ACL

Sumayyah Alahmadi [sfa8135@rit.edu](mailto:sfa8135@rit.edu)

CSEC.744.01

Professor Jonathan Weissman

**Table of contents**

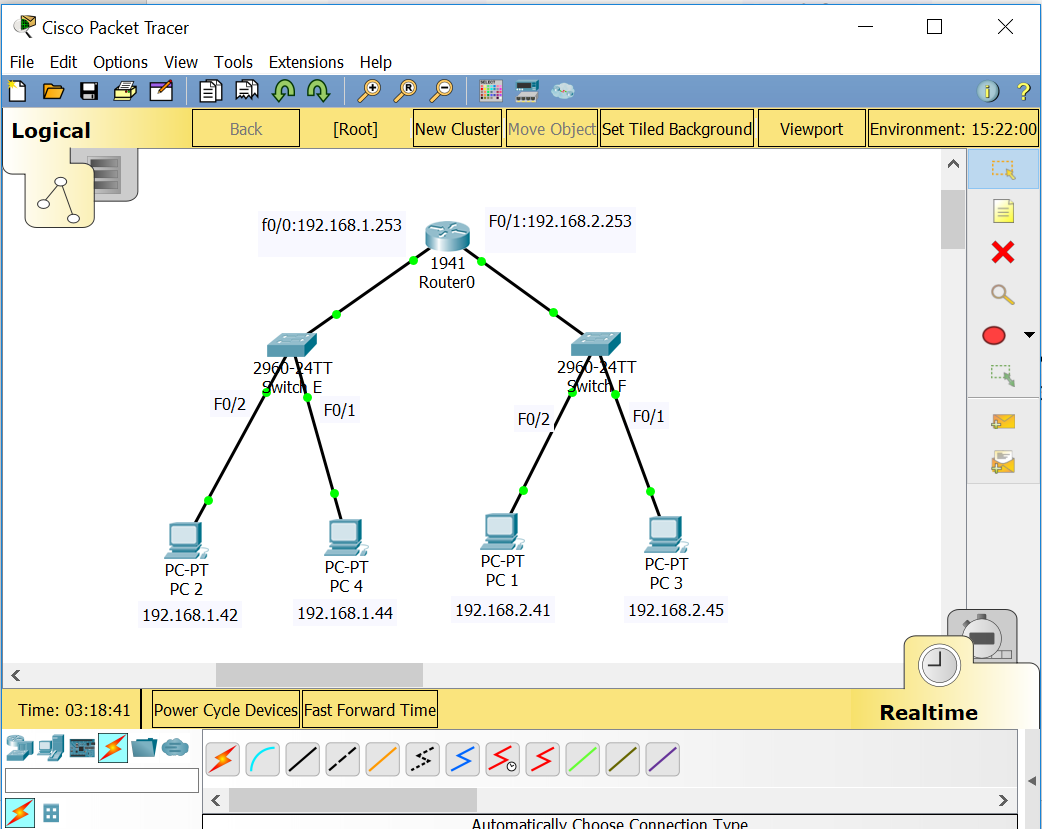
1. Concept….……………………………………………………………………………. 3
2. Implementation….……………………………………………………………………. 3
3. Conclusion……………………………………………………………………………. 16
4. References ……………………………………………………………………………. 16

Concept:

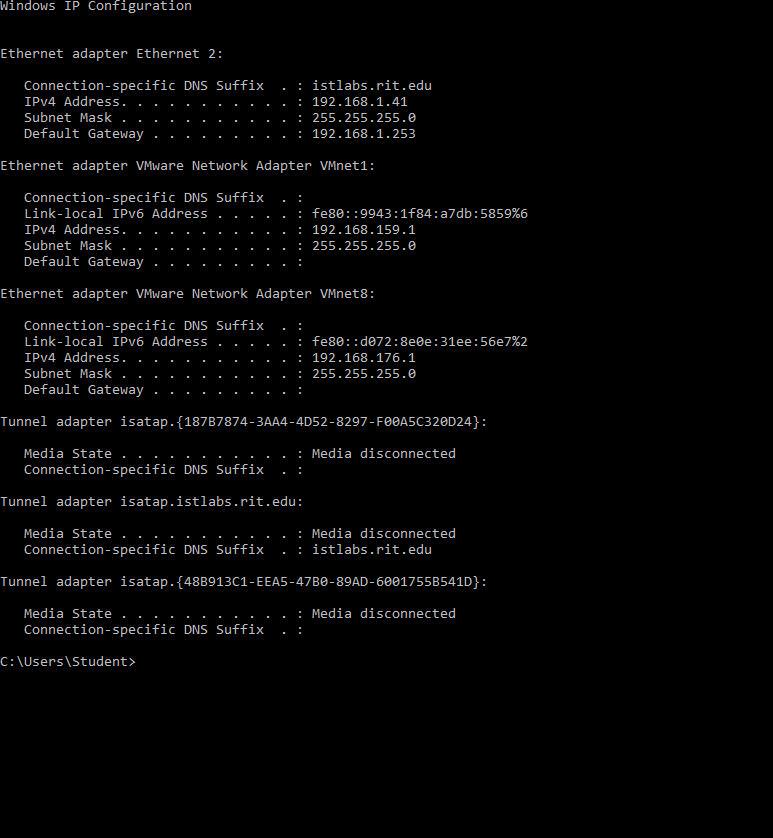
Access control tools is a powerful tool to emphases network security since it permits and deny access based on specific criteria. We can allow or prevent access depends on IP source, destination source, protocol or port. There are two types of ACL: standard and extended. Standard ACL puts regulation in the IP source only where in the extended ACL you can determine the source and destinations. Another difference between the standard and extended ACL is that standard ACL treat the traffic coming from a source as one packet where you cannot limit some protocols. On the other hand, ACL extended you can determine which protocol is allowed form the source and which protocol is denied. After writing all the conditions for the access control lists we end it by an implicit deny. In case of small network, we can deny specific IP address to go to unexcited destination which is known by blackhole route.

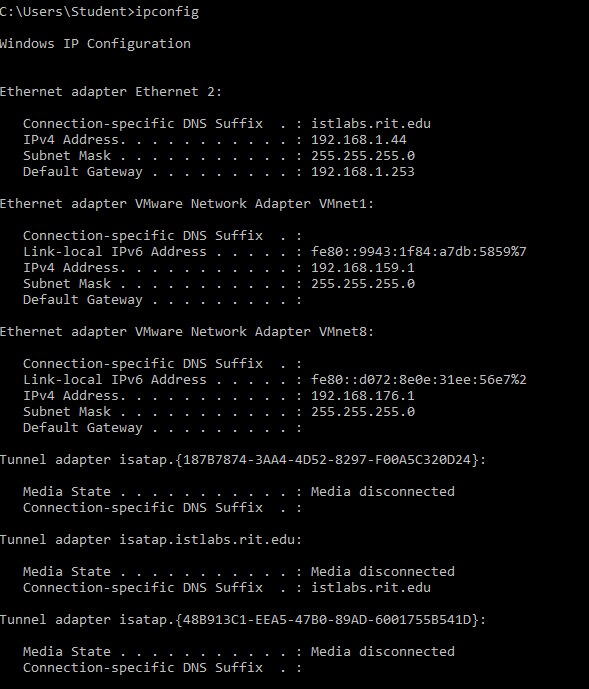
Implementation:

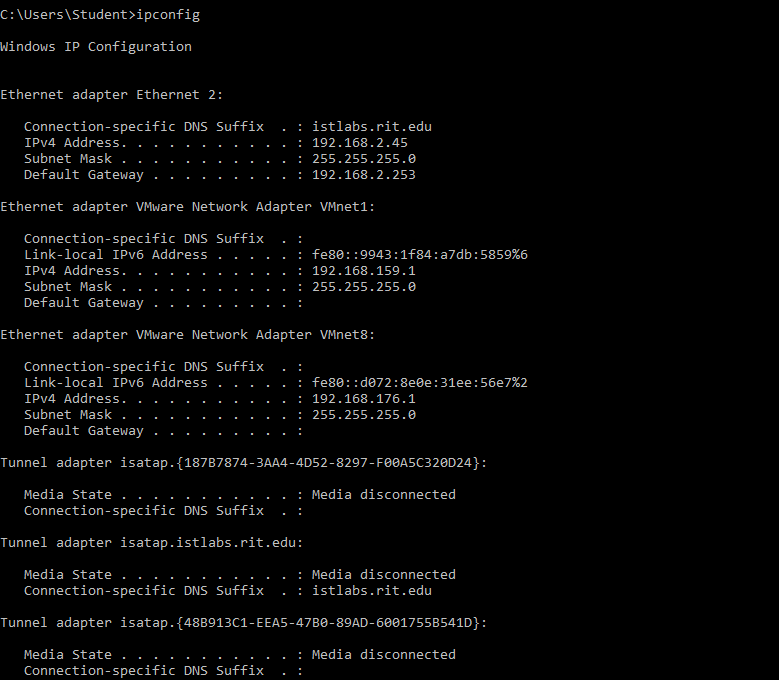
Topology



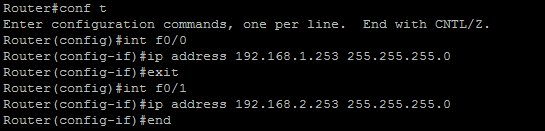
First we assign IP addresses for each hosts

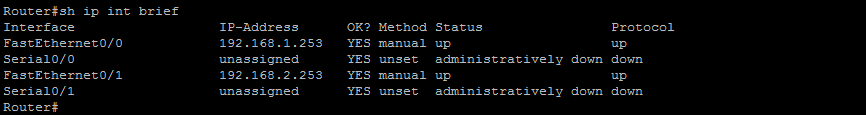




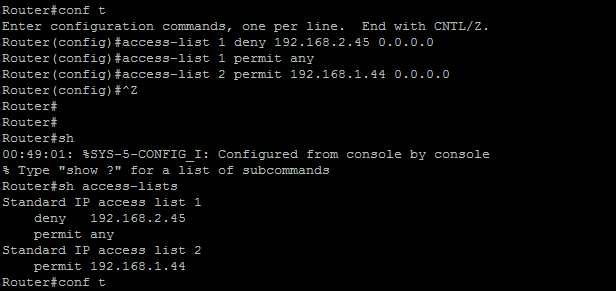


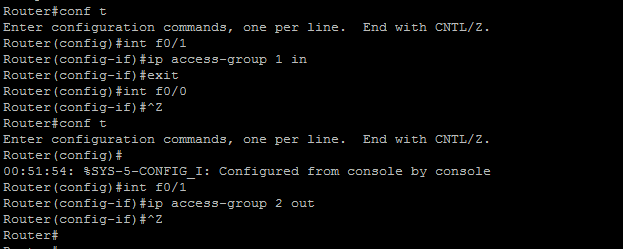
Then we assign IP address for two router interfaces

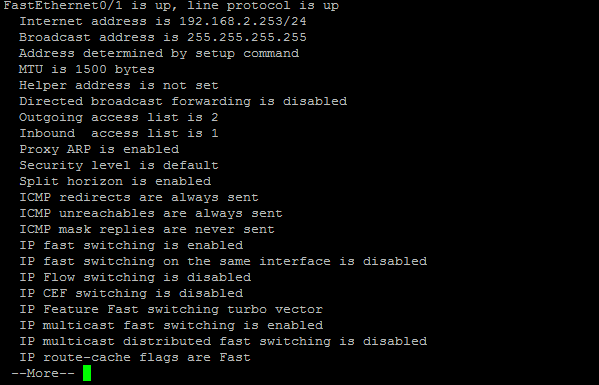


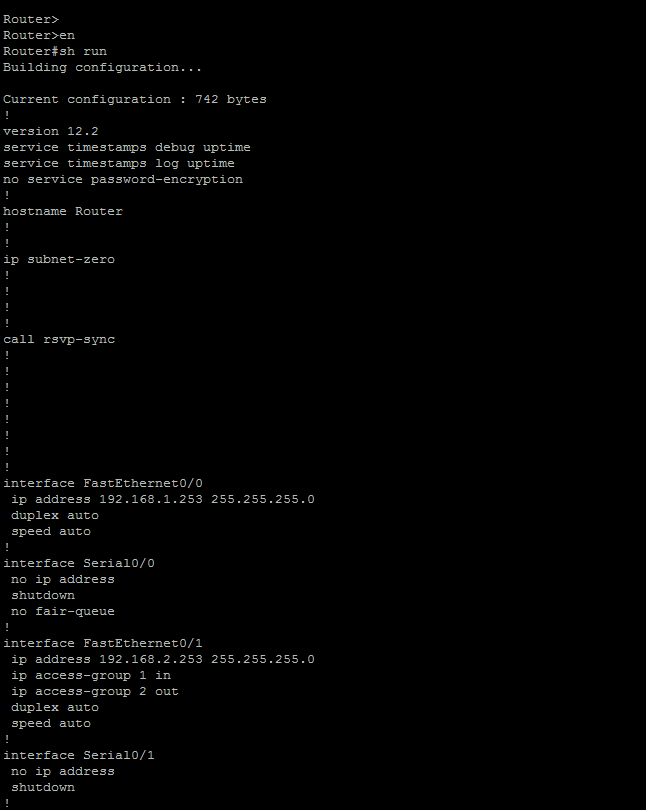


Then we start by implementing standard ACL where we permit all traffic but 192.168.2.45 on F0/1 inbound traffic.

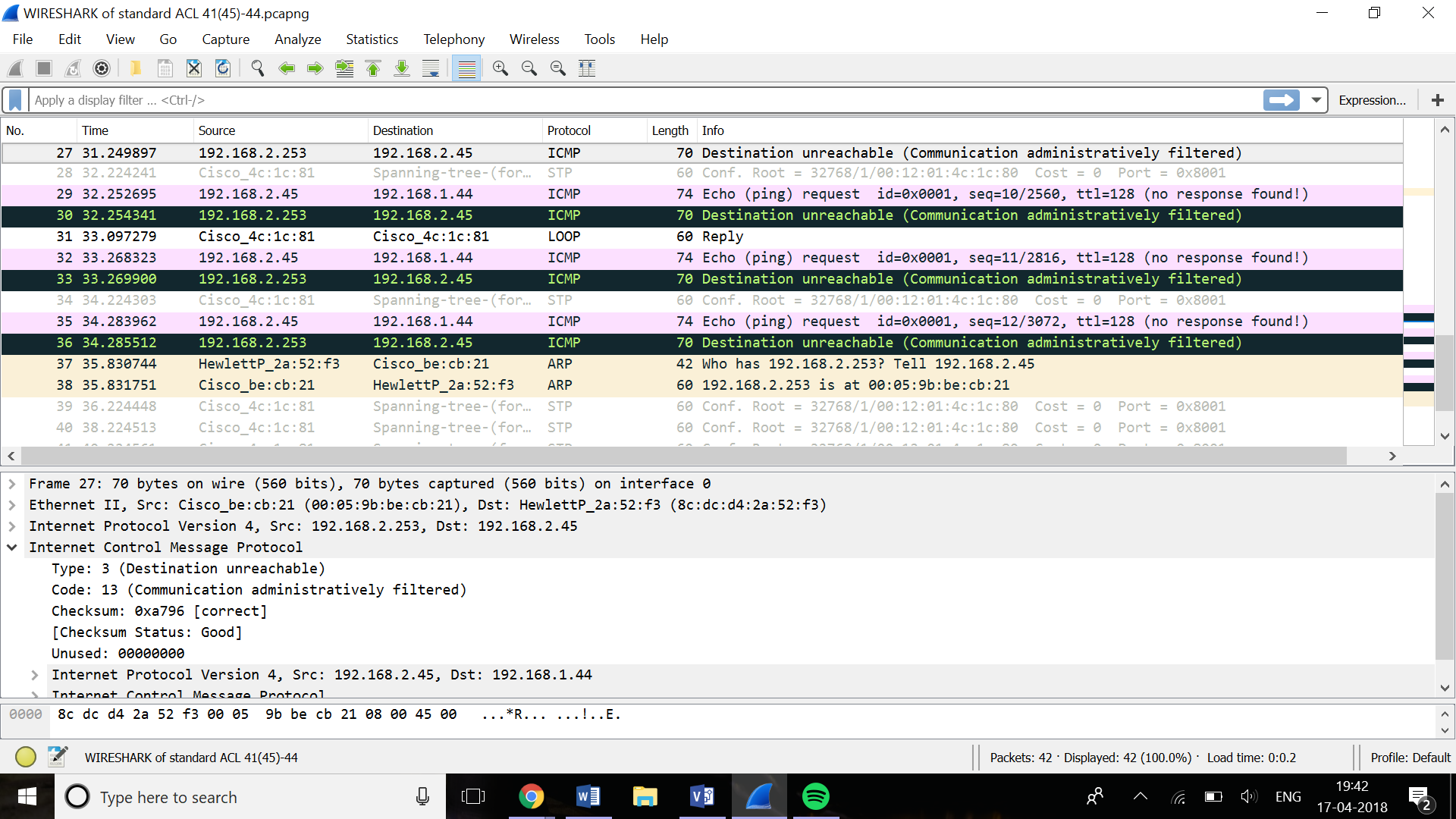


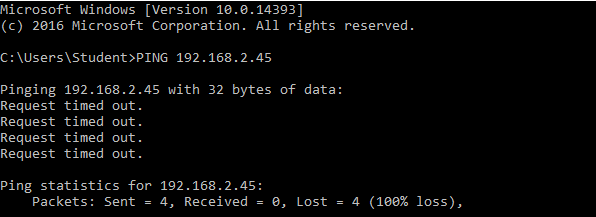






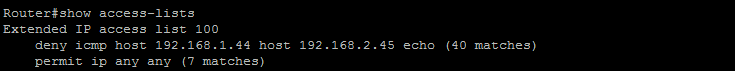
Here in wireshark we coming traffic by 192.168.2.45 are bloked

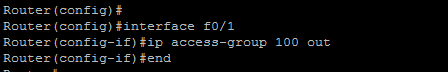


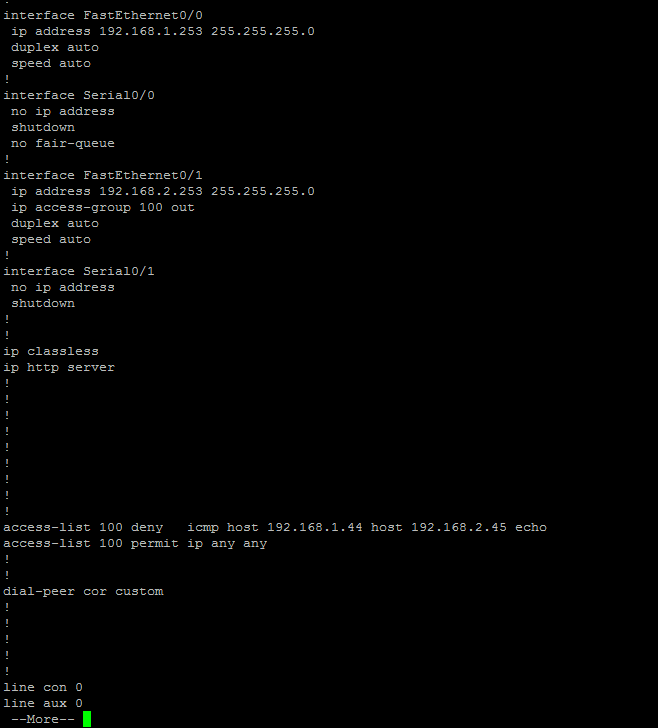


Also we notice here the ping faild for 192.168.2.45 by the standard ACL.

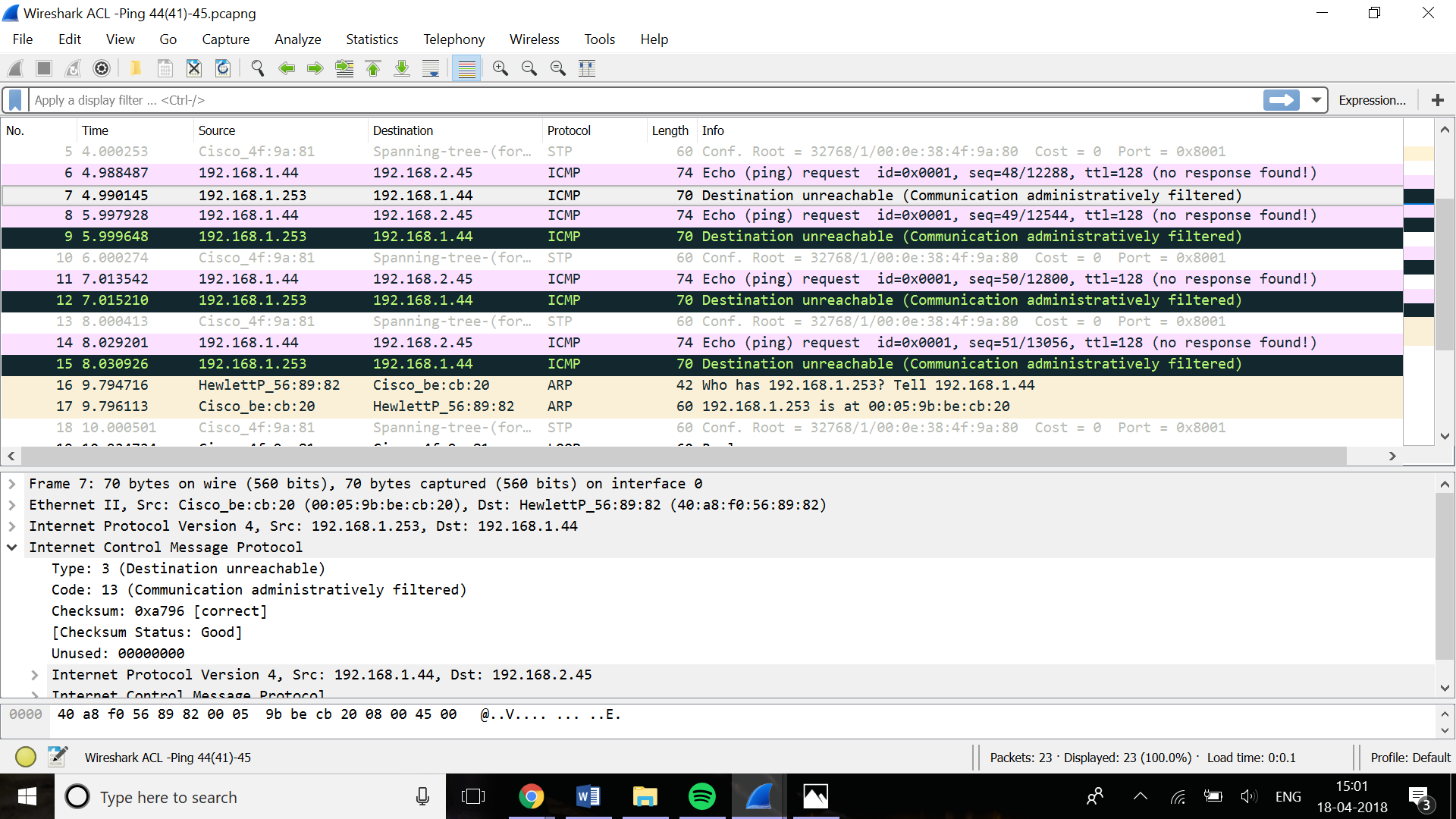
Also, we implement extended ACL to permit any IP exept ICMP from 192.168.1.44 to 192.168.2.45 on outbound traffic for F01 interface.

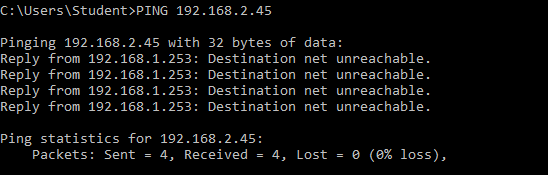






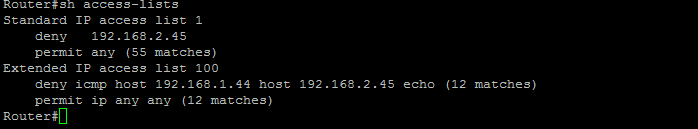
Here in Wireshark we notice that ICMP traffic is blocked from 192.168.1.44 to 192.168.2.45

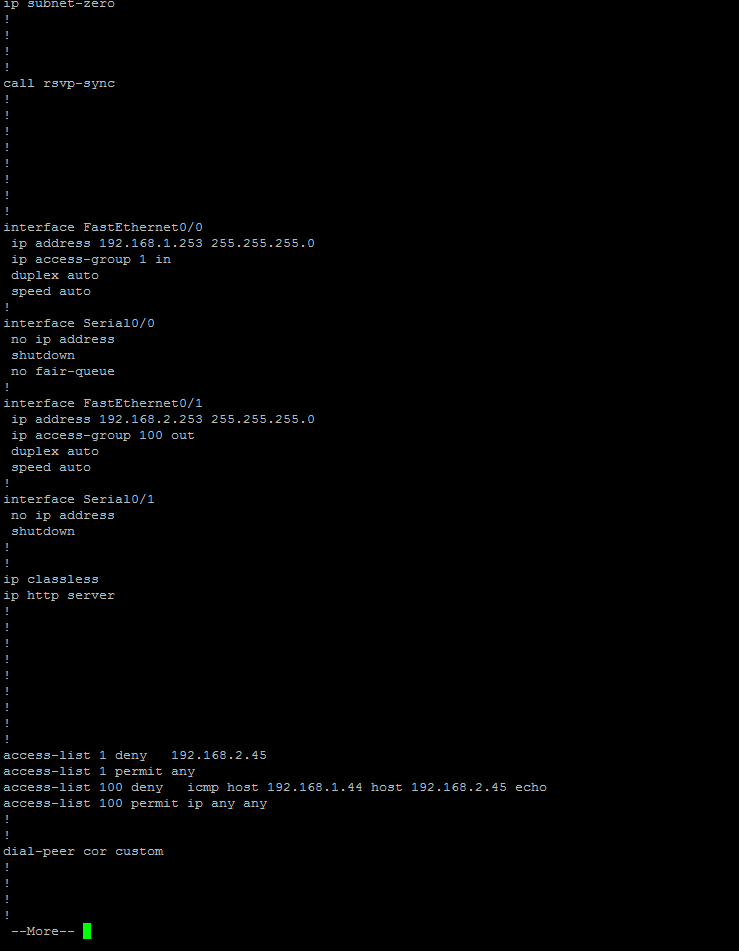


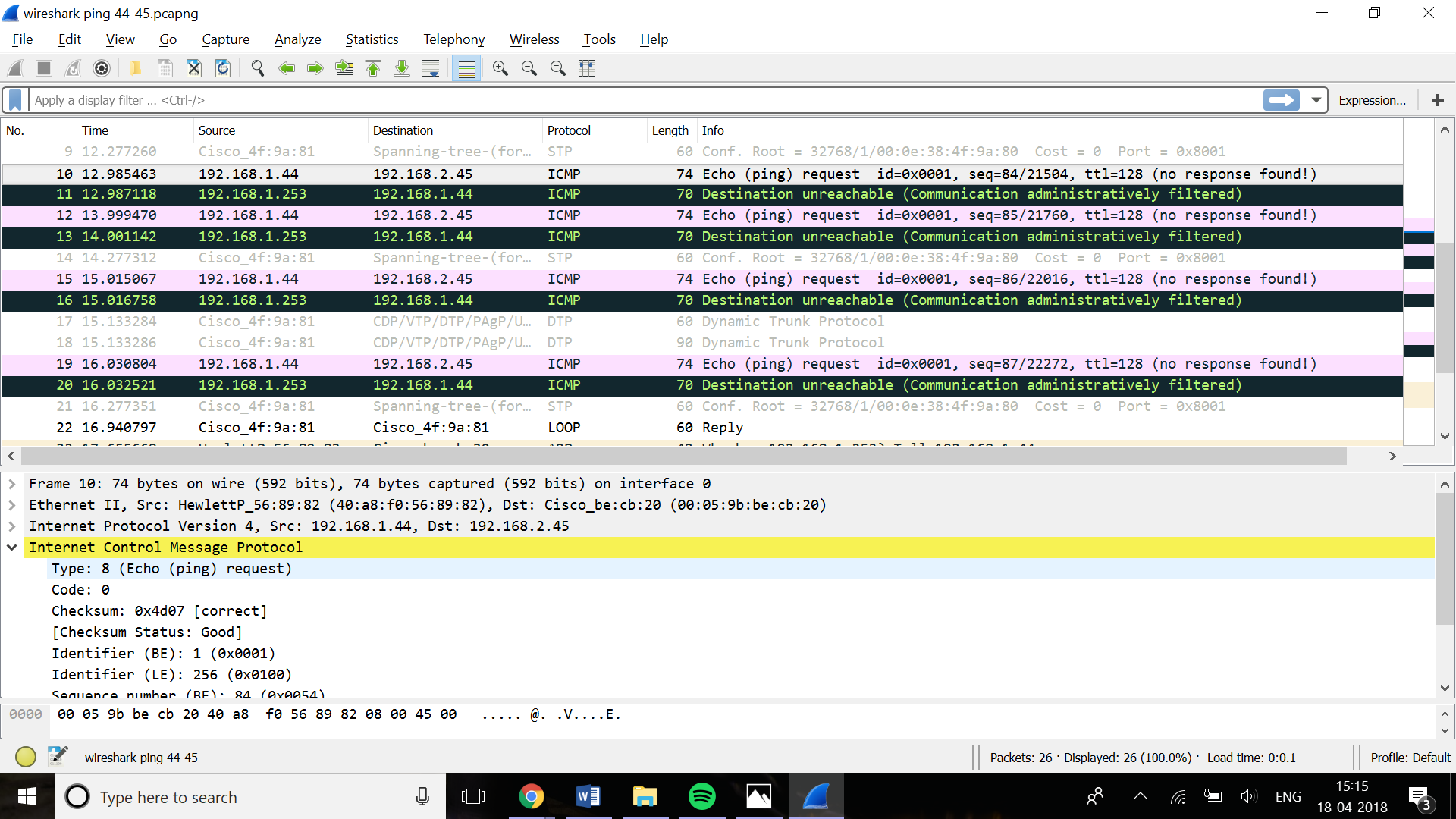


And we notice the ping failed as well

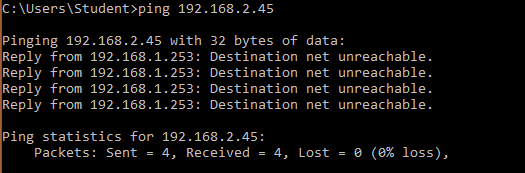
Then we combined both standard and extended ACL



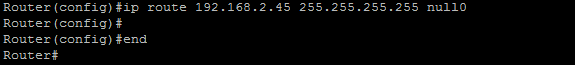


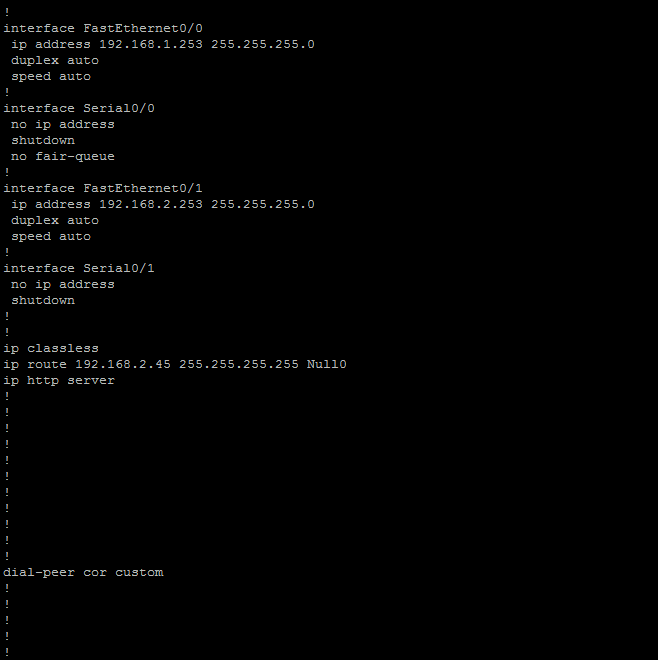


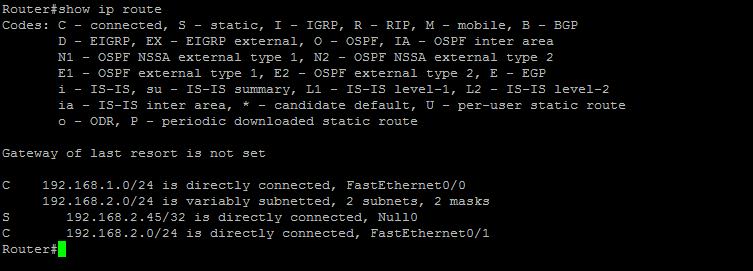
Wireshark show blocked traffic from192.168.1.44 to 192.168.2.45 by ACLs as well as failed ping



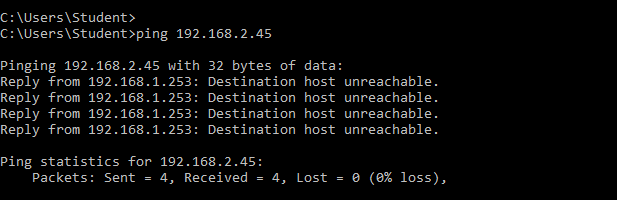
Then we create blackhole route (null route) for restricted traffic



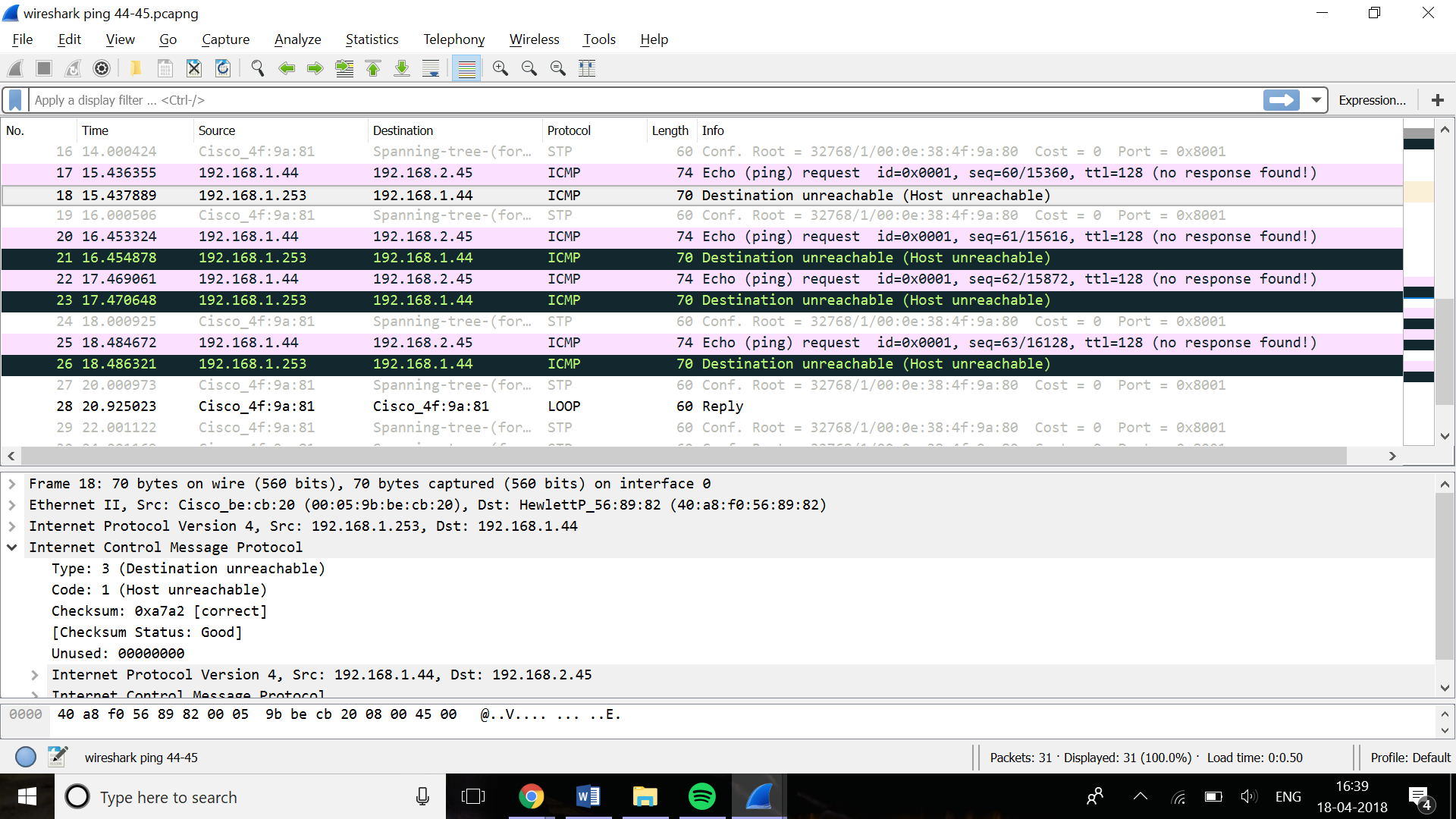




routing table show the blackhole route that we created



Ping to 192.168.2.45 is failed



Wireshark show traffic to 192.168.2.45 being directed to the specified blackhole route

Conclusion:

In this report, we applied ACL concept by creating a topology of a routers and two switches each of them connected with 2 hosts. Then, we wrote two ACL, standard and extended to permit and deny some hosts in the network. We show the command, router configuration and Wireshark captures. ACL is a great mechanism to secure the network and filter unwanted traffic. Then we create a blackhole route where we direct unwanted traffic to unexcited IP address. Comparing to ACL deny, null interface can be fast implemented but it’s not scalable so it’s better using for small network. Also, ACL apply host by host so it is not as effecint and easy to implement as blackhole. ACL costs more than blackhole. ACL can be filtered by IP source or destination, port and protocol while blackhole only filtered by network.

References:

ACLs slides and lecture notes.

|  |
| --- |
|  |