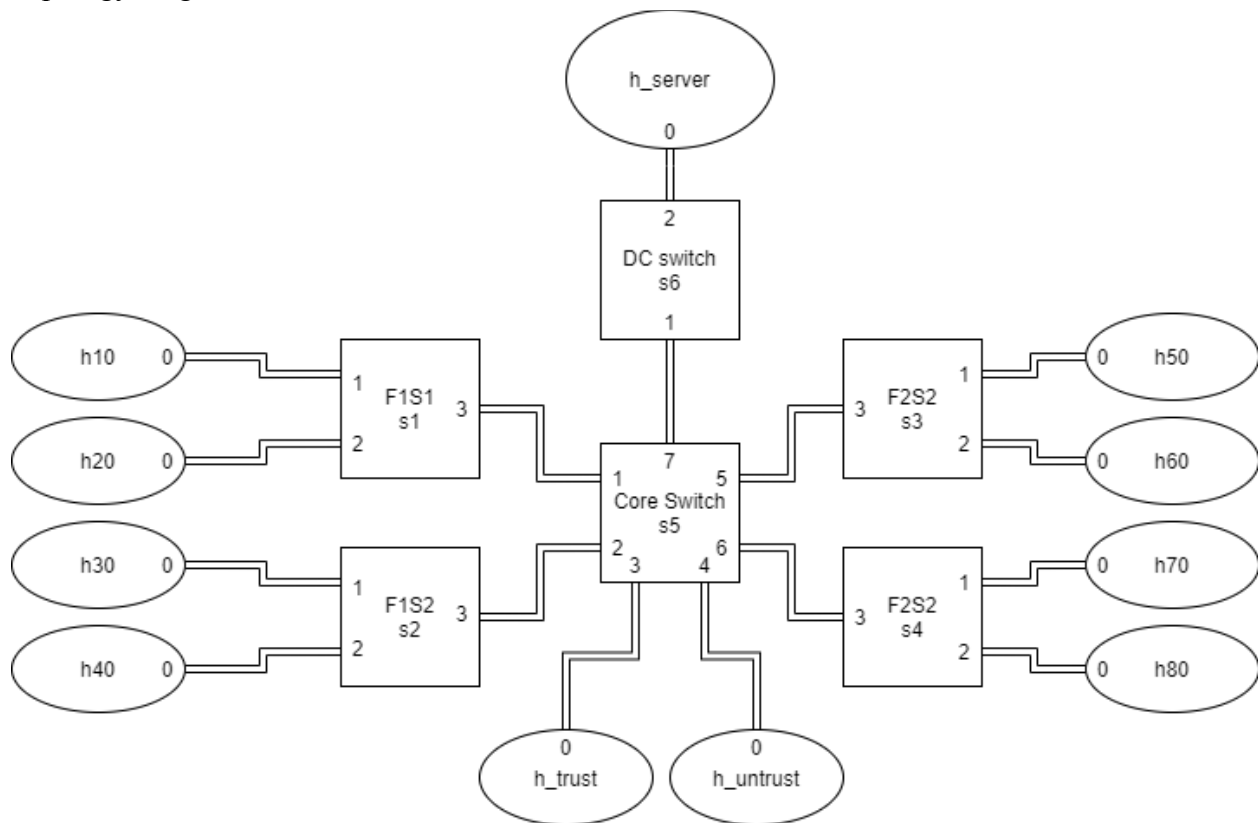


Yaroslav Yanin  
CSE150  
12/09/20

## Final Project Report

Topology diagram:



The topology diagram above shows switch names, host names, and used ports.

Pingall output:

```
mininet@mininet-vm: ~/Desktop/FinalLab
File Edit Tabs Help

1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 21.055/21.055/21.055/0.000 ms
mininet> h_trust ping -c 1 h_untrust
PING 106.44.82.103 (106.44.82.103) 56(84) bytes of data.
64 bytes from 106.44.82.103: icmp_seq=1 ttl=64 time=5.03 ms

--- 106.44.82.103 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 5.032/5.032/5.032/0.000 ms
mininet> pingall
*** Ping: testing ping reachability
h10 -> h20 h30 h40 X X X X h_server h_trust X
h20 -> h10 h30 h40 X X X X h_server h_trust X
h30 -> h10 h20 h40 X X X X h_server h_trust X
h40 -> h10 h20 h30 X X X X h_server h_trust X
h50 -> X X X X h60 h70 h80 h_server X X
h60 -> X X X X h50 h70 h80 h_server X X
h70 -> X X X X h50 h60 h80 h_server X X
h80 -> X X X X h50 h60 h70 h_server X X
h_server -> h10 h20 h30 h40 h50 h60 h70 h80 X X
h_trust -> h10 h20 h30 h40 X X X X h_untrust
h_untrust -> X X X X X X X X X h_trust
*** Results: 54% dropped (50/110 received)
mininet>
```

The pingall command sends ICMP traffic from each host to other hosts. This creates a chart that perfectly represents the established rules. The untrusted host(h\_untrust) is unable to send any ICMP traffic to any of the other hosts. Department A is unable to send ICMP traffic to the department B and vice versa. Both departments are able to communicate with each other and send ICMP traffic to the server. The trusted host(u\_trust) is able to communicate with the department A(h10-h40) and is unable to communicate with the department B(h50-h80). The trusted host is also unable to send ICMP traffic to the server. The untrusted host can communicate with the trusted host and vice versa.

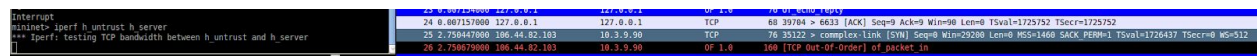
Iperf h10 to h\_server:

```
mininet> iperf h10 h_server
iperf: testing TCP bandwidth between h10 and h_server
*** Results: [ 38.3 Gbit/sec ]
mininet> iperf h10 h_server
iperf: testing TCP bandwidth between h10 and h_server
*** Results: [ 38.3 Gbit/sec ]
mininet> iperf h10 h_server
iperf: testing TCP bandwidth between h10 and h_server
*** Results: [ 38.3 Gbit/sec ]
mininet> iperf h10 h_server
iperf: testing TCP bandwidth between h10 and h_server
*** Results: [ 38.3 Gbit/sec ]
mininet>
```

14670	11.40931900	10.3.3.0	TCP	60	[TCP Seq=4360595] complex-link > 43603 [ACK] Seq=1 Ack=341327889 Win=7902720 Len=0 TVal=228352 TSecr=228352
14671	11.40932300	10.3.3.0	TCP	65228	42963 > complex-link [ACK] Seq=341332209 Ack=1 Win=28696 Len=65160 TVal=228352 TSecr=228352
14672	11.40932700	10.3.3.0	TCP	65228	42963 > complex-link [ACK] Seq=341332209 Ack=1 Win=28696 Len=65160 TVal=228352 TSecr=228352
14673	11.40932800	10.3.3.0	TCP	65228	42963 > complex-link [ACK] Seq=341332209 Ack=1 Win=28696 Len=65160 TVal=228352 TSecr=228352
14674	11.40933400	10.3.3.0	TCP	65228	42963 > complex-link [ACK] Seq=341332209 Ack=1 Win=28696 Len=65160 TVal=228352 TSecr=228352
14675	11.40933800	10.3.3.0	TCP	65228	42963 > complex-link [ACK] Seq=341332209 Ack=1 Win=28696 Len=65160 TVal=228352 TSecr=228352
14676	11.40934000	10.3.3.0	TCP	65228	42963 > complex-link [ACK] Seq=341332209 Ack=1 Win=28696 Len=65160 TVal=228352 TSecr=228352
14677	11.40934200	10.3.3.0	TCP	65228	42963 > complex-link [ACK] Seq=341332209 Ack=1 Win=28696 Len=65160 TVal=228352 TSecr=228352
14678	11.40934400	10.3.3.0	TCP	65228	42963 > complex-link [ACK] Seq=341332209 Ack=1 Win=28696 Len=65160 TVal=228352 TSecr=228352
14679	11.40934600	10.3.3.0	TCP	65228	42963 > complex-link [ACK] Seq=341332209 Ack=1 Win=28696 Len=65160 TVal=228352 TSecr=228352
14680	11.40934800	10.3.3.0	TCP	65228	42963 > complex-link [ACK] Seq=341332209 Ack=1 Win=28696 Len=65160 TVal=228352 TSecr=228352
14681	11.40935000	10.3.3.0	TCP	65228	42963 > complex-link [ACK] Seq=341332209 Ack=1 Win=28696 Len=65160 TVal=228352 TSecr=228352
14682	11.40935200	10.3.3.0	TCP	65228	42963 > complex-link [ACK] Seq=341332209 Ack=1 Win=28696 Len=65160 TVal=228352 TSecr=228352
14683	11.40935400	10.3.3.0	TCP	65228	42963 > complex-link [ACK] Seq=341332209 Ack=1 Win=28696 Len=65160 TVal=228352 TSecr=228352
14684	11.40935600	10.3.3.0	TCP	65228	42963 > complex-link [ACK] Seq=341332209 Ack=1 Win=28696 Len=65160 TVal=228352 TSecr=228352
14685	11.40935800	10.3.3.0	TCP	65228	42963 > complex-link [ACK] Seq=341332209 Ack=1 Win=28696 Len=65160 TVal=228352 TSecr=228352
14686	11.40936000	10.3.3.0	TCP	65228	42963 > complex-link [ACK] Seq=341332209 Ack=1 Win=28696 Len=65160 TVal=228352 TSecr=228352
14687	11.40936200	10.3.3.0	TCP	65228	42963 > complex-link [ACK] Seq=341332209 Ack=1 Win=28696 Len=65160 TVal=228352 TSecr=228352

Here is the successful connection between a floor host and a server as seen through wireshark

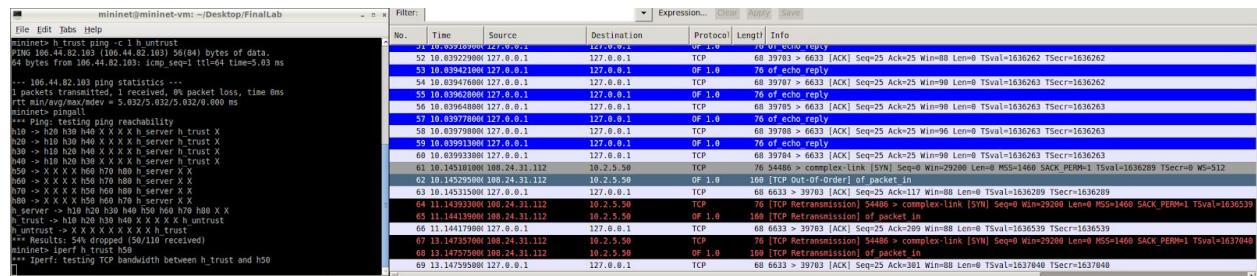
## Iperf h\_untrust to h\_server:



No.	Time	Source	Destination	Protocol	Length	Info
24	0.007157000	127.0.0.1	127.0.0.1	TCP	60	39784 > 6633 [ACK] Seq=9 Ack=9 Win=98 Len=0 TSval=1725752 TSecr=1725752
25	2.750447000	106.44.82.103	10.3.9.90	TCP	76	35122 > complex-link [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1726437 TSecr=0 WS=512
26	2.750679000	106.44.82.103	10.3.9.90	OF	1.0	100 [TCP Out-Of-Order] of packet in

As shown in the screenshot above, the packet is dropped when transmitted from h\_untrust to the server. This shows that no IP traffic from h\_untrust will reach the server.

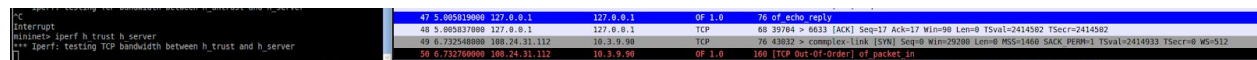
## Iperf h\_trust to h50:



No.	Time	Source	Destination	Protocol	Length	Info
24	0.007157000	127.0.0.1	127.0.0.1	TCP	60	39784 > 6633 [ACK] Seq=9 Ack=9 Win=98 Len=0 TSval=1725752 TSecr=1725752
25	2.750447000	106.44.82.103	10.3.9.90	TCP	76	35122 > complex-link [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1726437 TSecr=0 WS=512
26	2.750679000	106.44.82.103	10.3.9.90	OF	1.0	100 [TCP Out-Of-Order] of packet in

As seen in the screenshot above, a trusted host is capable of sending IP traffic to the department but, as shown before in pingall, is not capable of sending ICMP traffic that way.

## Iperf h\_trust to h\_server:



No.	Time	Source	Destination	Protocol	Length	Info
24	0.007157000	127.0.0.1	127.0.0.1	TCP	60	39784 > 6633 [ACK] Seq=9 Ack=9 Win=98 Len=0 TSval=1725752 TSecr=1725752
25	2.750447000	106.44.82.103	10.3.9.90	TCP	76	35122 > complex-link [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1726437 TSecr=0 WS=512
26	2.750679000	106.44.82.103	10.3.9.90	OF	1.0	100 [TCP Out-Of-Order] of packet in

As shown in the screenshot, all IP traffic from the trusted host to the server is dropped.

## Conclusion:

As shown in the screenshots above, all the features of the pox controller have been met. The ping all command shows the flow of ICMP traffic. The untrusted host can only send ICMP traffic to the trusted host and nothing else, as required. As shown via iperf command and through the use of wireshark, the untrusted host can't send any IP traffic to the server. The trusted host is not able to send any ICMP traffic to the Department B or the server. As shown via iperf command and through the use of wireshark, the trusted host is unable to send IP traffic to the server. In the pingall chart, it is shown that hosts from department A can't communicate with the hosts from department B and vice versa.