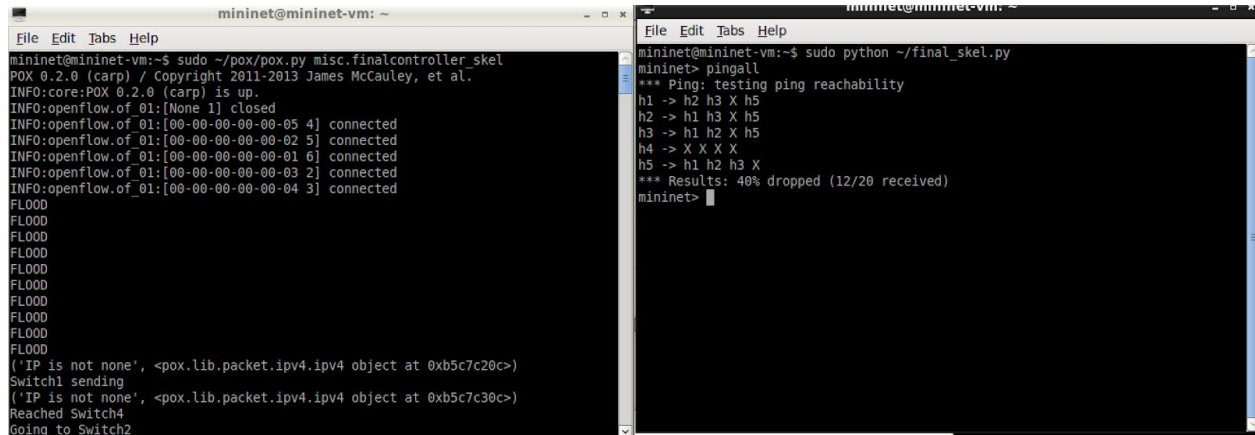


Presentation:

Listening on the “any” interface on wireshark, I were able to capture all the packets that were being sent to the different hosts. To do that, I used the command “pingall” which involves transfers/pings between all host pairs. Because pings involve ICMP packets, the ones from host 4 (or the “hacker”) are dropped to any other host and pings fail because this host is an untrusted host. Also in wireshark, is shown where there is a request but no reply as well as the print statement coded in the controller.



```

mininet@mininet-vm: ~
File Edit Tabs Help
mininet@mininet-vm:~$ sudo ~/pox/pox.py misc.finalcontroller skel
POX 0.2.0 (carp) / Copyright 2011-2013 James McCauley, et al.
INFO:core:POX 0.2.0 (carp) is up.
INFO:openflow.of_01:[None 1] closed
INFO:openflow.of_01:[00:00:00:00:00:05 4] connected
INFO:openflow.of_01:[00:00:00:00:00:02 5] connected
INFO:openflow.of_01:[00:00:00:00:00:01 6] connected
INFO:openflow.of_01:[00:00:00:00:00:03 2] connected
INFO:openflow.of_01:[00:00:00:00:00:04 3] connected
FLOOD
FLOOD
FLOOD
FLOOD
FLOOD
FLOOD
FLOOD
FLOOD
FLOOD
FLOOD
FLOOD
FLOOD
FLOOD
FLOOD
FLOOD
FLOOD
('IP is not none', <pox.lib.packet.ipv4.ipv4 object at 0xb5c7c20c>)
Switch1 sending
('IP is not none', <pox.lib.packet.ipv4.ipv4 object at 0xb5c7c30c>)
Reached Switch4
going to Switch2

mininet@mininet-vm:~$ sudo python ~/final_skel.py
mininet> pingall
*** Ping: testing ping reachability
h1 -> h2 h3 X h5
h2 -> h1 h3 X h5
h3 -> h1 h2 X h5
h4 -> X X X X
h5 -> h1 h2 h3 X
*** Results: 40% dropped (12/20 received)
mininet>

```

Capturing from any [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
178	10.62420000	00:00:00:00:00:03	00:00:00:00:00:01	OF 1.0	128	of_packet_in
179	10.62591000	127.0.0.1	127.0.0.1	OF 1.0	148	of_flow_add
180	10.62599000	00:00:00:00:00:03		ARP	44	10.3.3.30 is at 00:00:00:00:00:03
181	10.62599200	00:00:00:00:00:03		ARP	44	10.3.3.30 is at 00:00:00:00:00:03
182	10.62599400	00:00:00:00:00:03		ARP	44	10.3.3.30 is at 00:00:00:00:00:03
183	10.62599600	00:00:00:00:00:03		ARP	44	10.3.3.30 is at 00:00:00:00:00:03
184	10.62599800	00:00:00:00:00:03		ARP	44	10.3.3.30 is at 00:00:00:00:00:03
185	10.62599300	00:00:00:00:00:03		ARP	44	10.3.3.30 is at 00:00:00:00:00:03
186	10.62599700	00:00:00:00:00:03		ARP	44	10.3.3.30 is at 00:00:00:00:00:03
187	10.62599800	00:00:00:00:00:03		ARP	44	10.3.3.30 is at 00:00:00:00:00:03
188	10.62605700	00:00:00:00:00:03	00:00:00:00:00:01	OF 1.0	128	of_packet_in
189	10.62607900	00:00:00:00:00:03	00:00:00:00:00:01	OF 1.0	128	of_packet_in
190	10.62608700	00:00:00:00:00:03	00:00:00:00:00:01	OF 1.0	128	of_packet_in
191	10.62773500	127.0.0.1	127.0.0.1	OF 1.0	148	of_flow_add
192	10.62780500	00:00:00:00:00:03		ARP	44	10.3.3.30 is at 00:00:00:00:00:03
193	10.62780700	00:00:00:00:00:03		ARP	44	10.3.3.30 is at 00:00:00:00:00:03
194	10.62813700	127.0.0.1	127.0.0.1	OF 1.0	148	of_flow_add
195	10.62828700	00:00:00:00:00:03		ARP	44	10.3.3.30 is at 00:00:00:00:00:03
196	10.62829900	00:00:00:00:00:03		ARP	44	10.3.3.30 is at 00:00:00:00:00:03
197	10.62862900	127.0.0.1	127.0.0.1	OF 1.0	148	of_flow_add
198	10.62868800	00:00:00:00:00:03		ARP	44	10.3.3.30 is at 00:00:00:00:00:03
199	10.62869000	00:00:00:00:00:03		ARP	44	10.3.3.30 is at 00:00:00:00:00:03
200	10.62869500	10.1.1.10	10.3.3.30	ICMP	100	Echo (ping) request id=0x08cb, seq=1/256, ttl=64
201	10.62874400	10.1.1.10	10.3.3.30	OF 1.0	184	of_packet_in

any: <live capture in progress... Profile: Default

Using the command “h1 ping h3” I was able to get a successful ping between two trusted hosts (h1 and h3), which involve requests and replies. Which can be seen below in the pictures

```
mininet> h1 ping h3
PING 10.3.3.30 (10.3.3.30) 56(84) bytes of data.
64 bytes from 10.3.3.30: icmp_seq=1 ttl=64 time=0.213 ms
64 bytes from 10.3.3.30: icmp_seq=2 ttl=64 time=0.039 ms
64 bytes from 10.3.3.30: icmp_seq=3 ttl=64 time=0.040 ms
64 bytes from 10.3.3.30: icmp_seq=4 ttl=64 time=0.041 ms
^C
--- 10.3.3.30 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2998ms
rtt min/avg/max/mdev = 0.039/0.083/0.213/0.075 ms
```

Wireshark 1.10.6 (v1.10.6 from master-1.10) interface showing a packet capture. The filter is empty. The packet list shows 83 packets. Packets 61-68 are ICMP Echo (ping) requests and replies between 10.1.1.10 and 10.3.3.30. Packets 69-83 are TCP and OF 1.0 packets between 127.0.0.1 and 127.0.0.1.

No.	Time	Source	Destination	Protocol	Length	Info
61	3.315328000	10.1.1.10	10.3.3.30	ICMP	100	Echo (ping) request id=0x09d2, seq=4/1024, ttl=64
62	3.315329000	10.1.1.10	10.3.3.30	ICMP	100	Echo (ping) request id=0x09d2, seq=4/1024, ttl=64
63	3.315337000	10.3.3.30	10.1.1.10	ICMP	100	Echo (ping) reply id=0x09d2, seq=4/1024, ttl=64
64	3.315338000	10.3.3.30	10.1.1.10	ICMP	100	Echo (ping) reply id=0x09d2, seq=4/1024, ttl=64
65	3.315339000	10.3.3.30	10.1.1.10	ICMP	100	Echo (ping) reply id=0x09d2, seq=4/1024, ttl=64
66	3.315340000	10.3.3.30	10.1.1.10	ICMP	100	Echo (ping) reply id=0x09d2, seq=4/1024, ttl=64
67	3.315340000	10.3.3.30	10.1.1.10	ICMP	100	Echo (ping) reply id=0x09d2, seq=4/1024, ttl=64
68	3.315341000	10.3.3.30	10.1.1.10	ICMP	100	Echo (ping) reply id=0x09d2, seq=4/1024, ttl=64
69	5.000034000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_request
70	5.000054000	127.0.0.1	127.0.0.1	TCP	68	6633 > 56871 [ACK] Seq=9 Ack=17 Win=88 Len=0 TSval=
71	5.000077000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_request
72	5.000080000	127.0.0.1	127.0.0.1	TCP	68	6633 > 56872 [ACK] Seq=9 Ack=17 Win=88 Len=0 TSval=
73	5.000087000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_request
74	5.000089000	127.0.0.1	127.0.0.1	TCP	68	6633 > 56873 [ACK] Seq=9 Ack=17 Win=86 Len=0 TSval=
75	5.000095000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_request
76	5.000097000	127.0.0.1	127.0.0.1	TCP	68	6633 > 56874 [ACK] Seq=9 Ack=17 Win=86 Len=0 TSval=
77	5.000107000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_request
78	5.000109000	127.0.0.1	127.0.0.1	TCP	68	6633 > 56875 [ACK] Seq=9 Ack=17 Win=86 Len=0 TSval=
79	5.014452000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_reply
80	5.014466000	127.0.0.1	127.0.0.1	TCP	68	56871 > 6633 [ACK] Seq=17 Ack=17 Win=86 Len=0 TSv=
81	5.014611000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_reply
82	5.014616000	127.0.0.1	127.0.0.1	TCP	68	56874 > 6633 [ACK] Seq=17 Ack=17 Win=86 Len=0 TSv=
83	5.014702000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_reply

The pictures below show ping involving the untrusted host h4 (the hacker), in which there are ICMP echo requests but no replies because the packets are identified as a threat and therefore dropped at switch 4.

mininet@mininet-vm: ~

```
mininet@mininet-vm:~$ sudo python ~/final_skel.py
mininet> h4 ping h1
PING 10.1.1.10 (10.1.1.10) 56(84) bytes of data.
^C
--- 10.1.1.10 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3023ms

mininet> h4 ping h1
PING 10.1.1.10 (10.1.1.10) 56(84) bytes of data.
^C
--- 10.1.1.10 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4031ms

mininet>
```

No.	Time	Source	Destination	Protocol	Length	Info
160	6.609408000	00:00:00:00:00:01		ARP	44	10.1.1.10 is at 00:00:00:00:00:01
161	6.609409000	00:00:00:00:00:01		ARP	44	10.1.1.10 is at 00:00:00:00:00:01
162	6.609785000	127.0.0.1	127.0.0.1	OF 1.0	148	of_flow_add
163	6.609793000	127.0.0.1	127.0.0.1	TCP	68	56942 > 6633 [ACK] Seq=77 Ack=97 Win=86 Len=0 TSv
164	6.609821000	00:00:00:00:00:04		ARP	44	Who has 10.1.1.10? Tell 123.45.67.89
165	6.609823000	00:00:00:00:00:04		ARP	44	Who has 10.1.1.10? Tell 123.45.67.89
166	6.610539000	127.0.0.1	127.0.0.1	OF 1.0	148	of_flow_add
167	6.610550000	127.0.0.1	127.0.0.1	TCP	68	56945 > 6633 [ACK] Seq=77 Ack=97 Win=86 Len=0 TSv
168	6.610639000	00:00:00:00:00:04		ARP	44	Who has 10.1.1.10? Tell 123.45.67.89
169	6.610641000	00:00:00:00:00:04		ARP	44	Who has 10.1.1.10? Tell 123.45.67.89
170	11.001886000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_request
171	11.001933000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_request
172	11.001946000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_request
173	11.001957000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_request
174	11.001972000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_request
175	11.121254000	127.0.0.1	127.0.0.1	TCP	68	6633 > 56942 [ACK] Seq=97 Ack=85 Win=88 Len=0 TSv
176	11.121256000	127.0.0.1	127.0.0.1	TCP	68	6633 > 56943 [ACK] Seq=97 Ack=665 Win=88 Len=0 TSv
177	11.121257000	127.0.0.1	127.0.0.1	TCP	68	6633 > 56944 [ACK] Seq=97 Ack=85 Win=88 Len=0 TSv
178	11.121258000	127.0.0.1	127.0.0.1	TCP	68	6633 > 56945 [ACK] Seq=97 Ack=85 Win=88 Len=0 TSv
179	11.121259000	127.0.0.1	127.0.0.1	TCP	68	6633 > 56946 [ACK] Seq=97 Ack=85 Win=88 Len=0 TSv
180	11.121421000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_reply
181	11.121427000	127.0.0.1	127.0.0.1	TCP	68	56943 > 6633 [ACK] Seq=665 Ack=105 Win=86 Len=0 TSv
182	11.121784000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_reply

The below picture shows a similar situation with ping between an untrusted host (hacker) and the server h5. Here, ICMP echo requests are identified and dropped. Some of these print statements occur and alternate after the “IP is not None”, which means that IP packets are dropped and won't reach the server h5.

```

mininet@mininet-vm: ~
File Edit Tabs Help
FLOOD
FLOOD
('IP is not none', <pox.lib.packet.ipv4.ipv4 object at 0xb5c4194c>)
Reached Switch4
Hacker IP to h5, DROP
FLOOD
FLOOD
FLOOD
('IP is not none', <pox.lib.packet.ipv4.ipv4 object at 0xb5cb3fcc>)
Reached Switch4
Hacker IP to h5, DROP
('IP is not none', <pox.lib.packet.ipv4.ipv4 object at 0xb5cb3eec>)
Reached Switch4
Hacker IP to h5, DROP
('IP is not none', <pox.lib.packet.ipv4.ipv4 object at 0xb5cb37ac>)
Reached Switch4
Hacker IP to h5, DROP
('IP is not none', <pox.lib.packet.ipv4.ipv4 object at 0xb5cb362c>)
Reached Switch4
Hacker IP to h5, DROP
('IP is not none', <pox.lib.packet.ipv4.ipv4 object at 0xb5cb3b0c>)
Reached Switch4
Hacker IP to h5, DROP

```

```

mininet> h4 ping h5
PING 10.5.5.50 (10.5.5.50) 56(84) bytes of data.
^C
--- 10.5.5.50 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5038ms

```


Capturing from any [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_request
2	0.000021000	127.0.0.1	127.0.0.1	TCP	68	6633 > 56942 [ACK] Seq=1 Ack=9 Win=88 Len=0 TSval=
3	0.000042000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_request
4	0.000045000	127.0.0.1	127.0.0.1	TCP	68	6633 > 56943 [ACK] Seq=1 Ack=9 Win=88 Len=0 TSval=
5	0.000052000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_request
6	0.000054000	127.0.0.1	127.0.0.1	TCP	68	6633 > 56944 [ACK] Seq=1 Ack=9 Win=88 Len=0 TSval=
7	0.000060000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_request
8	0.000063000	127.0.0.1	127.0.0.1	TCP	68	6633 > 56945 [ACK] Seq=1 Ack=9 Win=88 Len=0 TSval=
9	0.000069000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_request
10	0.000071000	127.0.0.1	127.0.0.1	TCP	68	6633 > 56946 [ACK] Seq=1 Ack=9 Win=88 Len=0 TSval=
11	0.007820000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_reply
12	0.007830000	127.0.0.1	127.0.0.1	TCP	68	56943 > 6633 [ACK] Seq=9 Ack=9 Win=86 Len=0 TSval=
13	0.007986000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_reply
14	0.007992000	127.0.0.1	127.0.0.1	TCP	68	56944 > 6633 [ACK] Seq=9 Ack=9 Win=86 Len=0 TSval=
15	0.008142000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_reply
16	0.008146000	127.0.0.1	127.0.0.1	TCP	68	56946 > 6633 [ACK] Seq=9 Ack=9 Win=86 Len=0 TSval=
17	0.008227000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_reply
18	0.008232000	127.0.0.1	127.0.0.1	TCP	68	56942 > 6633 [ACK] Seq=9 Ack=9 Win=86 Len=0 TSval=
19	0.008342000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_reply
20	0.008346000	127.0.0.1	127.0.0.1	TCP	68	56945 > 6633 [ACK] Seq=9 Ack=9 Win=86 Len=0 TSval=
21	5.000042000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_request
22	5.000080000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_request
23	5.000089000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_request
24	5.000096000	127.0.0.1	127.0.0.1	OF 1.0	76	of_echo_request

any: <live capture in progress... Profile: Default

Now I will test the hosts using the “iperf” command. The below picture shows successful transmissions between the trusted hosts h1, h2, h3, and h5, as well as the first two iperf commands, as well as the print statements that are generated when the packets are sent from one host and received by another. The third command does not automatically resolve and requires interruption because of the IP packets not being able to reach the server h5 from the untrusted host h4 after they are dropped by the controller.

```
(('IP is not none', <pox.lib.packet.ipv4.ipv4 object at 0xb5cb3e4c>)
Switch1 sending
('IP is not none', <pox.lib.packet.ipv4.ipv4 object at 0xb5cb366c>)
Reached Switch4
Going to Switch5
('IP is not none', <pox.lib.packet.ipv4.ipv4 object at 0xb5cb324c>)
Switch5 receiving
('IP is not none', <pox.lib.packet.ipv4.ipv4 object at 0xb5cb354c>)
Switch5 is sending
('IP is not none', <pox.lib.packet.ipv4.ipv4 object at 0xb5cb350c>)
Reached Switch4
Going to Switch1
('IP is not none', <pox.lib.packet.ipv4.ipv4 object at 0xb5cb390c>)
Switch1 receiving
('IP is not none', <pox.lib.packet.ipv4.ipv4 object at 0xb5cb3f2c>)
Switch1 sending
('IP is not none', <pox.lib.packet.ipv4.ipv4 object at 0xb5c416cc>)
Reached Switch4
Going to Switch5
('IP is not none', <pox.lib.packet.ipv4.ipv4 object at 0xb5c4112c>)
Switch5 receiving
('IP is not none', <pox.lib.packet.ipv4.ipv4 object at 0xb5c4186c>)
Reached Switch4
Hacker IP to h5, DROP
('IP is not none', <pox.lib.packet.ipv4.ipv4 object at 0xb5c4160c>)
Reached Switch4
Hacker IP to h5, DROP
('IP is not none', <pox.lib.packet.ipv4.ipv4 object at 0xb5c419ac>)
Reached Switch4
Hacker IP to h5, DROP
FLOOD
FLOOD
FLOOD
FLOOD
FLOOD
('IP is not none', <pox.lib.packet.ipv4.ipv4 object at 0xb5c40f6c>)
Reached Switch4
Hacker IP to h5, DROP
('IP is not none', <pox.lib.packet.ipv4.ipv4 object at 0xb5c40c8c>)
Reached Switch4
Hacker IP to h5, DROP
```

```
mininet> iperf h1 h3
*** Iperf: testing TCP bandwidth between h1 and h3
*** Results: ['25.9 Gbits/sec', '25.9 Gbits/sec']
mininet> iperf h5 h1
*** Iperf: testing TCP bandwidth between h5 and h1
*** Results: ['26.1 Gbits/sec', '26.1 Gbits/sec']
mininet> iperf h4 h5
*** Iperf: testing TCP bandwidth between h4 and h5
^C
Interrupt
mininet> iperf h1 h2
*** Iperf: testing TCP bandwidth between h1 and h2
*** Results: ['30.9 Gbits/sec', '30.9 Gbits/sec']
```

Finally, using the command “dpctl dump-flows” i was able to get entries for each switch that I created using the “of_flow_mod.” I played around with the timeout settings and found out that if I didn't include a specific time, I would still receive entries.

```
*** s1 ***
NXST_FLOW reply (xid=0x4):
  cookie=0x0, duration=415.347s, table=0, n packets=147440, n bytes=9731048, idle age=410, tcp,vlan tci=0x0000,d1 src=00:00:00:00:00:02,d1 dst=00:00:00:00:00:01,nw src=10.2.2.20,nw_dst=10.1.1.10,nw_tos=0,tp_src=5001,tp_dst=51882 actions=output:8
  cookie=0x0, duration=649.429s, table=0, n packets=140321, n bytes=9270098, idle age=644, tcp,vlan tci=0x0000,d1 src=00:00:00:00:00:01,d1 dst=00:00:00:00:00:05,nw src=10.1.1.10,nw_dst=10.5.5.50,nw_tos=0,tp_src=5001,tp_dst=57611 actions=output:1
  cookie=0x0, duration=1735.384s, table=0, n packets=9, n bytes=882, idle age=1680, icmp,vlan tci=0x0000,d1 src=00:00:00:00:00:01,d1 dst=00:00:00:00:00:04,nw src=10.1.1.10,nw_dst=123.45.67.89,nw_tos=0,icmp type=0,icmp code=0 actions=output:1
  cookie=0x0, duration=706.714s, table=0, n packets=4, n bytes=272, idle age=706, tcp,vlan tci=0x0000,d1 src=00:00:00:00:00:01,d1 dst=00:00:00:00:00:03,nw src=10.1.1.10,nw_dst=10.3.3.30,nw_tos=16,tp_src=42723,tp_dst=5001 actions=output:1
  cookie=0x0, duration=706.708s, table=0, n packets=2, n bytes=140, idle age=706, tcp,vlan tci=0x0000,d1 src=00:00:00:00:00:03,d1 dst=00:00:00:00:00:01,nw src=10.3.3.30,nw_dst=10.1.1.10,nw_tos=0,tp_src=5001,tp_dst=42723 actions=output:8
  cookie=0x0, duration=415.405s, table=0, n packets=3, n bytes=206, idle age=415, tcp,vlan tci=0x0000,d1 src=00:00:00:00:00:02,d1 dst=00:00:00:00:00:01,nw src=10.2.2.20,nw_dst=10.1.1.10,nw_tos=0,tp_src=5001,tp_dst=51881 actions=output:8
  cookie=0x0, duration=649.445s, table=0, n packets=4, n bytes=272, idle age=649, tcp,vlan tci=0x0000,d1 src=00:00:00:00:00:05,d1 dst=00:00:00:00:00:01,nw src=10.5.5.50,nw_dst=10.1.1.10,nw_tos=16,tp_src=57610,tp_dst=5001 actions=output:8
  cookie=0x0, duration=415.397s, table=0, n packets=513366, n bytes=19326763084, idle age=410, tcp,vlan tci=0x0000,d1 src=00:00:00:00:00:01,d1 dst=00:00:00:00:00:02,nw src=10.1.1.10,nw_dst=10.2.2.20,nw_tos=0,tp_src=51882,tp_dst=5001 actions=output:1
```

```
*** s2 ***
NXST_FLOW reply (xid=0x4):
  cookie=0x0, duration=415.354s, table=0, n packets=513394, n bytes=19326764932, idle age=410, tcp,vlan tci=0x0000,d1 src=00:00:00:00:00:01,d1 dst=00:00:00:00:00:02,nw src=10.1.1.10,nw_dst=10.2.2.20,nw_tos=0,tp_src=51882,tp_dst=5001 actions=output:8
  cookie=0x0, duration=415.415s, table=0, n packets=4, n bytes=272, idle age=415, tcp,vlan tci=0x0000,d1 src=00:00:00:00:00:01,d1 dst=00:00:00:00:00:02,nw src=10.1.1.10,nw_dst=10.2.2.20,nw_tos=16,tp_src=51881,tp_dst=5001 actions=output:8
  cookie=0x0, duration=415.353s, table=0, n packets=147389, n bytes=9272682, idle age=410, tcp,vlan tci=0x0000,d1 src=00:00:00:00:00:02,d1 dst=00:00:00:00:00:01,nw src=10.2.2.20,nw_dst=10.1.1.10,nw_tos=0,tp_src=5001,tp_dst=51882 actions=output:1
  cookie=0x0, duration=615.837s, table=0, n packets=1, n bytes=42, idle age=615, arp,vlan tci=0x0000,d1 src=00:00:00:00:00:04,d1 dst=00:00:00:00:00:05,arp_spa=123.45.67.89,arp_tpa=10.5.5.50,arp_op=1 actions=FLOW00
  cookie=0x0, duration=706.719s, table=0, n packets=1, n bytes=42, idle age=706, tcp,vlan tci=0x0000,d1 src=00:00:00:00:00:03,d1 dst=00:00:00:00:00:01,arp_spa=10.3.3.30,arp_tpa=10.1.1.10,arp_op=2 actions=FLOW00
  cookie=0x0, duration=1169.235s, table=0, n packets=2, n bytes=84, idle age=615, arp,vlan tci=0x0000,d1 src=00:00:00:00:00:05,d1 dst=00:00:00:00:00:04,arp_spa=10.5.5.50,arp_tpa=123.45.67.89,arp_op=2 actions=FLOW00
  cookie=0x0, duration=649.453s, table=0, n packets=1, n bytes=42, idle age=649, arp,vlan tci=0x0000,d1 src=00:00:00:00:00:01,d1 dst=00:00:00:00:00:05,arp_spa=10.1.1.10,arp_tpa=10.5.5.50,arp_op=2 actions=FLOW00
```

```
*** s3 ***
NXST_FLOW reply (xid=0x4):
  cookie=0x0, duration=706.678s, table=0, n packets=277139, n bytes=18291182, idle age=701, tcp,vlan tci=0x0000,d1 src=00:00:00:00:00:03,d1 dst=00:00:00:00:00:01,nw src=10.3.3.30,nw_dst=10.1.1.10,nw_tos=0,tp_src=5001,tp_dst=42724 actions=output:1
  cookie=0x0, duration=706.68s, table=0, n packets=345657, n bytes=16215317202, idle age=701, tcp,vlan tci=0x0000,d1 src=00:00:00:00:00:01,d1 dst=00:00:00:00:00:03,nw src=10.1.1.10,nw_dst=10.3.3.30,nw_tos=0,tp_src=5001,tp_dst=5001 actions=output:8
  cookie=0x0, duration=706.723s, table=0, n packets=4, n bytes=272, idle age=706, tcp,vlan tci=0x0000,d1 src=00:00:00:00:00:01,d1 dst=00:00:00:00:00:03,nw src=10.1.1.10,nw_dst=10.3.3.30,nw_tos=16,tp_src=42723,tp_dst=5001 actions=output:8
  cookie=0x0, duration=706.722s, table=0, n packets=2, n bytes=140, idle age=706, tcp,vlan tci=0x0000,d1 src=00:00:00:00:00:03,d1 dst=00:00:00:00:00:01,nw src=10.3.3.30,nw_dst=10.1.1.10,nw_tos=0,tp_src=5001,tp_dst=42723 actions=output:1
  cookie=0x0, duration=615.844s, table=0, n packets=1, n bytes=42, idle age=615, arp,vlan tci=0x0000,d1 src=00:00:00:00:00:04,d1 dst=00:00:00:00:00:05,arp_spa=123.45.67.89,arp_tpa=10.5.5.50,arp_op=1 actions=FLOW00
  cookie=0x0, duration=706.735s, table=0, n packets=1, n bytes=42, idle age=706, arp,vlan tci=0x0000,d1 src=00:00:00:00:00:03,d1 dst=00:00:00:00:00:01,arp_spa=10.3.3.30,arp_tpa=10.1.1.10,arp_op=2 actions=FLOW00
  cookie=0x0, duration=1169.242s, table=0, n packets=2, n bytes=84, idle age=615, arp,vlan tci=0x0000,d1 src=00:00:00:00:00:05,d1 dst=00:00:00:00:00:04,arp_spa=10.5.5.50,arp_tpa=123.45.67.89,arp_op=2 actions=FLOW00
  cookie=0x0, duration=649.459s, table=0, n packets=1, n bytes=42, idle age=649, arp,vlan tci=0x0000,d1 src=00:00:00:00:00:01,d1 dst=00:00:00:00:00:05,arp_spa=10.1.1.10,arp_tpa=10.5.5.50,arp_op=2 actions=FLOW00
```

```
*** s4 ***
NXST_FLOW reply (xid=0x4):
  cookie=0x0, duration=415.361s, table=0, n packets=147389, n bytes=9272682, idle age=410, tcp,vlan tci=0x0000,d1 src=00:00:00:00:00:02,d1 dst=00:00:00:00:00:01,nw src=10.2.2.20,nw_dst=10.1.1.10,nw_tos=0,tp_src=5001,tp_dst=51882 actions=output:1
  cookie=0x0, duration=649.44s, table=0, n packets=140321, n bytes=9270098, idle age=644, tcp,vlan tci=0x0000,d1 src=00:00:00:00:00:01,d1 dst=00:00:00:00:00:05,nw src=10.1.1.10,nw_dst=10.5.5.50,nw_tos=0,tp_src=5001,tp_dst=57611 actions=output:1
  cookie=0x0, duration=706.727s, table=0, n packets=4, n bytes=272, idle age=706, tcp,vlan tci=0x0000,d1 src=00:00:00:00:00:01,d1 dst=00:00:00:00:00:03,nw src=10.1.1.10,nw_dst=10.3.3.30,nw_tos=16,tp_src=42723,tp_dst=5001 actions=output:3
  cookie=0x0, duration=706.723s, table=0, n packets=2, n bytes=140, idle age=706, tcp,vlan tci=0x0000,d1 src=00:00:00:00:00:03,d1 dst=00:00:00:00:00:01,nw src=10.3.3.30,nw_dst=10.1.1.10,nw_tos=0,tp_src=5001,tp_dst=42723 actions=output:1
  cookie=0x0, duration=415.42s, table=0, n packets=3, n bytes=206, idle age=415, tcp,vlan tci=0x0000,d1 src=00:00:00:00:00:02,d1 dst=00:00:00:00:00:01,nw src=10.2.2.20,nw_dst=10.1.1.10,nw_tos=0,tp_src=5001,tp_dst=51881 actions=output:1
  cookie=0x0, duration=649.459s, table=0, n packets=4, n bytes=272, idle age=649, tcp,vlan tci=0x0000,d1 src=00:00:00:00:00:05,d1 dst=00:00:00:00:00:01,nw src=10.5.5.50,nw_dst=10.1.1.10,nw_tos=16,tp_src=57610,tp_dst=5001 actions=output:1
  cookie=0x0, duration=415.369s, table=0, n packets=513366, n bytes=19326763084, idle age=410, tcp,vlan tci=0x0000,d1 src=00:00:00:00:00:01,d1 dst=00:00:00:00:00:02,nw src=10.1.1.10,nw_dst=10.2.2.20,nw_tos=0,tp_src=51882,tp_dst=5001 actions=output:2
```

```
*** s5 ***
NXST_FLOW reply (xid=0x4):
  cookie=0x0, duration=649.444s, table=0, n packets=140372, n bytes=9273464, idle age=644, tcp,vlan tci=0x0000,d1 src=00:00:00:00:00:01,d1 dst=00:00:00:00:00:05,nw src=10.1.1.10,nw_dst=10.5.5.50,nw_tos=0,tp_src=5001,tp_dst=57611 actions=output:8
  cookie=0x0, duration=649.457s, table=0, n packets=627459, n bytes=16359931550, idle age=644, tcp,vlan tci=0x0000,d1 src=00:00:00:00:00:05,d1 dst=00:00:00:00:00:01,nw src=10.5.5.50,nw_dst=10.1.1.10,nw_tos=16,tp_src=57610,tp_dst=5001 actions=output:1
  cookie=0x0, duration=649.463s, table=0, n packets=3, n bytes=206, idle age=649, tcp,vlan tci=0x0000,d1 src=00:00:00:00:00:01,d1 dst=00:00:00:00:00:05,nw src=10.1.1.10,nw_dst=10.5.5.50,nw_tos=0,tp_src=5001,tp_dst=57610 actions=output:8
  cookie=0x0, duration=615.855s, table=0, n packets=1, n bytes=42, idle age=615, arp,vlan tci=0x0000,d1 src=00:00:00:00:00:04,d1 dst=00:00:00:00:00:05,arp_spa=123.45.67.89,arp_tpa=10.5.5.50,arp_op=1 actions=FLOW00
  cookie=0x0, duration=706.736s, table=0, n packets=1, n bytes=42, idle age=706, arp,vlan tci=0x0000,d1 src=00:00:00:00:00:03,d1 dst=00:00:00:00:00:01,arp_spa=10.3.3.30,arp_tpa=10.1.1.10,arp_op=2 actions=FLOW00
  cookie=0x0, duration=1169.257s, table=0, n packets=2, n bytes=84, idle age=615, arp,vlan tci=0x0000,d1 src=00:00:00:00:00:05,d1 dst=00:00:00:00:00:04,arp_spa=10.5.5.50,arp_tpa=123.45.67.89,arp_op=2 actions=FLOW00
  cookie=0x0, duration=649.47s, table=0, n packets=1, n bytes=42, idle age=649, arp,vlan tci=0x0000,d1 src=00:00:00:00:00:01,d1 dst=00:00:00:00:00:05,arp_spa=10.1.1.10,arp_tpa=10.5.5.50,arp_op=2 actions=FLOW00
```