

Kyle Zhang  
kmzhang  
[kmzhang@ucsc.edu](mailto:kmzhang@ucsc.edu)  
1669388  
Lab1  
April 19, 2020

2.

```
mininet> dump
<Host h1: h1-eth0:10.0.0.1 pid=5458>
<Host h2: h2-eth0:10.0.0.2 pid=5462>
<Host h3: h3-eth0:10.0.0.3 pid=5464>
<Host h4: h4-eth0:10.0.0.4 pid=5466>
<Host h5: h5-eth0:10.0.0.5 pid=5468>
<Host h6: h6-eth0:10.0.0.6 pid=5470>
<OVSSwitch s1: lo:127.0.0.1,s1-eth1:None,s1-eth2:None,s1-eth3:None pid=5475>
<OVSSwitch s2: lo:127.0.0.1,s2-eth1:None,s2-eth2:None,s2-eth3:None pid=5478>
<OVSSwitch s3: lo:127.0.0.1,s3-eth1:None,s3-eth2:None,s3-eth3:None,s3-eth4:None pid=5481>
<Controller c0: 127.0.0.1:6633 pid=5451>
mininet> pingall
*** Ping: testing ping reachability
h1 -> h2 h3 h4 h5 h6
h2 -> h1 h3 h4 h5 h6
h3 -> h1 h2 h4 h5 h6
h4 -> h1 h2 h3 h5 h6
h5 -> h1 h2 h3 h4 h6
h6 -> h1 h2 h3 h4 h5
*** Results: 0% dropped (30/30 received)
mininet> █
```

The dump command lists all the switches and hosts that are a part of the topology. This command shows the host and switch names, as well as their source IP addresses. It also shows the controller.

The pingall command does a ping for all the pairs. Because every host is connected to every other host for this topology, the pingall command has a total 30 pings, where each host pings the other 5 hosts once each. You can see which hosts are pinging the others on the left hand side of the arrows, and the hosts that were pinged on the right hand side of arrows.

3.

```
mininet> iperf
*** Iperf: testing TCP bandwidth between h1 and h6
*** Results: ['44.1 Gbits/sec', '44.1 Gbits/sec']
mininet> █
```

The connect speed is 44.1 Gbits/sec.

4.

a.

No.	Time	Source	Destination	Protocol	Length	Info
29	10.633003000	10.0.0.1	10.0.0.2	OF 1.0	184	of_packet_in
36	10.633356000	10.0.0.1	10.0.0.2	OF 1.0	184	of_packet_in
44	10.633593000	10.0.0.1	10.0.0.2	OF 1.0	184	of_packet_in
51	10.633832000	10.0.0.2	10.0.0.1	OF 1.0	184	of_packet_in
55	10.634089000	10.0.0.2	10.0.0.1	OF 1.0	184	of_packet_in
59	10.634462000	10.0.0.2	10.0.0.1	OF 1.0	184	of_packet_in
66	11.634393000	10.0.0.1	10.0.0.2	OF 1.0	184	of_packet_in
71	11.634645000	10.0.0.1	10.0.0.2	OF 1.0	184	of_packet_in
76	11.634938000	10.0.0.1	10.0.0.2	OF 1.0	184	of_packet_in
123	15.640263000	52:68:5b:e5:0b:0e	e2:be:59:18:93:9e	OF 1.0	128	of_packet_in
128	15.640660000	52:68:5b:e5:0b:0e	e2:be:59:18:93:9e	OF 1.0	128	of_packet_in
133	15.640989000	52:68:5b:e5:0b:0e	e2:be:59:18:93:9e	OF 1.0	128	of_packet_in
138	15.641253000	e2:be:59:18:93:9e	52:68:5b:e5:0b:0e	OF 1.0	128	of_packet_in
142	15.641509000	e2:be:59:18:93:9e	52:68:5b:e5:0b:0e	OF 1.0	128	of_packet_in
146	15.641748000	e2:be:59:18:93:9e	52:68:5b:e5:0b:0e	OF 1.0	128	of_packet_in

There are 15 of\_packet\_in messages, and the sources IP addresses are “10.0.0.1”, “10.0.0.2”, “52:68:5b:e5:0b:0e”, and “e2:be:59:18:93:9e”. Source IP addresses “10.0.0.1” and “10.0.0.2” correspond to the two hosts that were used in the ping command. The destination IP addresses are “10.0.0.1”, “10.0.0.2”, “52:68:5b:e5:0b:0e”, and “e2:be:59:18:93:9e” as well, and “10.0.0.1”, “10.0.0.2” are again present since the two hosts are communicating with each other.

b.

No.	Time	Source	Destination	Protocol	Length	Info
30	10.633225000	127.0.0.1	127.0.0.1	OF 1.0	92	of_packet_out
37	10.633472000	127.0.0.1	127.0.0.1	OF 1.0	92	of_packet_out
45	10.633706000	127.0.0.1	127.0.0.1	OF 1.0	92	of_packet_out

The source IP address is “127.0.0.1” and the destination IP address is also “127.0.0.1”. This is the IP address of the controller.

C.

Filter: icmp && not of							Expression...	Clear	Apply	Save
No.	Time	Source	Destination	Protocol	Length	Info				
908	6.191064000	10.0.0.3	10.0.0.6	ICMP	100	Echo (ping) reply id=0x0b42, seq=1/256, ttl=64				
909	6.191065000	10.0.0.3	10.0.0.6	ICMP	100	Echo (ping) reply id=0x0b42, seq=1/256, ttl=64				
912	6.191428000	10.0.0.3	10.0.0.6	ICMP	100	Echo (ping) reply id=0x0b42, seq=1/256, ttl=64				
913	6.194526000	10.0.0.6	10.0.0.4	ICMP	100	Echo (ping) request id=0x0b43, seq=1/256, ttl=64				
916	6.194965000	10.0.0.6	10.0.0.4	ICMP	100	Echo (ping) request id=0x0b43, seq=1/256, ttl=64				
917	6.194966000	10.0.0.6	10.0.0.4	ICMP	100	Echo (ping) request id=0x0b43, seq=1/256, ttl=64				
920	6.195484000	10.0.0.6	10.0.0.4	ICMP	100	Echo (ping) request id=0x0b43, seq=1/256, ttl=64				
921	6.195493000	10.0.0.4	10.0.0.6	ICMP	100	Echo (ping) reply id=0x0b43, seq=1/256, ttl=64 (request in 920)				
924	6.196577000	10.0.0.4	10.0.0.6	ICMP	100	Echo (ping) reply id=0x0b43, seq=1/256, ttl=64				
925	6.196578000	10.0.0.4	10.0.0.6	ICMP	100	Echo (ping) reply id=0x0b43, seq=1/256, ttl=64				
928	6.197042000	10.0.0.4	10.0.0.6	ICMP	100	Echo (ping) reply id=0x0b43, seq=1/256, ttl=64				
929	6.198181000	10.0.0.6	10.0.0.5	ICMP	100	Echo (ping) request id=0x0b44, seq=1/256, ttl=64				
932	6.198492000	10.0.0.6	10.0.0.5	ICMP	100	Echo (ping) request id=0x0b44, seq=1/256, ttl=64 (reply in 933)				
933	6.198513000	10.0.0.5	10.0.0.6	ICMP	100	Echo (ping) reply id=0x0b44, seq=1/256, ttl=64 (request in 932)				
936	6.198871000	10.0.0.5	10.0.0.6	ICMP	100	Echo (ping) reply id=0x0b44, seq=1/256, ttl=64				
Frame 936: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface 0										
Linux cooked capture										
Packet type: Sent by us (4)										
Link-layer address type: 1										
Link-layer address length: 6										
Source: da:c7:e8:b7:f8:42 (da:c7:e8:b7:f8:42)										
Protocol: IP (0x0800)										
Internet Protocol Version 4, Src: 10.0.0.5 (10.0.0.5), Dst: 10.0.0.6 (10.0.0.6)										
Version: 4										
Header length: 20 bytes										
Differentiated Services Field: 0x00 (DSCP: 0x00, Default; ECN: 0x00, Not-ECT (Not ECT-Capable Transport))										
0000	00 04 00 01 00 06	da c7 e8 b7 f8 42	00 00 08 00	.....	...B....					
0010	45 00 00 54 89 f1	00 00 40 01 dc ad	0a 00 00 05	E..T....	@.....					
0020	0a 00 00 06 00 00	55 6e 0b 44 00 01	66 cd 9c 5e	.....Un	.D..f..^					
0030	aa 1d 07 00 08 09	0a 0b 0c 0d 0e 0f	10 11 12 13	.....	.....					
Source link-layer address (sll.s...)										
Packets: 3533 · Displayed: 248 (7.0%)										

There are 248 “icmp && not of” entries. Some of these entries are echo requests and echo replies.