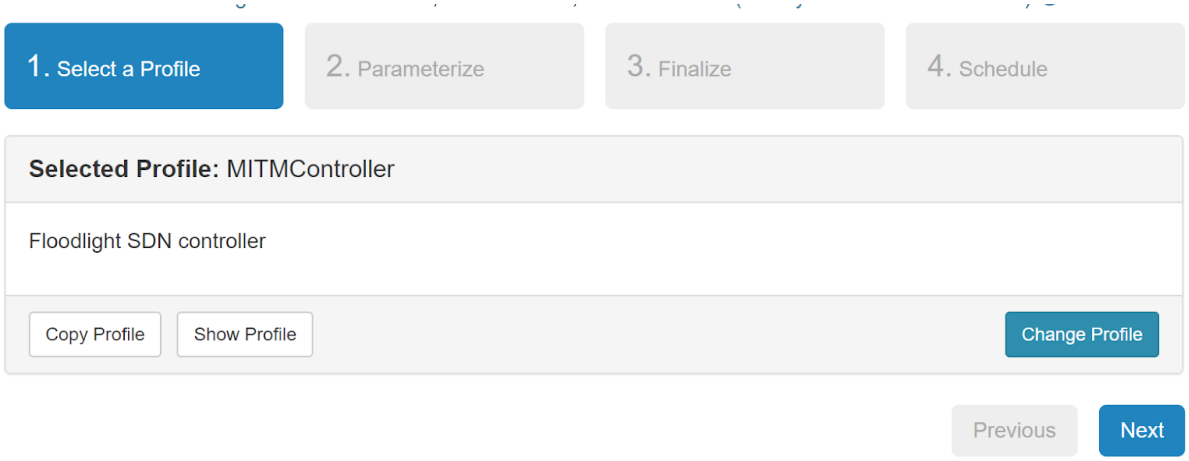


Figure 2: Click “Next” button to proceed.

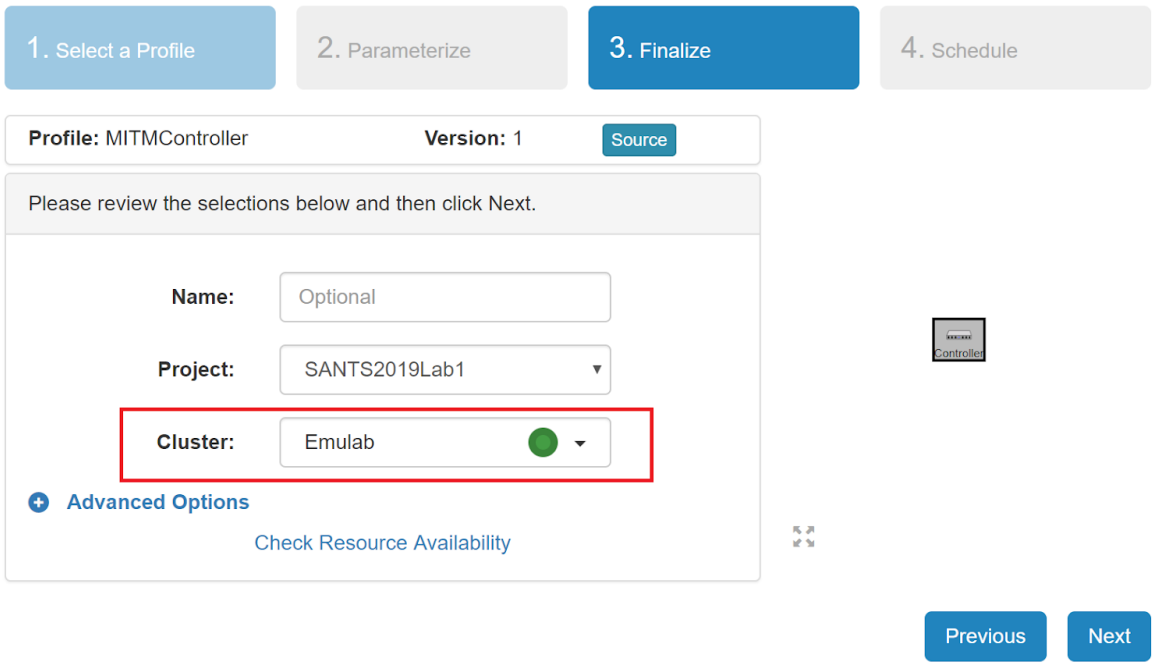


Figure 3: Choose a cluster and click “Next” to proceed.

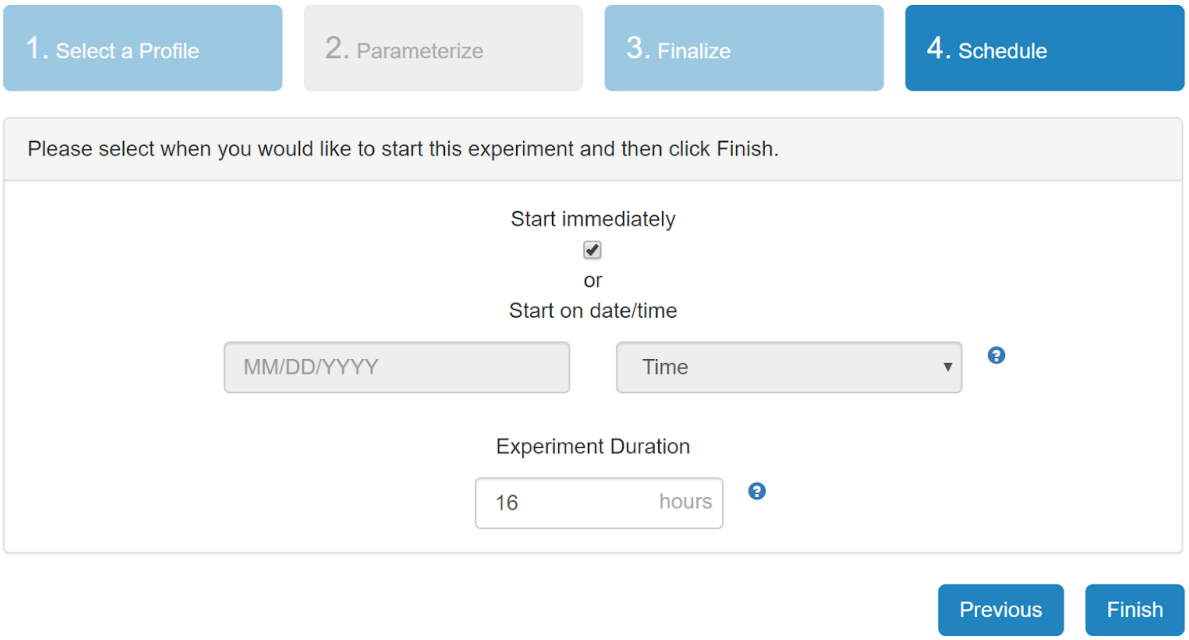


Figure 4: Click “Finish” to proceed.

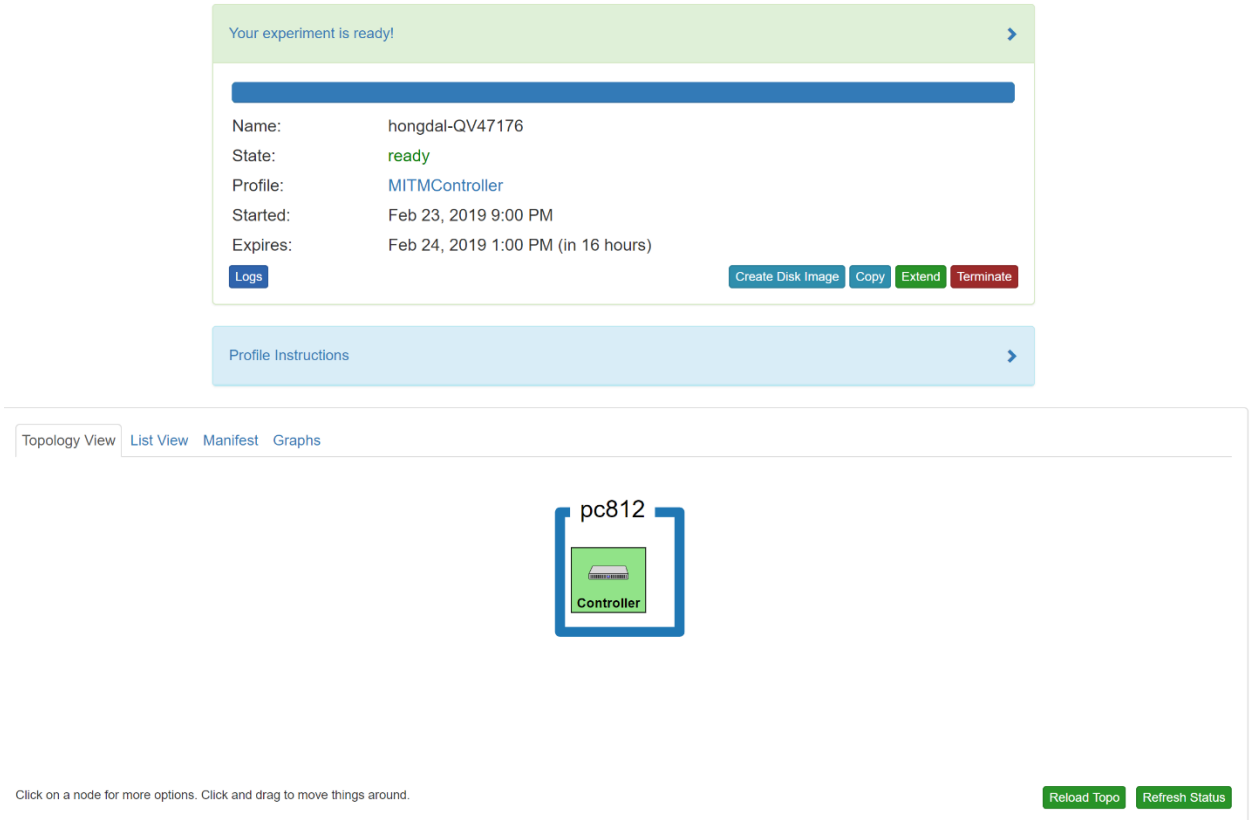


Figure 5: The controller is successfully running.

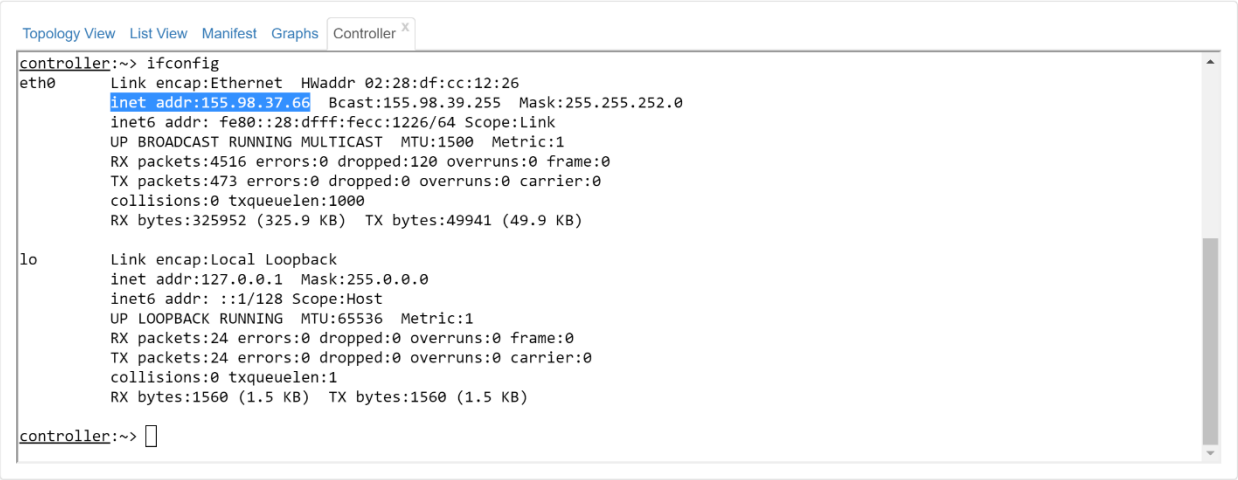


Figure 6: Start a shell. Type "***ifconfig***" to check the IP. This IP will be used when we configure the switches. Let's note it as ***controller_ip***

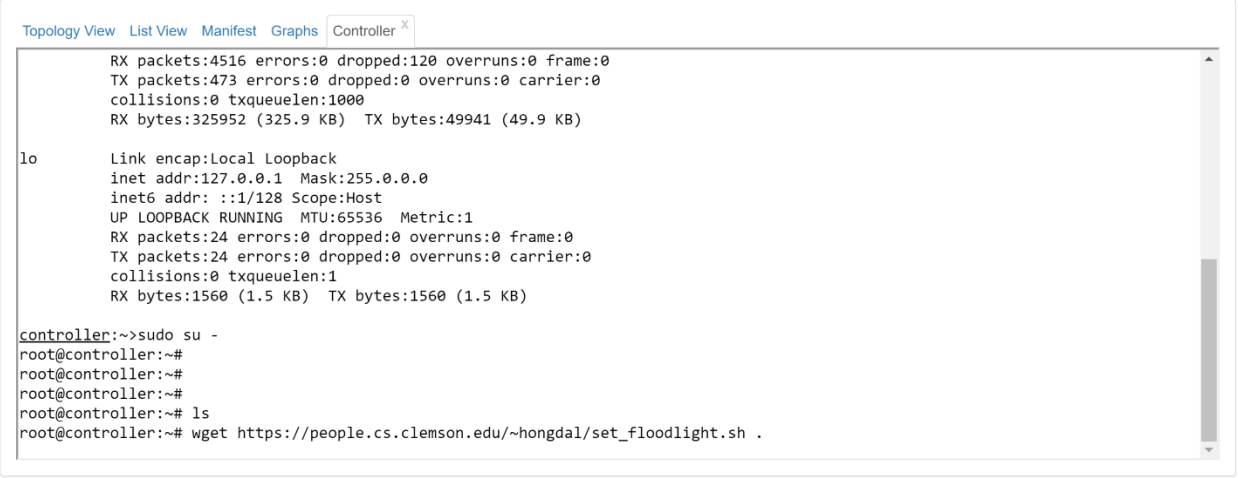


Figure 7: setup controller.

1) Switch to root. Type "***sudo su -***"

2) Type "***wget*** [***https://people.cs.clemson.edu/~hongdal/set_floodlight.sh***](https://people.cs.clemson.edu/~hongdal/set_floodlight.sh) ***.***"

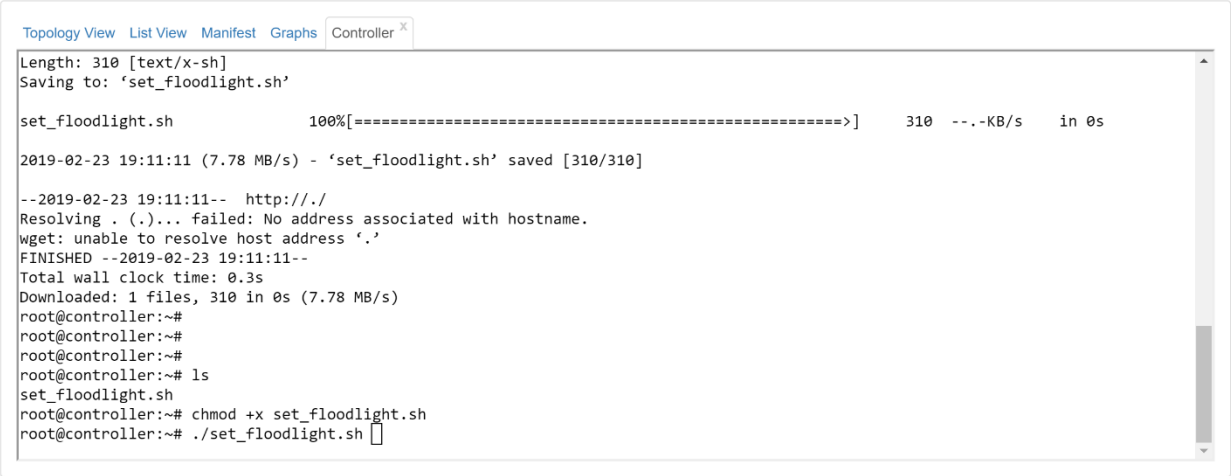


Figure 8: Run the scripts.

1) Type “***chmod +x set_floodlight.sh***”
2) Type “***./set_floodlight.sh***”

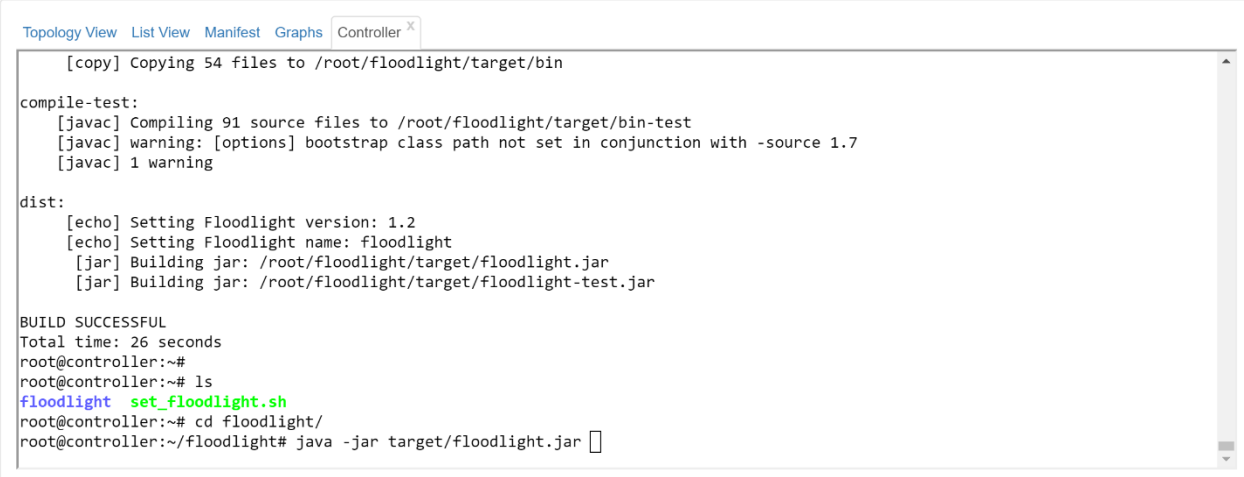


Figure 9: Launch the controller.

1) Type “***cd floodlight***”
2) Type “***java -jar target/floodlight.jar***”

Prepare the Nodes

Download a topology from here: https://people.cs.clemson.edu/~hongdal/mitm-attack.xml
Create a new profile using the download topology.

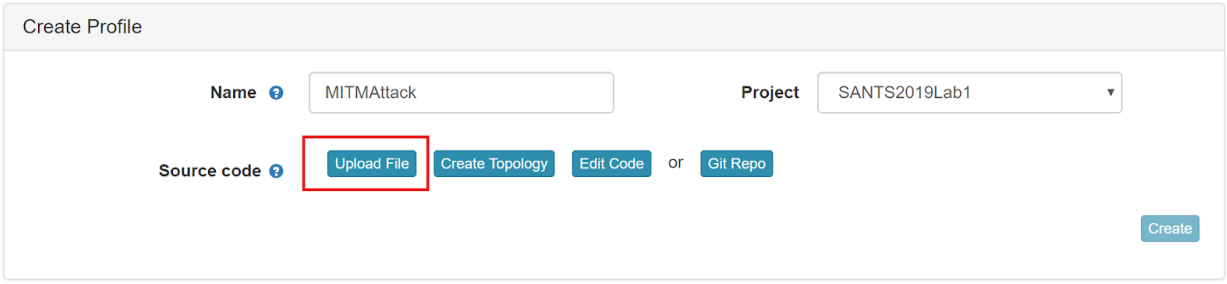


Figure 10: Upload the topology when creating the profile.

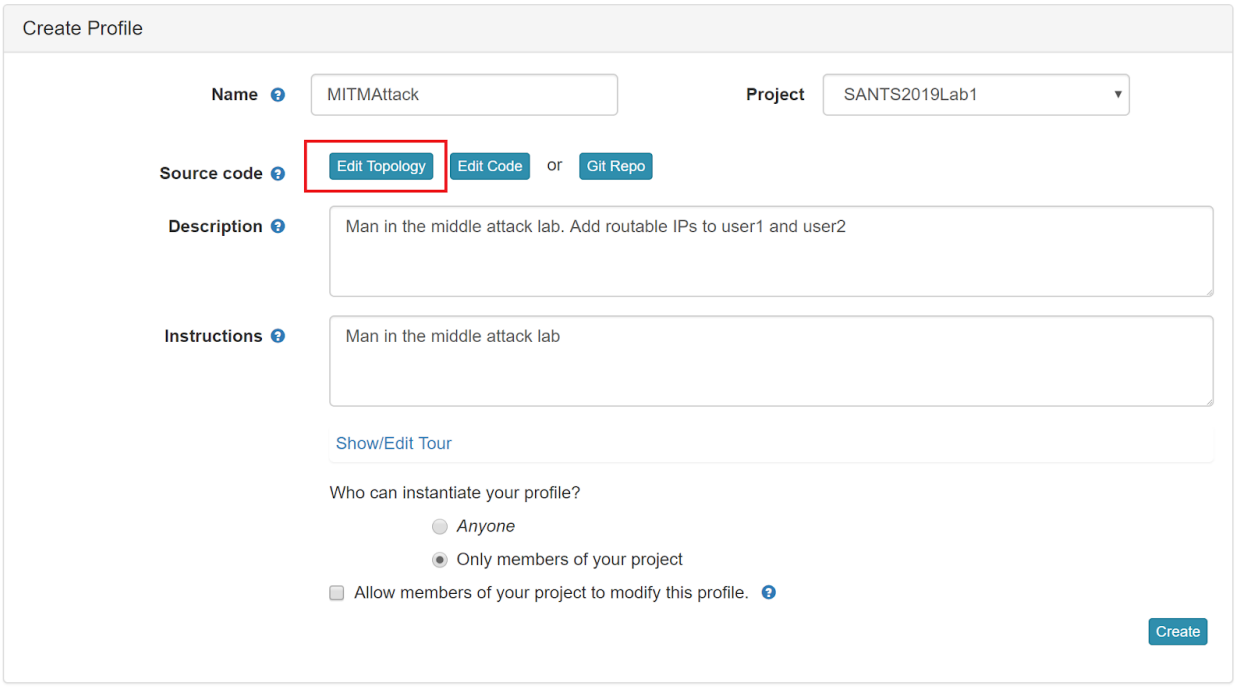


Figure 11: Click “Edit topology” to configure the SDN controller.

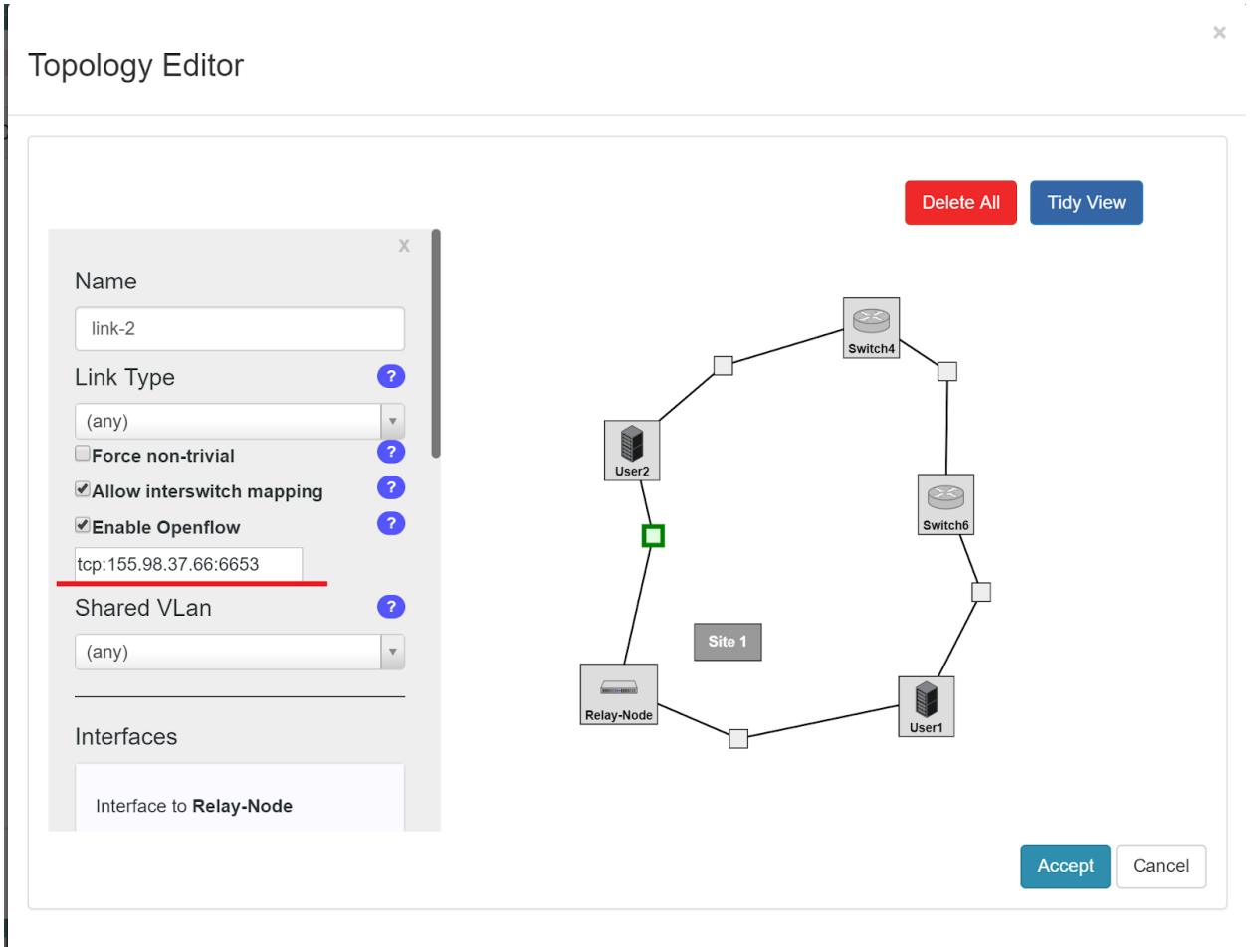


Figure 12: Update the IP address to the ***controller_ip*** and select the **Link Type** as "**Ethernet**" all the 5 links in the profile. Then click "Accept".

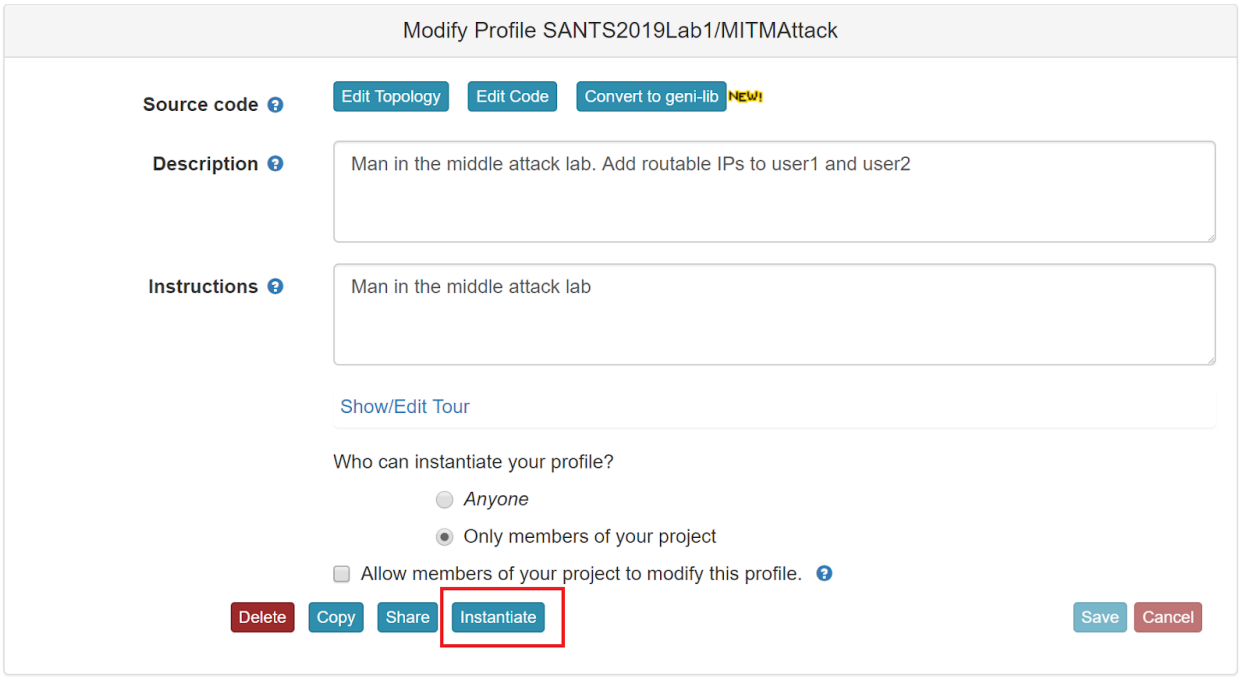


Figure 13: Click “instantiate” to proceed.

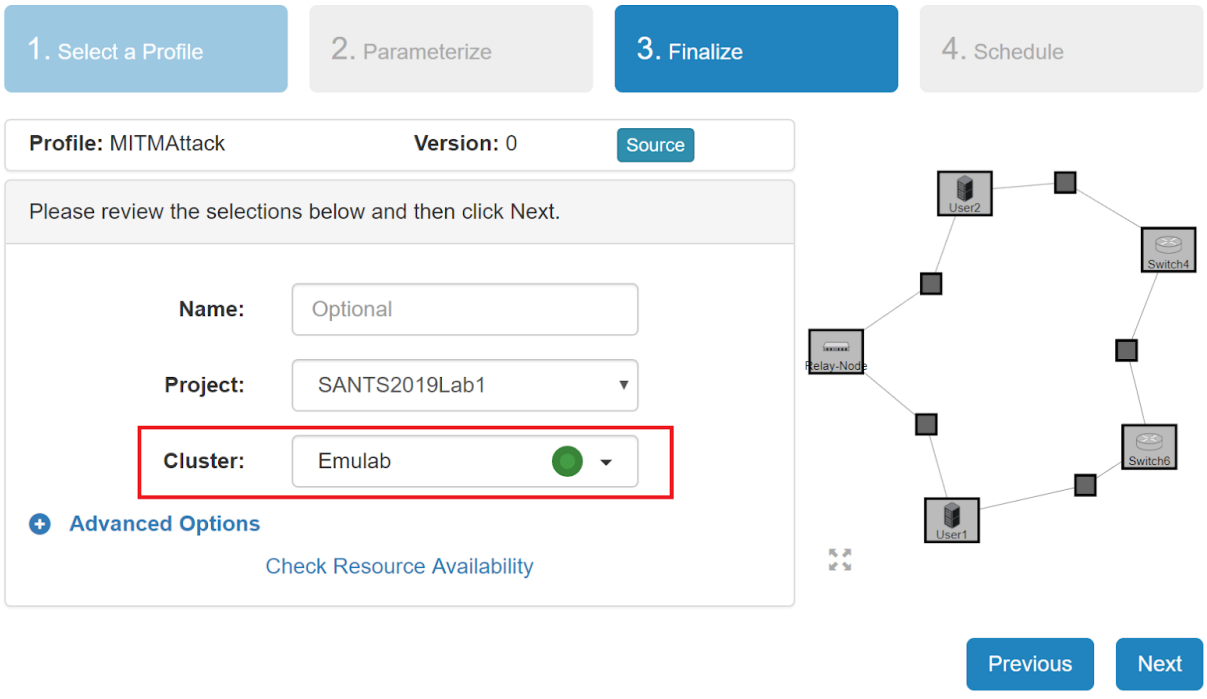


Figure 14: Choose a cluster. Click “Next” to proceed.

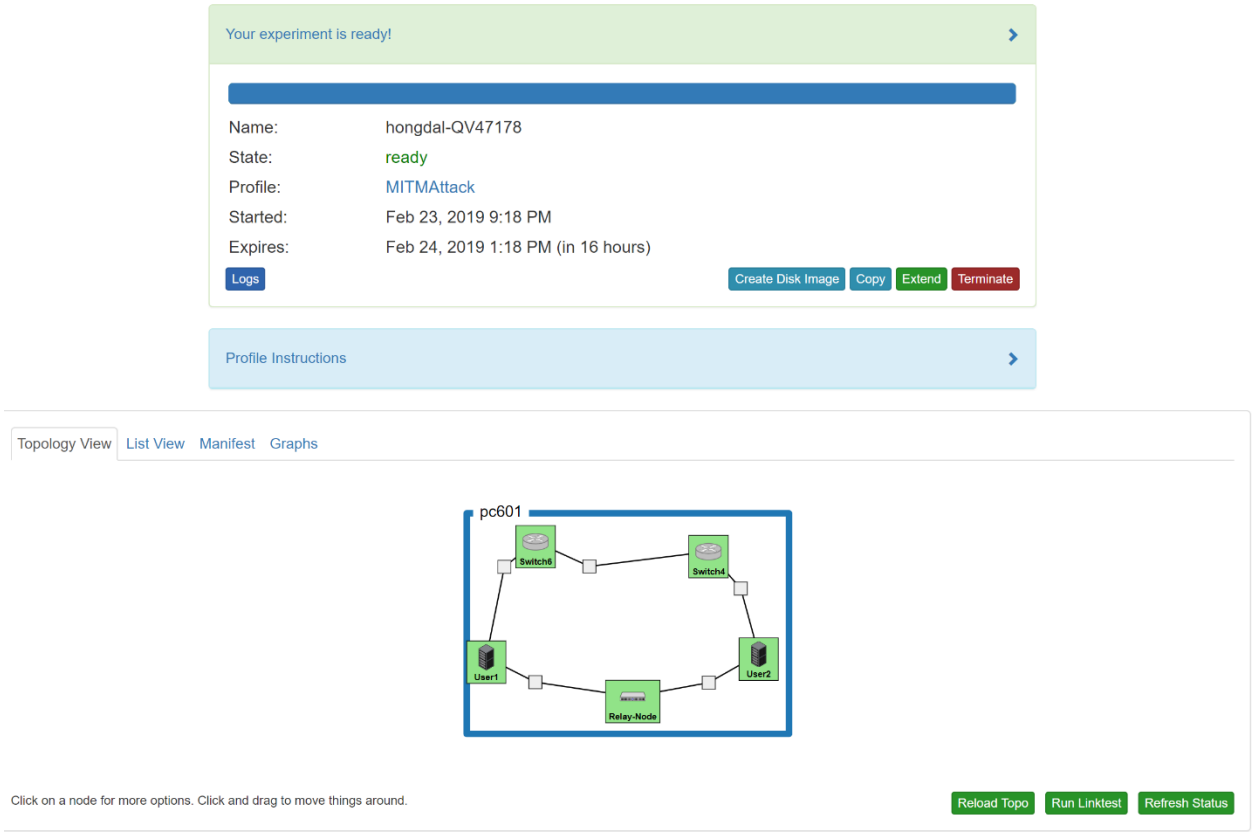


Figure 15: The nodes are running successfully.

Conduct the Experiment

Scenario 1 (Normal Traffic)

1) Open the shells for each of the node. Do steps 2) and 3) for each node. We will use ***User1*** as and example. The node IP should be different for different nodes.
2) Run "**sudo su**" and download the "set_ovs.sh" script by running the command "**wget https://people.cs.clemson.edu/~hongdal/set_ovs.sh**" on all the nodes.
3) change permission and run the script.

"***chmod +x set_ovs.sh***"
"***./set_ovs.sh eth1 eth2 155.98.37.66 10.10.10.1***"

The **red IP** is the ***controller_ip***, the **blue IP** is the node IP. Use different node IP for different nodes. E.g., 10.10.10.2 for ***User2***, 10.10.10.3 for ***Switch4***, and 10.10.10.4 for ***Switch6***.

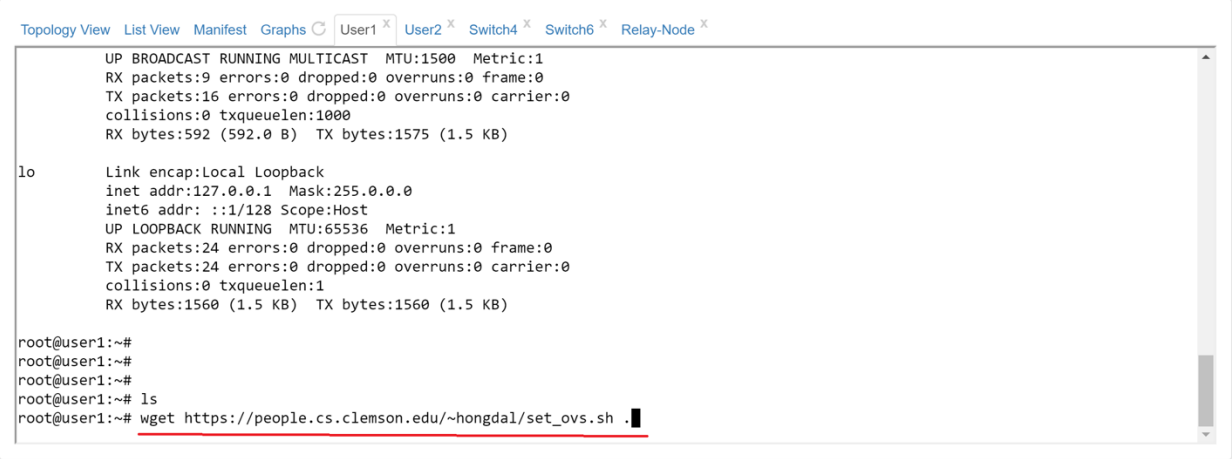


Figure 16: Download the script

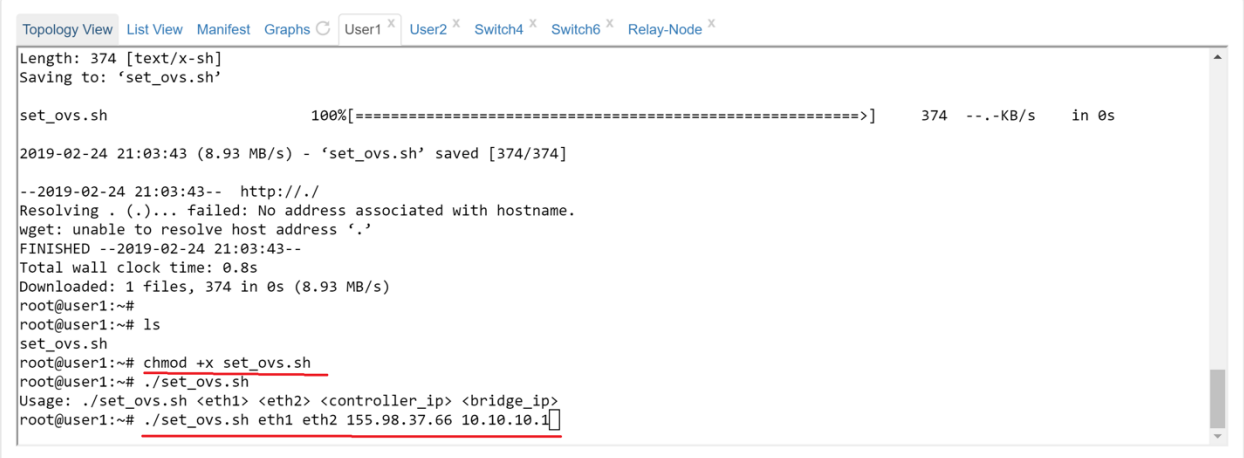


Figure 17: Change permission and run

4)Check IP of ***User1*** and ***User2***. Note that we will work with experimental IP (ovs-lan), not the public IP.
2) PING from ***User1*** to ***User2*** again.

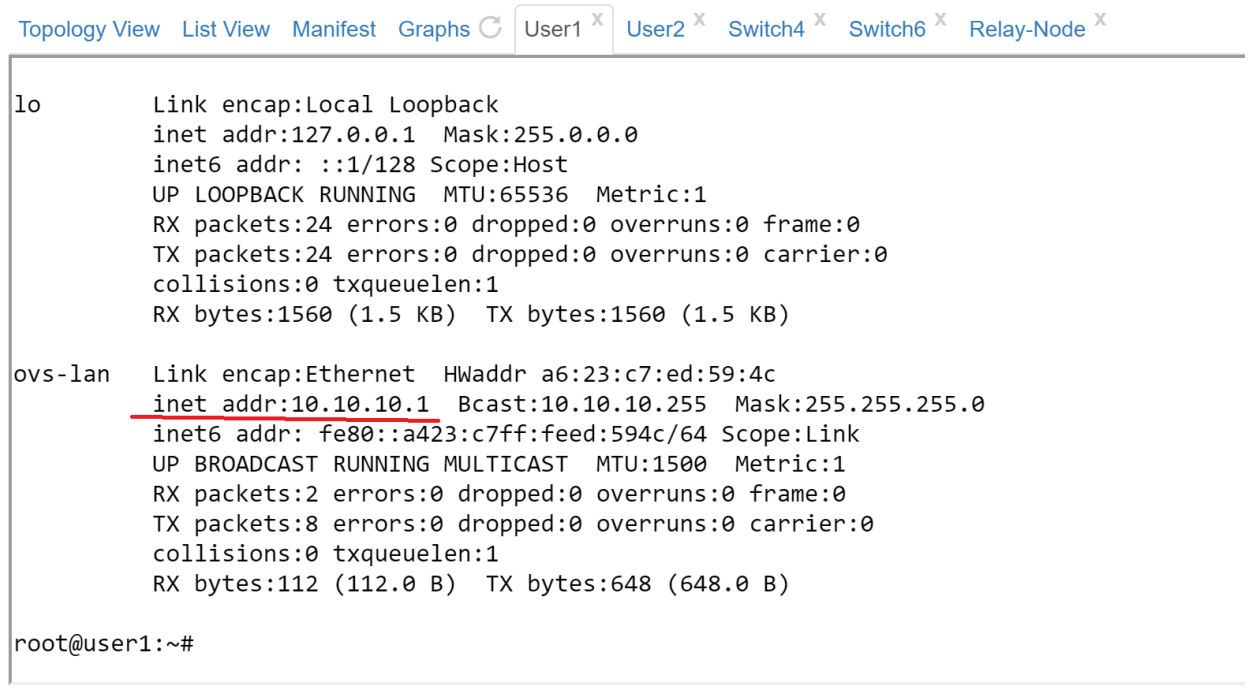


Figure 18: Check the experimental IP of User1.

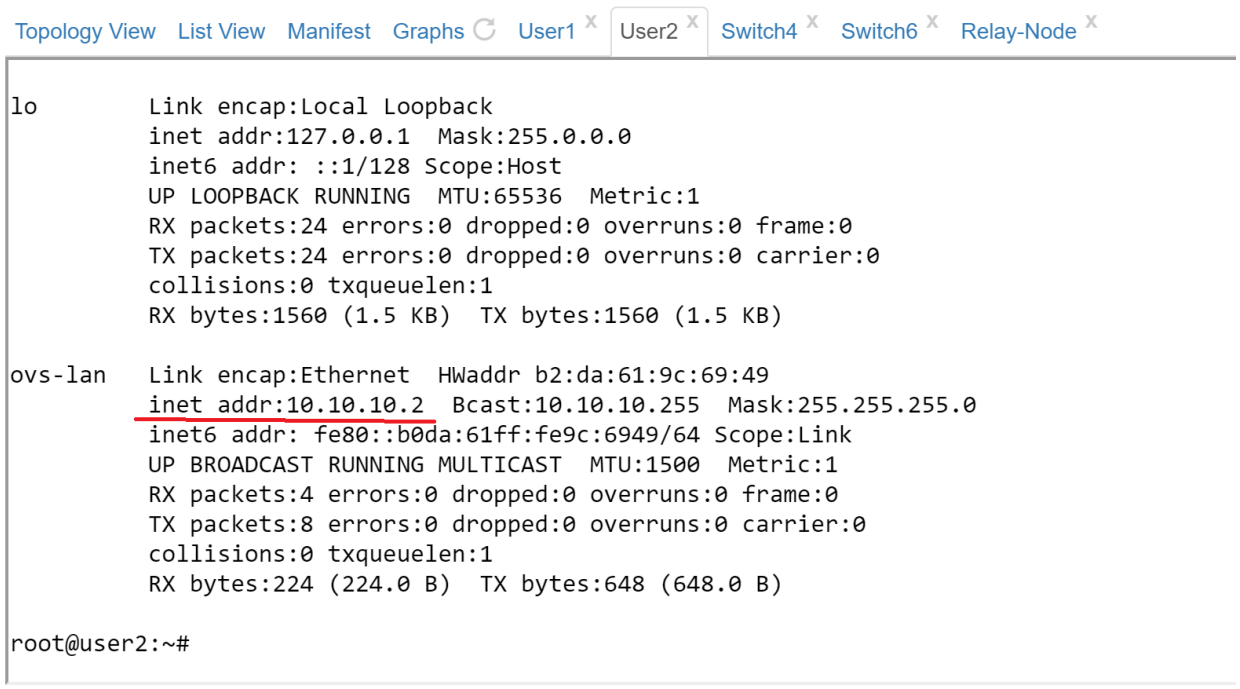


Figure 19: Check the experimental IP of User2.

3) Observe the packets from ***Swith4*** or ***Switch6***. Type "***tcpdump -i eth1 -nq icmp***" in their shells.

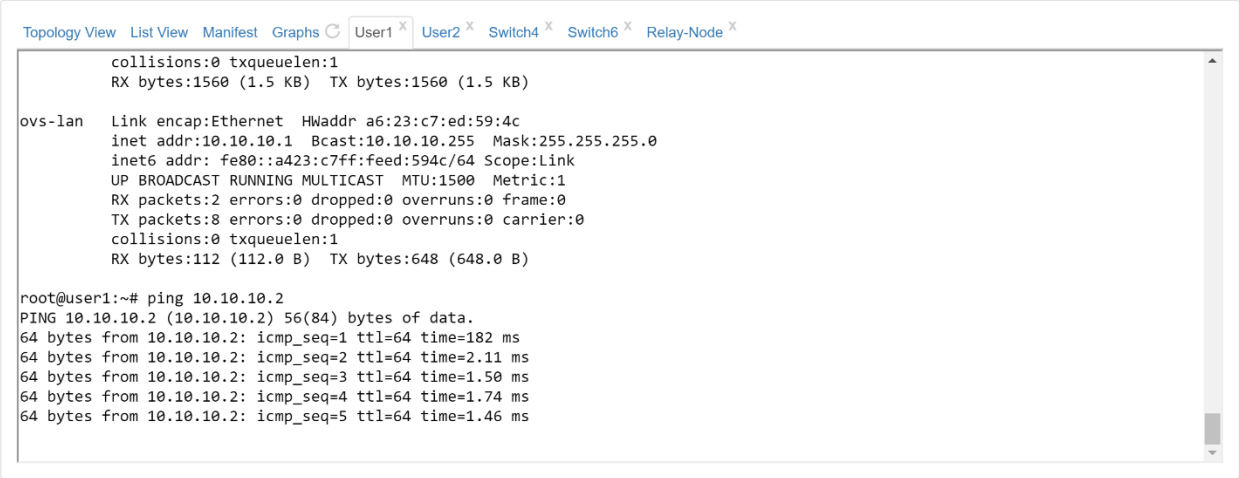


Figure 20: PINF from User1 to User2.

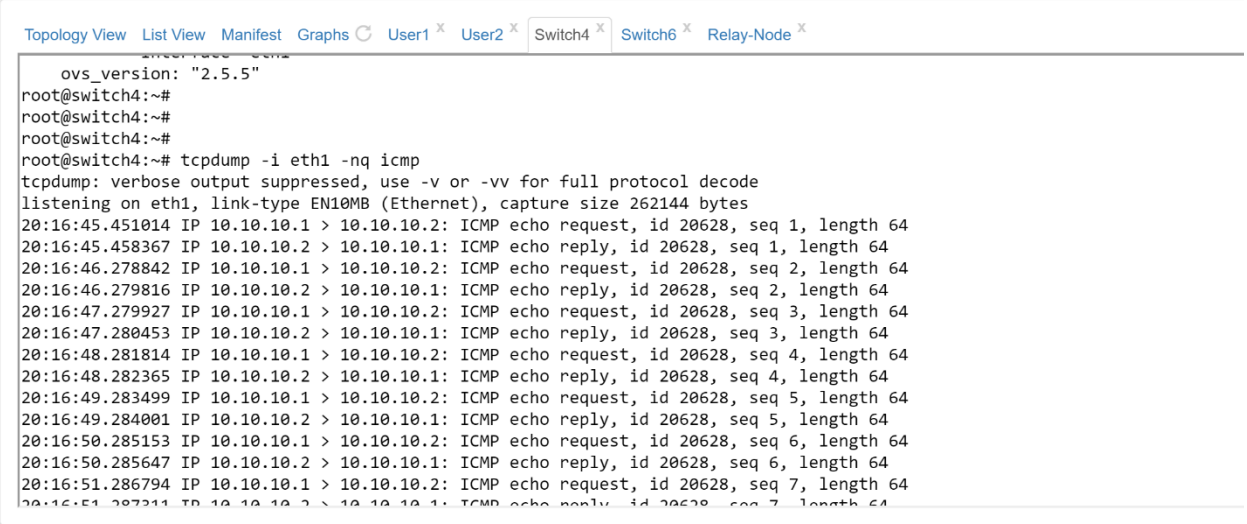
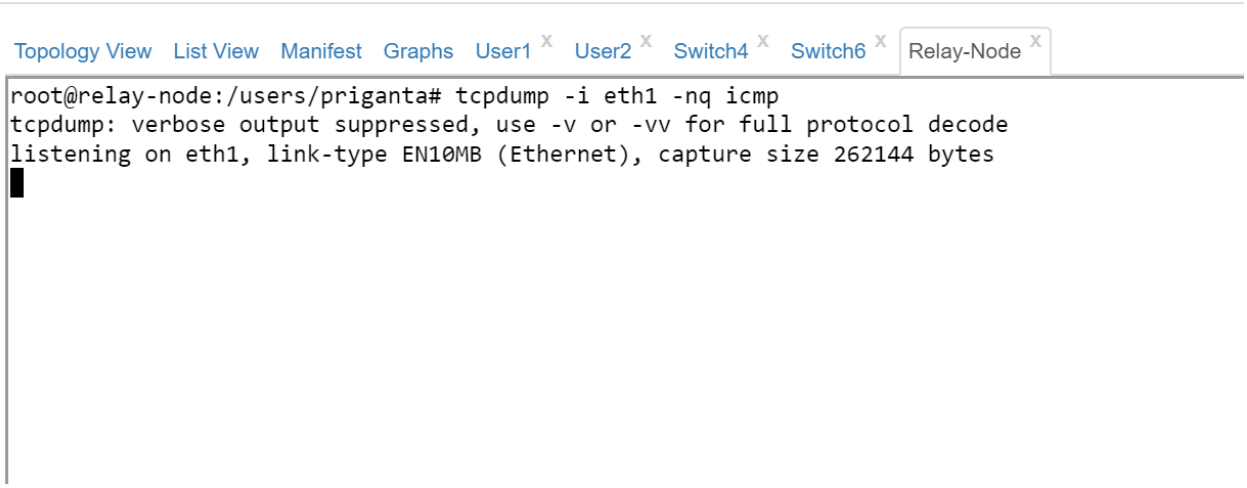


Figure 21: Observe the packets at Switch4 or Switch6.

4) Observe the packets from Relay node. Type "***tcpdump -i eth1 -nq icmp***" in its shell.



No traffic is observed on Relay node.

Scenario 2 (MITM Attack)

1) Stop the PING at ***User1***
2) Conduct attack.
   (1) Download the attack script by running the command "**wget https://people.cs.clemson.edu/~hongdal/attack.sh**"
   The "attack.sh" script creates a ovs-switch on the relay node and connects it to the controller which is very similar to the "set_ovs.sh" script that is run in the remaining nodes.

   (2) Type "chmod +x attack.sh"
   (3) Run attack.sh. "attack.sh eth1 eth2 155.98.37.66 10.10.10.5". The ***controller_ip*** is use here.

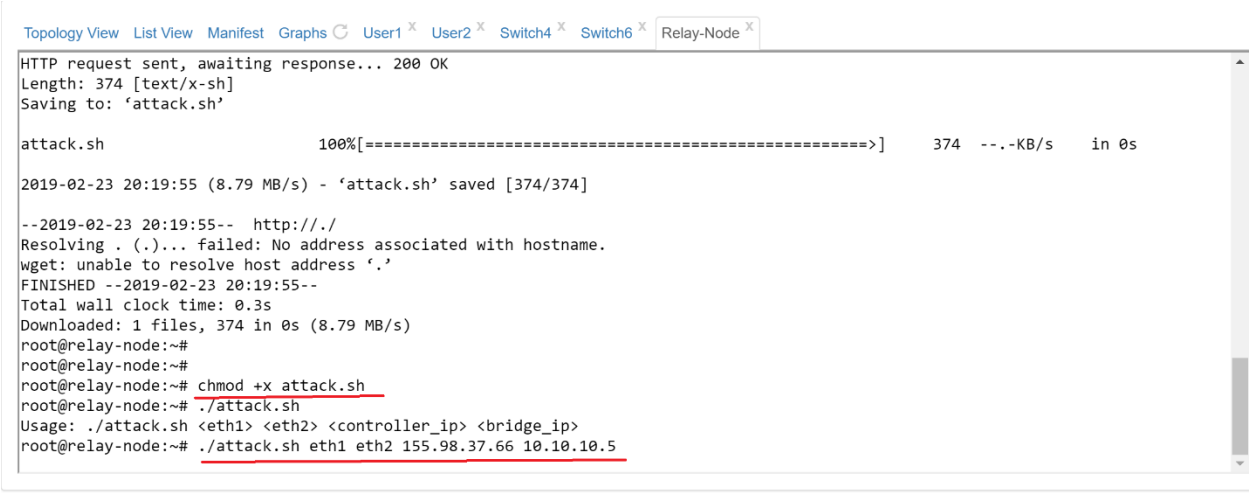


Figure 22: Download attack.sh, change permission, and run the attack.sh script.

5) Wait for a minute to let the attack take effect.
6) PING from ***User1*** to ***User2*** again.
7) Observe the packets from the ***Relay node***.
8) Observe the packets from ***Switch6*** or ***Switch4***.

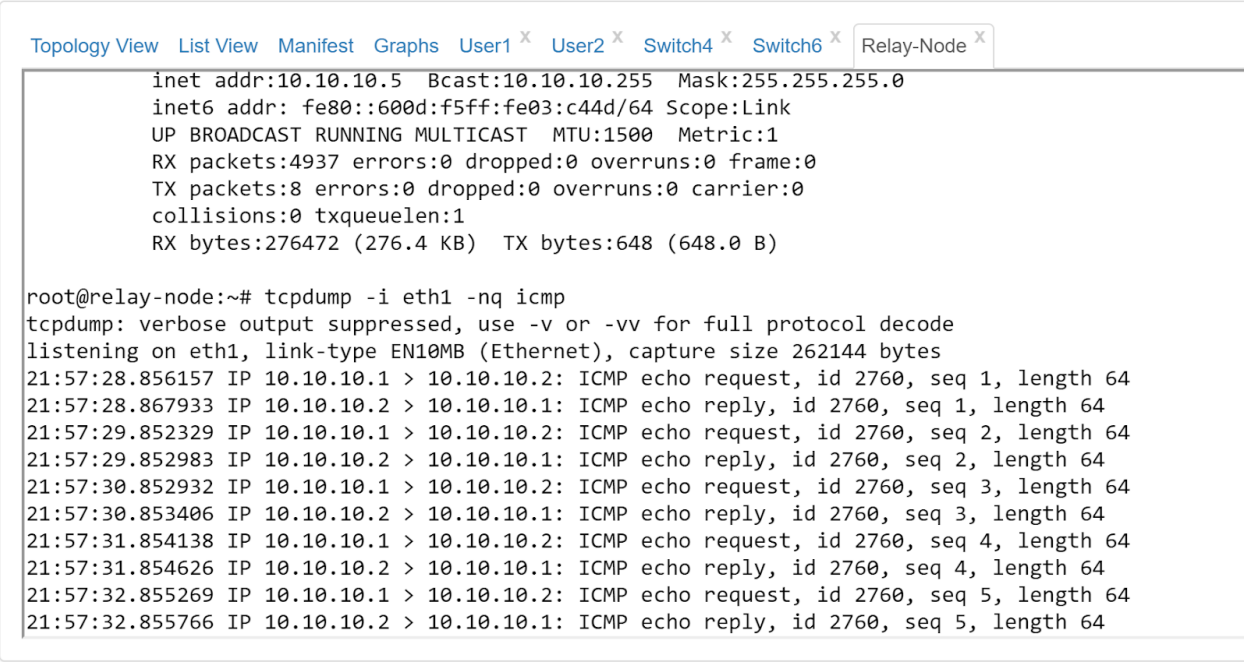


Figure 23: Packets observed from Relay Node

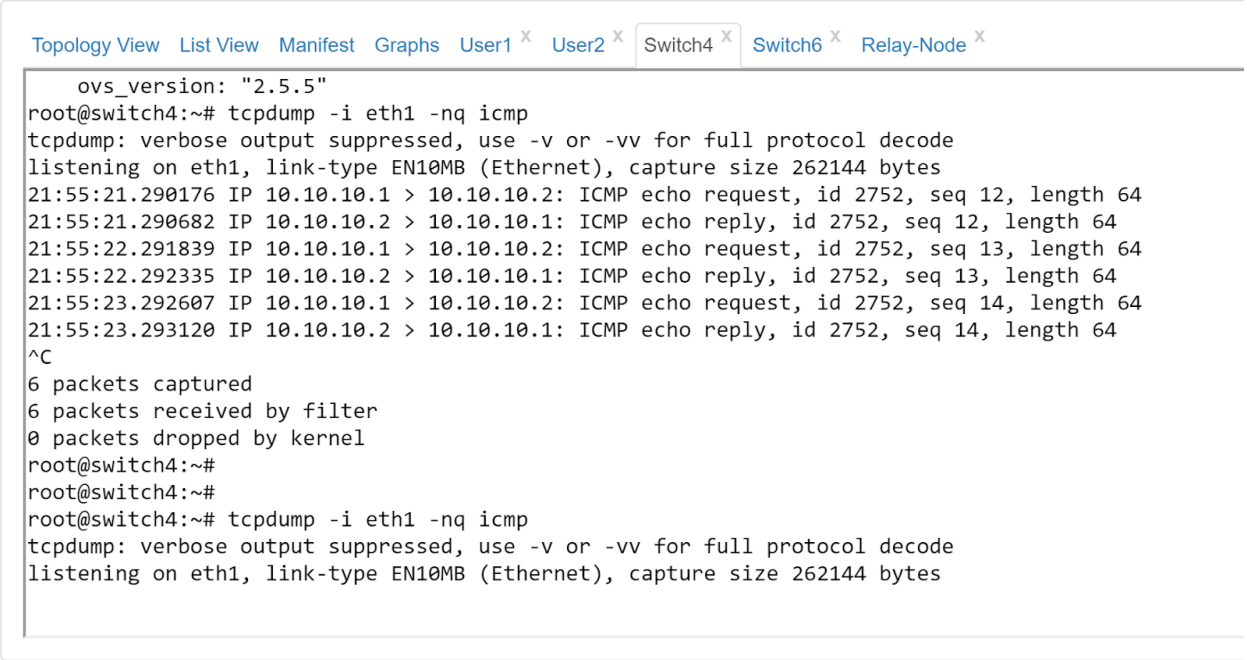


Figure 24: Packets observed from Switch4 or Switch6

Working:

In the second scenario, when the relay node is connected to the controller, the controller tends to route the packets through the shortest path which is through the relay node. In this case the packets are routed from source to destination and the relay node is capable of sniffing the raffic flowing between the two nodes. Hence, this acts as Man-in-the-middle, making no changes to the
traffic flow, but capable of sniffing it.