Exercise: Firewall

- Topology is the same as that used for loadbalancing

(40P) Simple firewall

-
- We will be using the load-balancer experiment as basis
- put blocker.py (https://dl.dropboxusercontent.com/u/1652374/SDN_course_WS2015-2016/Exercises/ex3/blocker.py) in pox/ext/blocker.py

```
  $ sudo mn --topo single,6 --mac --arp --controller remote
  $ ./pox/pox.py forwarding.l2_learning blocker py (Note that there is
a space between blocker and py to enable interactive mode)
```

-
    -
    - or

```
  $ ./pox/pox.py forwarding.l2_learning blocker --ports=80,8888,8000
(not recommended)
```

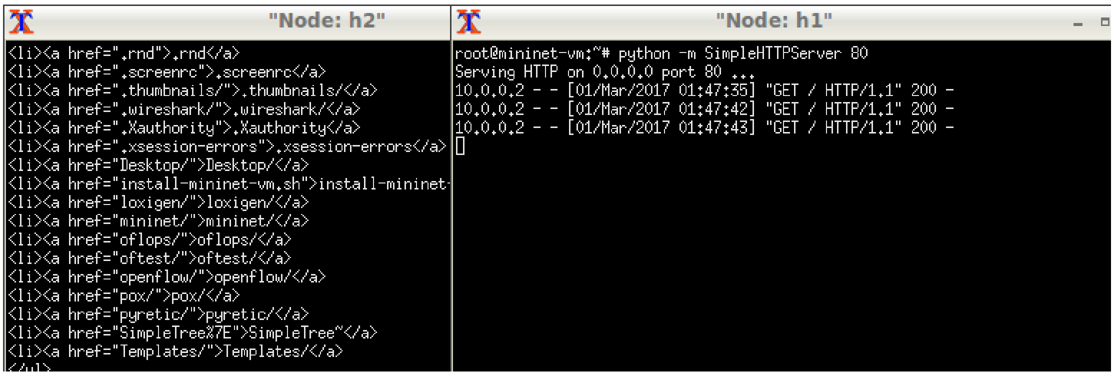
-
- start Webserver in h1

```
  h1$ python -m SimpleHTTPServer 80
```

-
- Try to perform curl or wget from h2 to h1

```
  h2$ curl 10.0.0.1
```

h2 has access to h2 through port 80.



```
<li><a href=".rnd">.rnd</a>
<li><a href=".screenrc">.screenrc</a>
<li><a href=".thumbnails/">.thumbnails/</a>
<li><a href=".wireshark/">.wireshark/</a>
<li><a href=".Xauthority">.Xauthority</a>
<li><a href=".xsession-errors">.xsession-errors</a>
<li><a href="Desktop/">Desktop/</a>
<li><a href="install-mininet-vm.sh">install-mininet-
<li><a href="loxigen/">loxigen/</a>
<li><a href="mininet/">mininet/</a>
<li><a href="oflops/">oflops/</a>
<li><a href="oftest/">oftest/</a>
<li><a href="openflow/">openflow/</a>
<li><a href="pox/">pox/</a>
<li><a href="pyretic/">pyretic/</a>
<li><a href="SimpleTree%7E">SimpleTree~</a>
<li><a href="Templates/">Templates/</a>
</ul>
```

```
root@mininet-vm:~# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.0.0.2 - - [01/Mar/2017 01:47:35] "GET / HTTP/1.1" 200 -
10.0.0.2 - - [01/Mar/2017 01:47:42] "GET / HTTP/1.1" 200 -
10.0.0.2 - - [01/Mar/2017 01:47:43] "GET / HTTP/1.1" 200 -
```

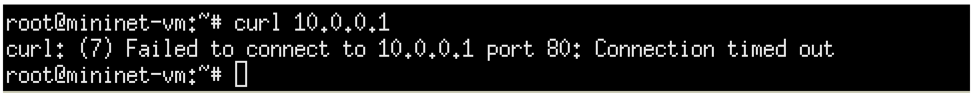
- Then block port 80 in pox controller

```
pox> block(80)
```

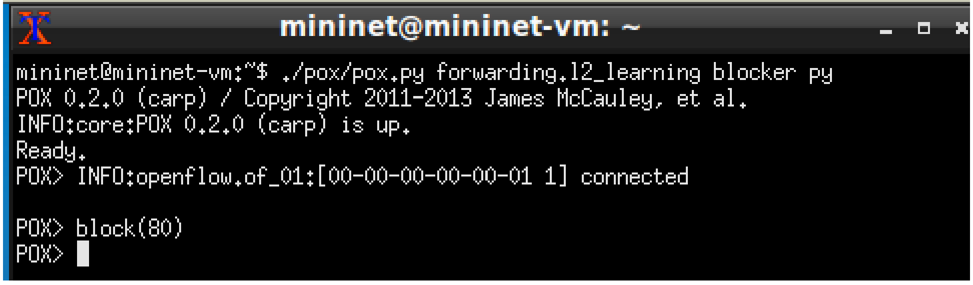
- Now, again try the following and report what happens

```
h2$ curl 10.0.0.1
```

We can see the port 80 is blocked.



```
root@mininet-vm:~# curl 10.0.0.1
curl: (7) Failed to connect to 10.0.0.1 port 80: Connection timed out
root@mininet-vm:~#
```



```
mininet@mininet-vm:~$ ./pox/pox.py forwarding.l2_learning blocker py
POX 0.2.0 (carp) / Copyright 2011-2013 James McCauley, et al.
INFO:core:POX 0.2.0 (carp) is up.
Ready.
POX> INFO:openflow.of_01:[00-00-00-00-00-01 1] connected

POX> block(80)
POX>
```

(60P) Advanced Firewall (I will give you hints)

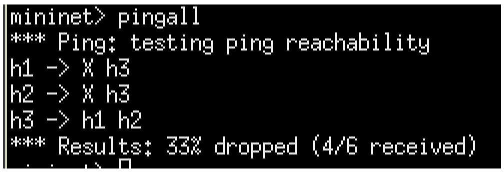
- Topology [1]
- Aim: Implement a layer 2 firewall that runs alongside the MAC learning module on the POX OpenFlow Controller. Your firewall should be agnostic to the underlying topology. Take MAC pair list as input and install it on the switches in the network
- Note that MAC learning can be done in conjunction with firewall. Therefore you might have to assign priority to each application.
- Copy firewall.py from [2] into pox/pox/misc folder
- Start editing firewall.py
    - Write code to block h1 to h2 (Mac IDs: 00:00:00:00:00:01, 00:00:00:00:00:02)

- Do the following to quickly test code

```
$ ./pox/pox.py --verbose forwarding.l2_learning misc.firewall
$ sudo mn --topo single,3 --controller remote --mac
$ dpctl dump-flows tcp:127.0.0.1:6634
```

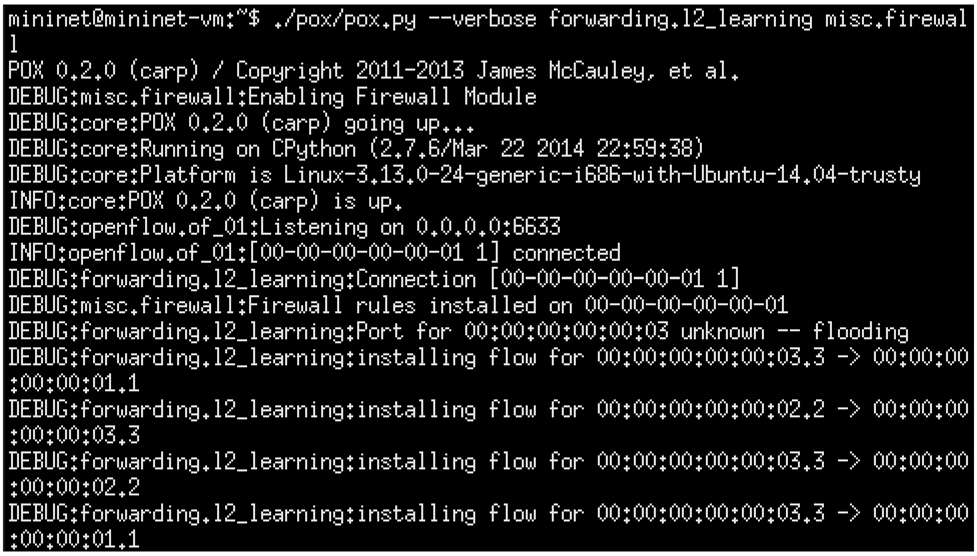
Because ping command will block the ack from h1 to h2 when h2 ping h1. So generally in this layer it is hard to achieve that goal.

The code is in the attachment.



```
mininet> pingall
*** Ping: testing ping reachability
h1 -> X h3
h2 -> X h3
h3 -> h1 h2
*** Results: 33% dropped (4/6 received)
```

Screen shot from the controller side:



```
mininet@mininet-vm:~$ ./pox/pox.py --verbose forwarding.l2_learning misc.firewal
l
POX 0.2.0 (carp) / Copyright 2011-2013 James McCauley, et al.
DEBUG:misc.firewall:Enabling Firewall Module
DEBUG:core:POX 0.2.0 (carp) going up...
DEBUG:core:Running on CPython (2.7.6/Mar 22 2014 22:59:38)
DEBUG:core:Platform is Linux-3.13.0-24-generic-i686-with-Ubuntu-14.04-trusty
INFO:core:POX 0.2.0 (carp) is up.
DEBUG:openflow.of_01:Listening on 0.0.0.0:6633
INFO:openflow.of_01:[00-00-00-00-00-01 1] connected
DEBUG:forwarding.l2_learning:Connection [00-00-00-00-00-01 1]
DEBUG:misc.firewall:Firewall rules installed on 00-00-00-00-00-01
DEBUG:forwarding.l2_learning:Port for 00:00:00:00:00:03 unknown -- flooding
DEBUG:forwarding.l2_learning:installing flow for 00:00:00:00:00:03.3 -> 00:00:00
:00:00:01.1
DEBUG:forwarding.l2_learning:installing flow for 00:00:00:00:00:02.2 -> 00:00:00
:00:00:03.3
DEBUG:forwarding.l2_learning:installing flow for 00:00:00:00:00:03.3 -> 00:00:00
:00:00:02.2
DEBUG:forwarding.l2_learning:installing flow for 00:00:00:00:00:03.3 -> 00:00:00
:00:00:01.1
```