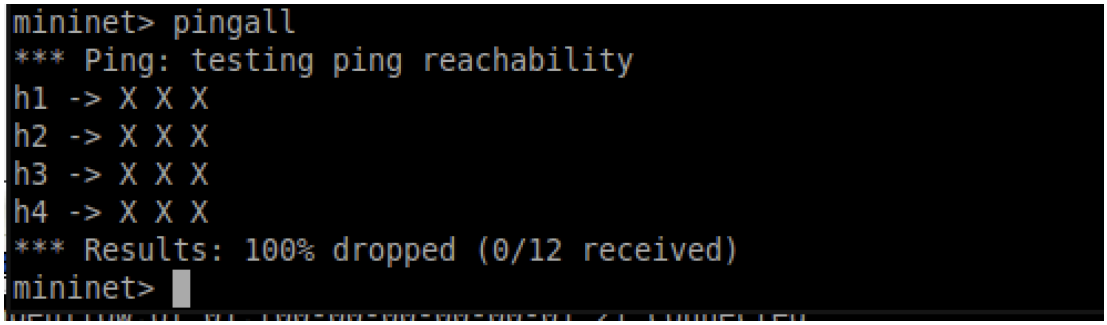
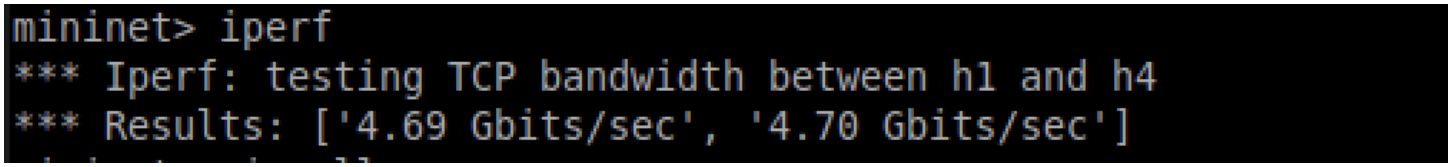
Lab 3

Pingall: As expected, pingall should fail because the firewall will block all ICMP traffic and it will drop it. The firewall will allow TCP and ARP traffic and it will be flooded. The ping command relies on ICMP Echo Request and Echo Reply messages to determine if a host is reachable. Since ICMP is neither TCP nor ARP, it falls under the rule that drops all other types of traffic. In my output it shows that all the packets are dropping packets or that none were received by each other.



Iperf: Iperf allows users to test the maximum TCP and UDP bandwidth performance, which is useful for diagnosing network performance issues, testing network configurations, and ensuring network devices are operating correctly. In my output it shows that bandwidth between h1 and h4 in gigabits per second (Gbits/sec). The first value represents the bandwidth in one direction (from h1 to h4), and the second value represents the bandwidth in the reverse direction (from h4 to h1). Both values are very close, showing that the network connection between these two hosts is symmetric and capable of approximately 4.7 Gbps bandwidth in both directions.



dpctl dump-flows: After running pingall, and iperf, I ran ‘dpctl dump-flows’ and this is what my output was. In this screenshot, it shows the flow entries currently installed in the OpenFlow switch. Each flow entry represents a rule that dictates how packets should be handled. Each entry includes the duration the rule has been active, packet and byte counts, timeouts, and the source/destination MAC and IP addresses, ICMP type, ARP operation. The actions specify how packets matching the criteria are handled: ICMP packets are dropped to prevent ping attacks,

while ARP packets are flooded to ensure devices can discover each other on the network. This setup reflects a basic firewall that selectively permits ARP traffic while blocking certain ICMP traffic.

```
mininet> dpctl dump-flows
*** s1 ------------------------------------------------------------------------
NXST_FLOW reply (xid=0x4):
 cookie=0x0, duration=27.519s, table=0, n_packets=1, n_bytes=98, idle_timeout=30
, hard_timeout=60, idle_age=27, icmp,vlan_tci=0x0000,dl_src=00:00:00:00:00:04,dl
_dst=00:00:00:00:00:02,nw_src=10.0.1.40,nw_dst=10.0.1.20,nw_tos=0,icmp_type=8,ic
mp_code=0 actions=drop
 cookie=0x0, duration=17.463s, table=0, n_packets=1, n_bytes=98, idle_timeout=30
, hard_timeout=60, idle_age=17, icmp,vlan_tci=0x0000,dl_src=00:00:00:00:00:04,dl
_dst=00:00:00:00:00:03,nw_src=10.0.1.40,nw_dst=10.0.1.30,nw_tos=0,icmp_type=8,ic
mp_code=0 actions=drop
 cookie=0x0, duration=12.483s, table=0, n_packets=1, n_bytes=42, idle_timeout=30
, hard_timeout=60, idle_age=12, arp,vlan_tci=0x0000,dl_src=00:00:00:00:00:04,dl_
dst=00:00:00:00:00:03,arp_spa=10.0.1.40,arp_tpa=10.0.1.30,arp_op=1 actions=FLOOD
 cookie=0x0, duration=12.467s, table=0, n_packets=1, n_bytes=42, idle_timeout=30
, hard_timeout=60, idle_age=12, arp,vlan_tci=0x0000,dl_src=00:00:00:00:00:03,dl_
dst=00:00:00:00:00:04,arp_spa=10.0.1.30,arp_tpa=10.0.1.40,arp_op=2 actions=FLOOD
 cookie=0x0, duration=22.49s, table=0, n_packets=1, n_bytes=42, idle_timeout=30,
 hard_timeout=60, idle_age=22, arp,vlan_tci=0x0000,dl_src=00:00:00:00:00:02,dl_d
st=00:00:00:00:00:04,arp_spa=10.0.1.20,arp_tpa=10.0.1.40,arp_op=2 actions=FLOOD
 cookie=0x0, duration=22.51s, table=0, n_packets=1, n_bytes=42, idle_timeout=30,
 hard_timeout=60, idle_age=22, arp,vlan_tci=0x0000,dl_src=00:00:00:00:00:04,dl_d
st=00:00:00:00:00:02,arp_spa=10.0.1.40,arp_tpa=10.0.1.20,arp_op=1 actions=FLOOD
```

Resources:
https://pox-dev.noxrepo.narkive.com/yqy9JuDC/usage-ofp-flow-mod-and-ofp-packet-out-messages