

TP2 - Network Managment

F. Ferraz PG46512, J. Martins PG47916, and M. Alves PG45516

Departamento de Informática, Universidade do Minho

Abstract. The goal of this work is to refine your knowledge of the OpenFlow protocol and SDN architecture. To that end, this assignment focus in the development of a routing application and a firewall on top of the SDN controller.

1 Introduction

In this exercise, the goal would be to develop a firewall to be implemented in the following infrastructure:

A corporate structure network with three departments, Executive, Research and Development (RD) and Customer Support. RD develops a product and stores the release versions on the HTTP1 server. As the name implies, this server has an HTTP API so that the CEO (H8) can track the product development, and the Customer Support Administrator (H5) can report bugs and user suggestions.

2 Exercise 2

The goal of this exercise is to create a firewall capable of blocking all the traffic between Networks (A, B and C) and only allow HTTP traffic to a specific port from H8 and H5 to HTTP1.

2.1 Strategy

Our strategy started by defining the topology, and in this step we encountered our first problem. Since we couldn't do the first exercise in this practical work, we couldn't use the topology mentioned in this practical exercise, and the problem was that we couldn't get the three routers to communicate with each other, and without this step it wouldn't be possible to do the topology because the networks would be completely separated from each other.

And for that reason we opted to use the topology mentioned in exercise 2 of the first practical work, with that being:

This topology differs from the one mentioned by this paper in that all networks are located on the same router and only there are packets exchanged between networks.

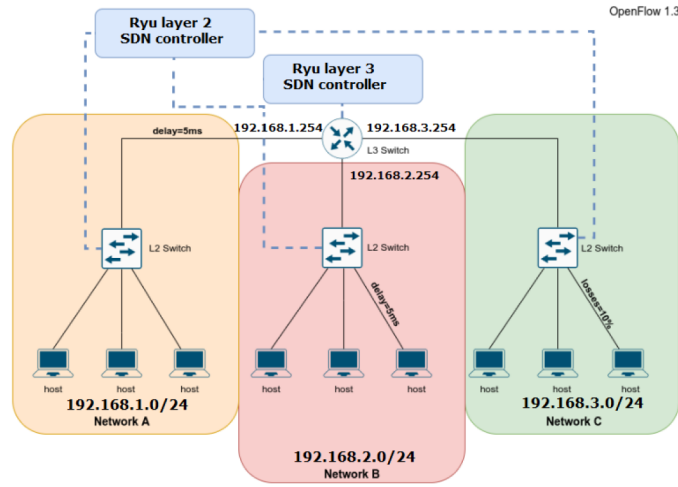


Fig. 1. Topology

2.2 Implementation

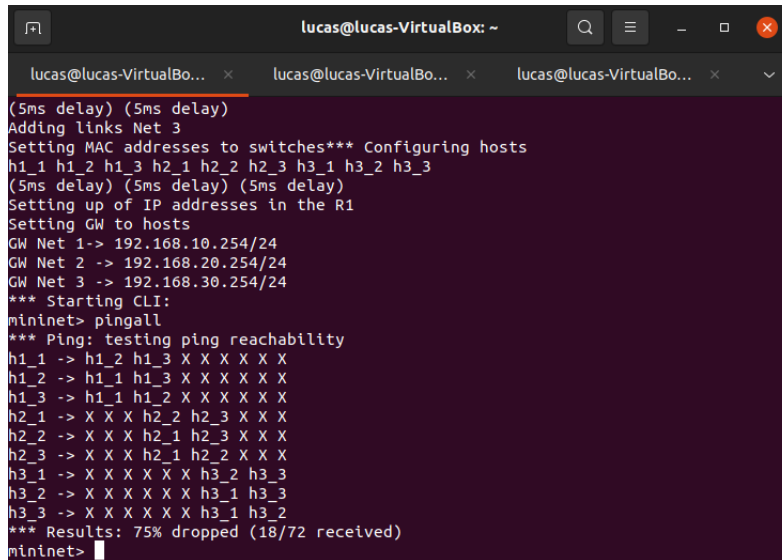
The firewall implementation was achieved by injecting blocking and TCP access rules into the switches with different priorities. That is, a blocking rule was injected to block all kinds of traffic between different networks, only allowing them to communicate within the same network. And then, with a higher priority, a rule was injected allowing certain authorized hosts to communicate with the server through port 5555.

This will result in all traffic that is not from a particular authorized host to the server with port 5555 in use being blocked.

2.3 Tests

During our tests of the function, it was possible to block the communication between different networks. That can be verified on the below image, where the pings only have answer when within the same network.

In terms of allowing TCP traffic between the networks, that couldn't be verified with any of the performed tests. The group thinks that the code made meets the rules proposed in the exercise and according to the research done, however the error could not be traced, so unfortunately the practical work was not thus completed. The research done on this topic proved to be useful in giving us knowledge about this topic.



```

lucas@lucas-VirtualBox: ~
(5ms delay) (5ms delay)
Adding links Net 3
Setting MAC addresses to switches*** Configuring hosts
h1_1 h1_2 h1_3 h2_1 h2_2 h2_3 h3_1 h3_2 h3_3
(5ms delay) (5ms delay) (5ms delay)
Setting up of IP addresses in the R1
Setting GW to hosts
GW Net 1-> 192.168.10.254/24
GW Net 2 -> 192.168.20.254/24
GW Net 3 -> 192.168.30.254/24
*** Starting CLI:
mininet> pingall
*** Ping: testing ping reachability
h1_1 -> h1_2 h1_3 X X X X X
h1_2 -> h1_1 h1_3 X X X X X
h1_3 -> h1_1 h1_2 X X X X X
h2_1 -> X X X h2_2 h2_3 X X X
h2_2 -> X X X h2_1 h2_3 X X X
h2_3 -> X X X h2_1 h2_2 X X X
h3_1 -> X X X X X h3_2 h3_3
h3_2 -> X X X X X h3_1 h3_3
h3_3 -> X X X X X h3_1 h3_2
*** Results: 75% dropped (18/72 received)
mininet>

```

Fig. 2. Pings result

3 Conclusion

To conclude this work, the group decided to try to develop the second exercise only due to time constraints the group managed to activate the firewall and implement the part where the networks can only communicate with the hosts inside the networks. The second part of the firewall where the hosts 8 and 5 can communicated with the http server through port 5555 we tried to implement some code but while the group thinks it's well implemented we couldn't make it work. Even with these difficulties the group still investigated both exercises and learn some things about how firewalls can be deployed inside these switches in SDN's.