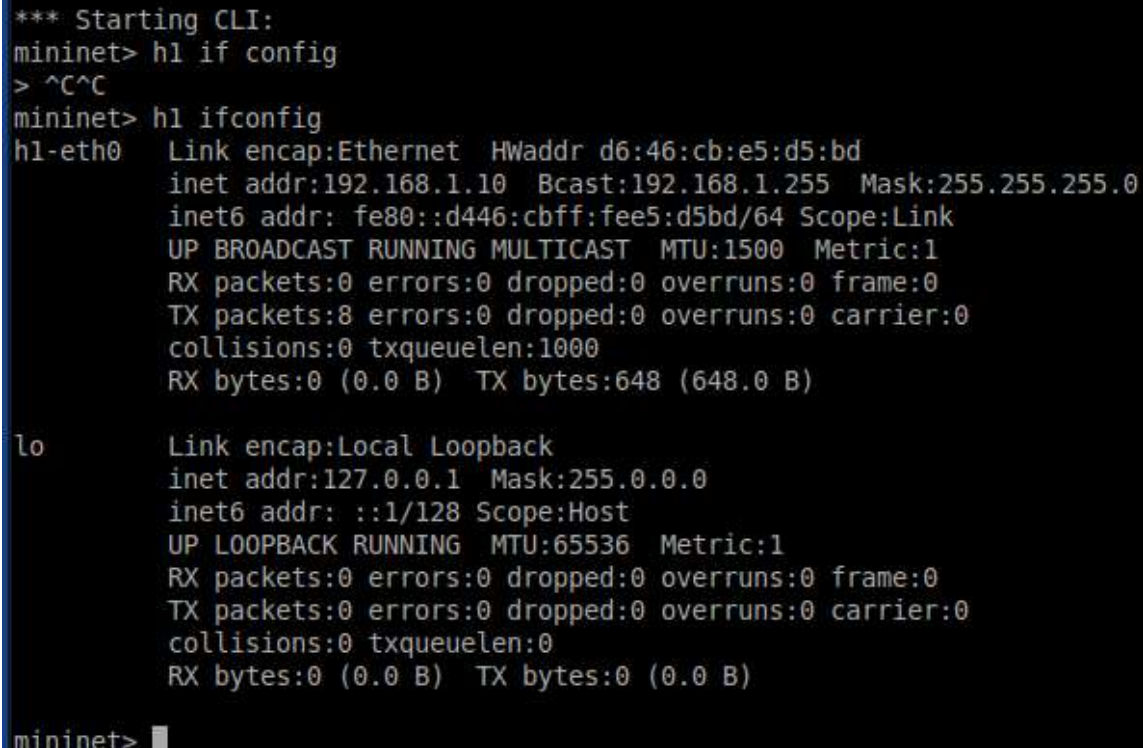


Name: Akshay A Nayak

Part 1: Setting up the network in Mininet

Deliverable 1:

Screenshot for the IP configuration of h2 (192.168.1.20). **(1 POINT)**

A screenshot of a terminal window showing the Mininet CLI. The user has entered the command 'h2 ifconfig' to configure the IP address of host h2. The output shows the configuration for the 'h2-eth0' interface, including the IP address 192.168.1.20, broadcast address 192.168.1.255, and mask 255.255.255.0. It also shows statistics for RX and TX packets and bytes.

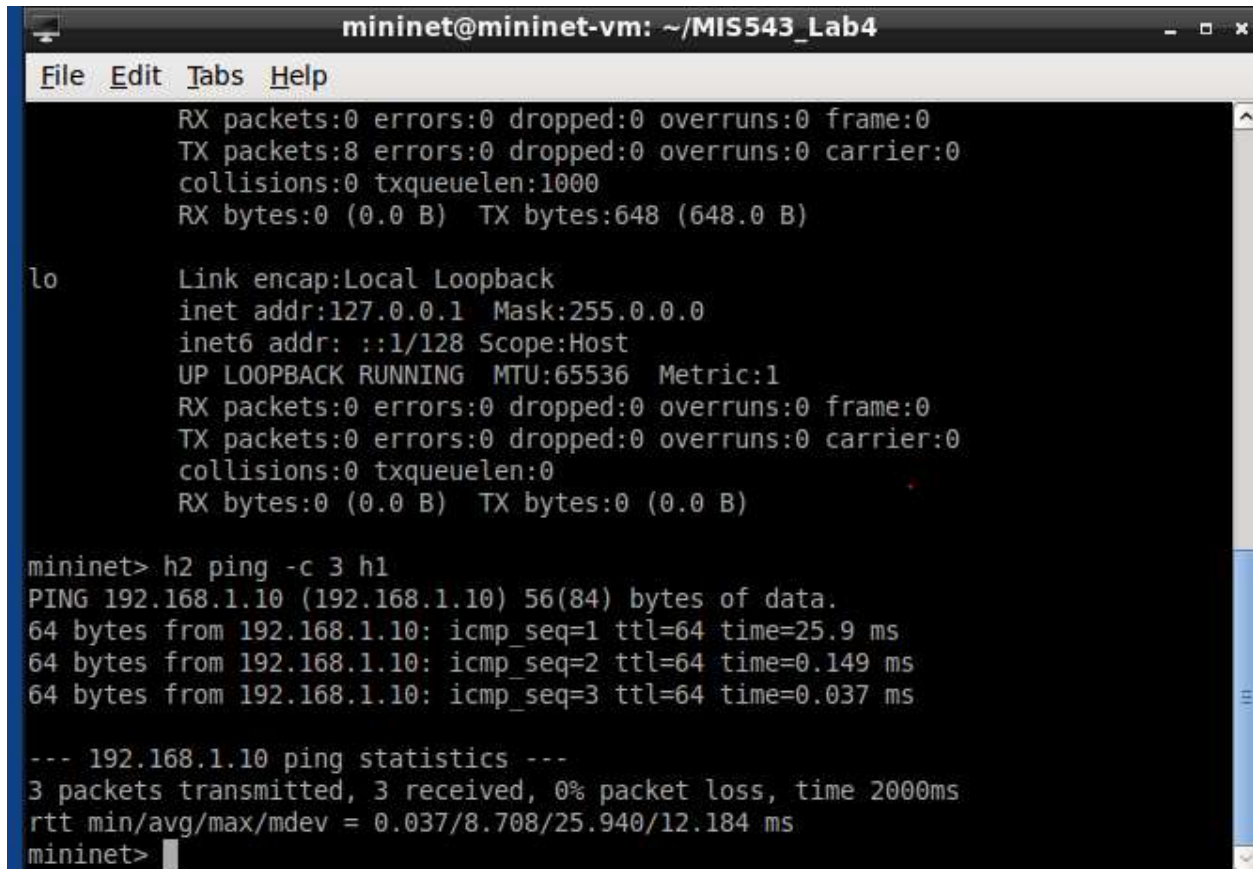
```
*** Starting CLI:
mininet> h2 if config
> ^C^C
mininet> h2 ifconfig
h2-eth0  Link encap:Ethernet  HWaddr d6:46:cb:e5:d5:bd
         inet addr:192.168.1.20  Bcast:192.168.1.255  Mask:255.255.255.0
         inet6 addr: fe80::d446:cbff:fee5:d5bd/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:0 errors:0 dropped:0 overruns:0 frame:0
         TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:0 (0.0 B)  TX bytes:648 (648.0 B)

lo       Link encap:Local Loopback
         inet addr:127.0.0.1  Mask:255.0.0.0
         inet6 addr: ::1/128 Scope:Host
         UP LOOPBACK RUNNING  MTU:65536  Metric:1
         RX packets:0 errors:0 dropped:0 overruns:0 frame:0
         TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

mininet>
```

Deliverable 2:

Screenshot for successful ping from h2 (192.168.1.20) to h1 (192.168.1.10) for three times. **(1 POINT)**



```
mininet@mininet-vm: ~/MIS543_Lab4
File Edit Tabs Help
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:648 (648.0 B)

lo
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

mininet> h2 ping -c 3 h1
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.
64 bytes from 192.168.1.10: icmp_seq=1 ttl=64 time=25.9 ms
64 bytes from 192.168.1.10: icmp_seq=2 ttl=64 time=0.149 ms
64 bytes from 192.168.1.10: icmp_seq=3 ttl=64 time=0.037 ms

--- 192.168.1.10 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.037/8.708/25.940/12.184 ms
mininet>
```

Deliverable 3:

Screenshot for successful ping from h3 (192.168.1.30) to server (10.0.0.5) for three times. **(1 POINT)**

```

mininet@mininet-vm: ~/MIS543_Lab4
File Edit Tabs Help
h1 h2 h3 server
**** Starting 1 controllers
c0
**** Starting 1 switches
s1
No NetFlow targets specified.
No sFlow targets specified.

NOTE: PLEASE REMEMBER TO EXIT THE CLI BEFORE YOU PRESS THE STOP BUTTON. Not exiting will prevent MiniEdit from quitting and will prevent you from starting the network again during this session.

*** Starting CLI:
mininet> h3 ping -c 3 server
PING 10.0.0.5 (10.0.0.5) 56(84) bytes of data.
64 bytes from 10.0.0.5: icmp_seq=1 ttl=64 time=109 ms
64 bytes from 10.0.0.5: icmp_seq=2 ttl=64 time=31.0 ms
64 bytes from 10.0.0.5: icmp_seq=3 ttl=64 time=0.178 ms

--- 10.0.0.5 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.178/46.752/109.007/45.792 ms
mininet>

```

Part 2: Blocking traffic for one host or traffic into a subnet

Deliverable 1:

- 1) Explain the steps that you had taken to place a firewall. **(1 POINT)**

```

aksahy2.py x lab4_pox_firewall.py x firewall-policies.csv
1 id,ip_src,ip_dst
2 1,192.168.1.10,192.168.1.20
3

```

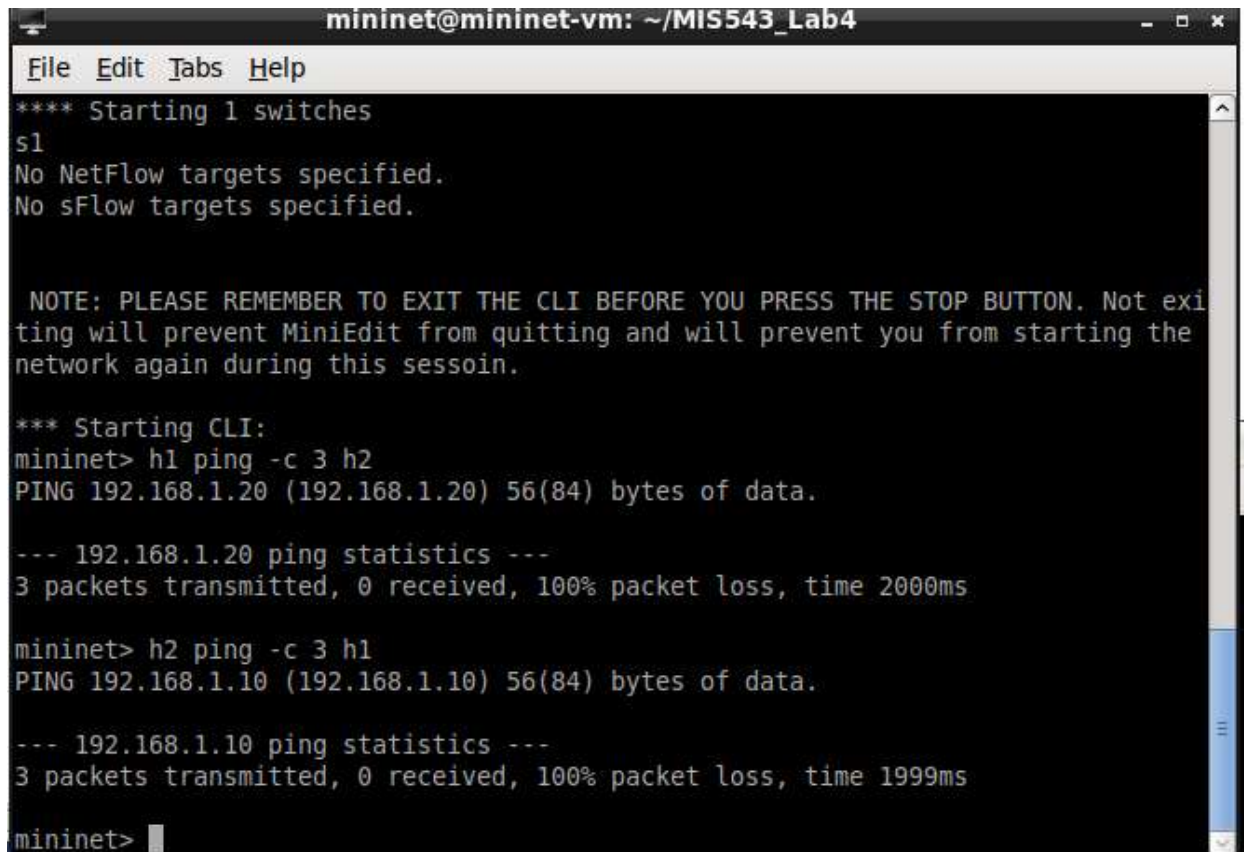
To place a firewall the src and dst ip was written in firewall-policies.csv to block the packet from travelling .

Deliverable 2:

- 2) Ping h1 to h2 and from h2 to h1 for three times. Provide a screenshot that verifies that you have successfully added a firewall to the network. Why a host can or cannot ping the other host? What can you say about the result? **(3 POINTS)**

```
*** Starting CLI:
mininet> h1 ping -c 3 h2
PING 192.168.1.20 (192.168.1.20) 56(84) bytes of data.

--- 192.168.1.20 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2000ms
```



```
mininet@mininet-vm: ~/MIS543_Lab4
File Edit Tabs Help
**** Starting 1 switches
s1
No NetFlow targets specified.
No sFlow targets specified.

NOTE: PLEASE REMEMBER TO EXIT THE CLI BEFORE YOU PRESS THE STOP BUTTON. Not exiting will prevent MiniEdit from quitting and will prevent you from starting the network again during this session.

*** Starting CLI:
mininet> h1 ping -c 3 h2
PING 192.168.1.20 (192.168.1.20) 56(84) bytes of data.

--- 192.168.1.20 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2000ms

mininet> h2 ping -c 3 h1
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.

--- 192.168.1.10 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 1999ms

mininet> 
```

The host cannot ping as I have blocked the data packet from travelling from source to destination ip address

Deliverable 3:

- 3) Ping h2 to h3 and server. Provide a screenshot that verifies that you have successfully tested the connectivity of the network. Is the host able to ping other devices in the network? Explain why the host can/cannot ping the devices on the network. **(3 POINTS)**

```
mininet@mininet-vm: ~/MIS543_Lab4
File Edit Tabs Help
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.

--- 192.168.1.10 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 1999ms

mininet> h2 ping -c 3 h3
PING 192.168.1.30 (192.168.1.30) 56(84) bytes of data.
64 bytes from 192.168.1.30: icmp_seq=1 ttl=64 time=8.20 ms
64 bytes from 192.168.1.30: icmp_seq=2 ttl=64 time=0.215 ms
64 bytes from 192.168.1.30: icmp_seq=3 ttl=64 time=0.057 ms

--- 192.168.1.30 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 0.057/2.827/8.209/3.806 ms
mininet> h2 ping -c 3 server
PING 10.0.0.5 (10.0.0.5) 56(84) bytes of data.
64 bytes from 10.0.0.5: icmp_seq=1 ttl=64 time=91.0 ms
64 bytes from 10.0.0.5: icmp_seq=2 ttl=64 time=12.9 ms
64 bytes from 10.0.0.5: icmp_seq=3 ttl=64 time=0.129 ms

--- 10.0.0.5 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.129/34.686/91.019/40.173 ms
mininet>
```

```
mininet> pingall
*** Ping: testing ping reachability
h1 -> h2 h3 server
h2 -> h1 h3 server
h3 -> h1 h2 X
server -> h1 h2 X
*** Results: 16% dropped (10/12 received)
mininet>
```

The firewall or ACL is done for h3 and server so no packet transfer takes place between h3 and server while packet travels in the network to other hosts.

Part 3: Monitoring network traffic using Wireshark

Deliverable

Ping h2 for three times in xterm of h1 and monitor the ICMP traffic in Wireshark. Provide a screenshot of your Wireshark capture. Explain what you see in Wireshark, and why. **(2 POINTS)**

MIS 543 – Business Data Communications & Networking

Assignment 4: Understanding Firewalls using Mininet

1	0.000000000	192.168.1.10	192.168.1.20	ICMP	98 Echo (ping) request id=0x07f3, seq=1/256, ttl=64
2	0.999485000	192.168.1.10	192.168.1.20	ICMP	98 Echo (ping) request id=0x07f3, seq=2/512, ttl=64
3	1.999184000	192.168.1.10	192.168.1.20	ICMP	98 Echo (ping) request id=0x07f3, seq=3/768, ttl=64
4	5.007199000	76:ed:a8:0b:fd:f9	c2:a5:e9:ae:78:e0	ARP	42 Who has 192.168.1.20? Tell 192.168.1.10
5	5.055205000	c2:a5:e9:ae:78:e0	76:ed:a8:0b:fd:f9	ARP	42 192.168.1.20 is at c2:a5:e9:ae:78:e0

There is no reply from the h2.

Deliverable 2:

Ping server from h3 for three times. Monitor the ICMP traffic in Wireshark on h3. Provide a screenshot of your Wireshark capture. Explain what you see in Wireshark. Is it the same as in Deliverable 1? Why? **(2 POINTS)**

1	0.000000000	82:c1:a9:ff:ac:68	Broadcast	ARP	42 Who has 192.168.1.1? Tell 192.168.1.30
2	0.013547000	00:00:00:00:00:01	82:c1:a9:ff:ac:68	ARP	42 192.168.1.1 is at 00:00:00:00:00:01
3	0.013555000	192.168.1.30	10.0.0.5	ICMP	98 Echo (ping) request id=0x083d, seq=1/256, ttl=64
4	0.016653000	10.0.0.5	192.168.1.30	ICMP	98 Echo (ping) reply id=0x083d, seq=1/256, ttl=64
5	1.001161000	192.168.1.30	10.0.0.5	ICMP	98 Echo (ping) request id=0x083d, seq=2/512, ttl=64
6	1.001295000	10.0.0.5	192.168.1.30	ICMP	98 Echo (ping) reply id=0x083d, seq=2/512, ttl=64
7	2.001467000	192.168.1.30	10.0.0.5	ICMP	98 Echo (ping) request id=0x083d, seq=3/768, ttl=64
8	2.001500000	10.0.0.5	192.168.1.30	ICMP	98 Echo (ping) reply id=0x083d, seq=3/768, ttl=64

There is a reply from server as there is no blocking of ip address from h3 and server.No it is not same as the device communicates back and forth.

Deliverable 3:

Ping server from h3 for three times. Monitor the ICMP traffic in Wireshark on h3. Provide a screenshot of your Wireshark capture. Explain what you see in Wireshark. Is it the same as in Deliverable 2? Why? **(2 POINTS)**

1	0.000000000	82:c1:a9:ff:ac:68	Broadcast	ARP	42 Who has 192.168.1.1? Tell 192.168.1.30
2	0.013547000	00:00:00:00:00:01	82:c1:a9:ff:ac:68	ARP	42 192.168.1.1 is at 00:00:00:00:00:01
3	0.013555000	192.168.1.30	10.0.0.5	ICMP	98 Echo (ping) request id=0x083d, seq=1/256, ttl=64
4	0.016653000	10.0.0.5	192.168.1.30	ICMP	98 Echo (ping) reply id=0x083d, seq=1/256, ttl=64
5	1.001161000	192.168.1.30	10.0.0.5	ICMP	98 Echo (ping) request id=0x083d, seq=2/512, ttl=64
6	1.001295000	10.0.0.5	192.168.1.30	ICMP	98 Echo (ping) reply id=0x083d, seq=2/512, ttl=64
7	2.001467000	192.168.1.30	10.0.0.5	ICMP	98 Echo (ping) request id=0x083d, seq=3/768, ttl=64
8	2.001500000	10.0.0.5	192.168.1.30	ICMP	98 Echo (ping) reply id=0x083d, seq=3/768, ttl=64

Yes it is the same.

Deliverable 4:

Ping server from h3 for three times. Monitor the ICMP traffic in Wireshark on the server. Provide a screenshot of your Wireshark capture. Explain what you see in Wireshark. Is it the same as in Deliverable 3? Why? **(2 POINTS)**

MIS 543 – Business Data Communications & Networking

Assignment 4: Understanding Firewalls using Mininet

1	0.000000000	a2:f4:4d:1a:fb:dc	Broadcast	ARP	42 Who has 192.168.1.1? Tell 192.168.1.30
2	0.015572000	00:00:00:00:00:01	a2:f4:4d:1a:fb:dc	ARP	42 192.168.1.1 is at 00:00:00:00:00:01
3	0.015581000	192.168.1.30	10.0.0.5	ICMP	98 Echo (ping) request id=0x0976, seq=1/256, ttl=64
4	0.999926000	192.168.1.30	10.0.0.5	ICMP	98 Echo (ping) request id=0x0976, seq=2/512, ttl=64
5	1.999925000	192.168.1.30	10.0.0.5	ICMP	98 Echo (ping) request id=0x0976, seq=3/768, ttl=64

No It is nto same as we have blocked the ip address of server.

Deliverable 5:

- 1) What does the method *read_policies* do? **(1 POINT)**
Opens a file and describes the policies
- 2) What does the method *_handle_ConnectionUp* do (roughly)? **(1 POINT)**
Defines the priority and blocks and It blocks certain IP address from communicating with specified IP address.