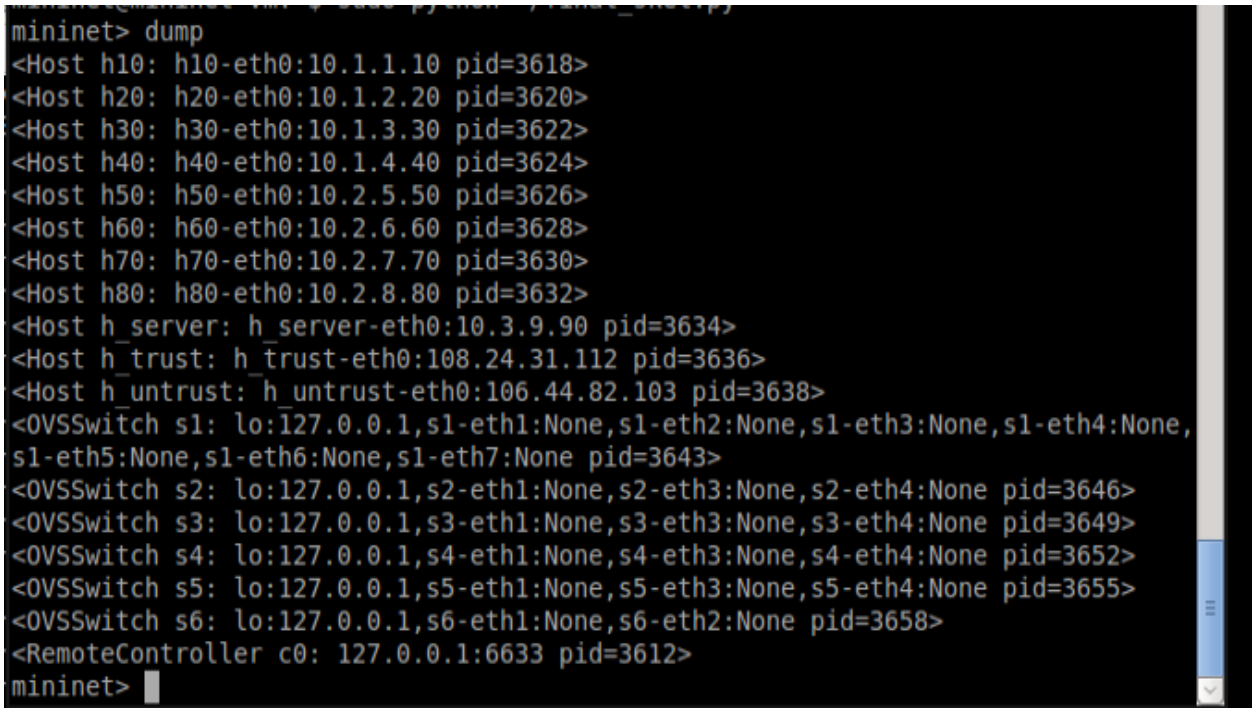
Darren Lee
Final Project
CSE150

dump



Dump is a command to dump all the information about all nodes and shows that the devices were created successfully. It shows that all the hosts and switches are set up correctly in the mininet topology for final_skel.py. We can see the IP addresses and pids for hosts h10 through h_untrust and that the IP addresses are correct according to the lab specification. The IP address of the localhost and the ethernet are given too. Also listed are the pids for switch s1 through switch s6 and controller c0. The port for the controller is 6633.

links

```
mininet> links
s1-eth6<->h_trust-eth0 (OK OK)
s1-eth7<->h_untrust-eth0 (OK OK)
s1-eth2<->s2-eth1 (OK OK)
s1-eth3<->s3-eth1 (OK OK)
s1-eth4<->s4-eth1 (OK OK)
s1-eth5<->s5-eth1 (OK OK)
s1-eth1<->s6-eth1 (OK OK)
s2-eth3<->h10-eth0 (OK OK)
s2-eth4<->h20-eth0 (OK OK)
s3-eth3<->h30-eth0 (OK OK)
s3-eth4<->h40-eth0 (OK OK)
s4-eth3<->h50-eth0 (OK OK)
s4-eth4<->h60-eth0 (OK OK)
s5-eth3<->h70-eth0 (OK OK)
s5-eth4<->h80-eth0 (OK OK)
s6-eth2<->h_server-eth0 (OK OK)
mininet>
```

The links command shows the links in the mininet topology. This screenshot shows that the topology is correctly set up because s1 is the core switch, s2 through s5 are the floor switches, and s6 is the data center switch. Then you can see that the switches are connected to the hosts that they are supposed to be as listed in the lab specification.

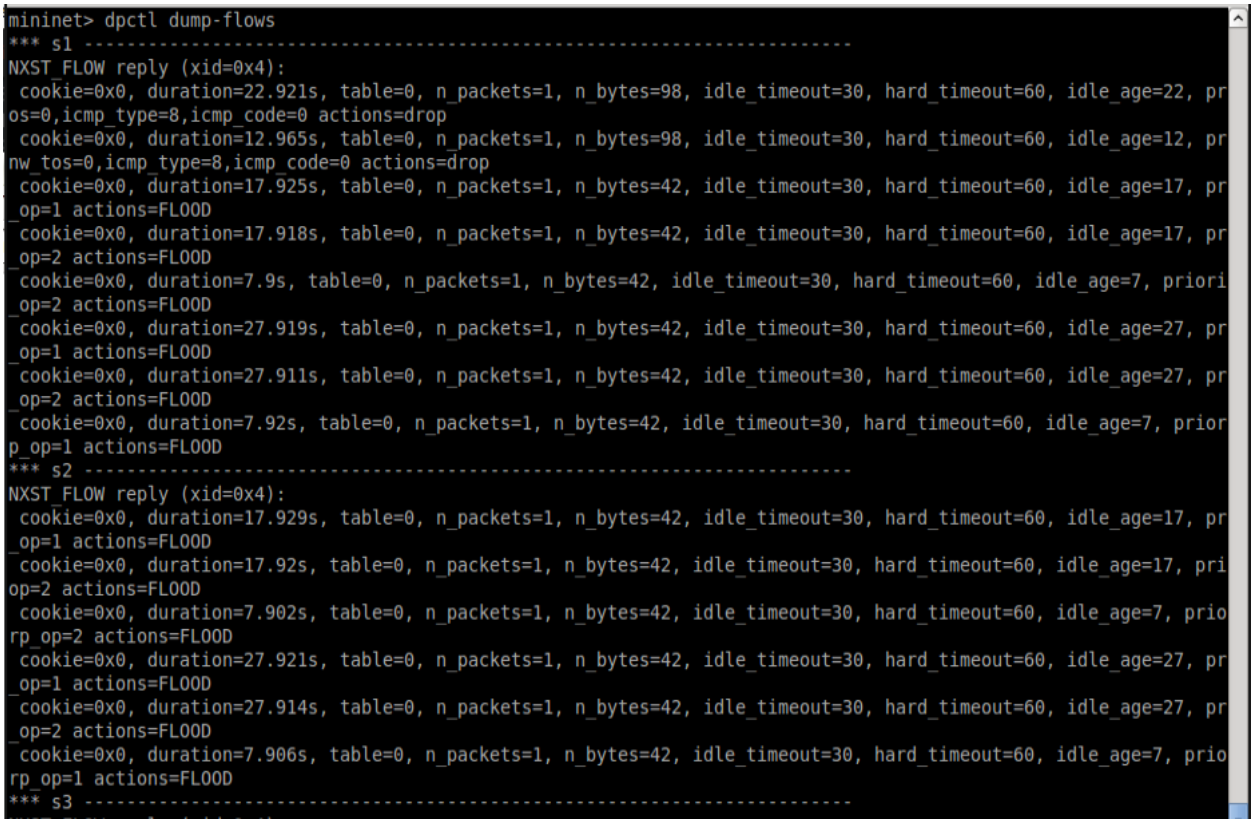
ICMP protocols
pingall

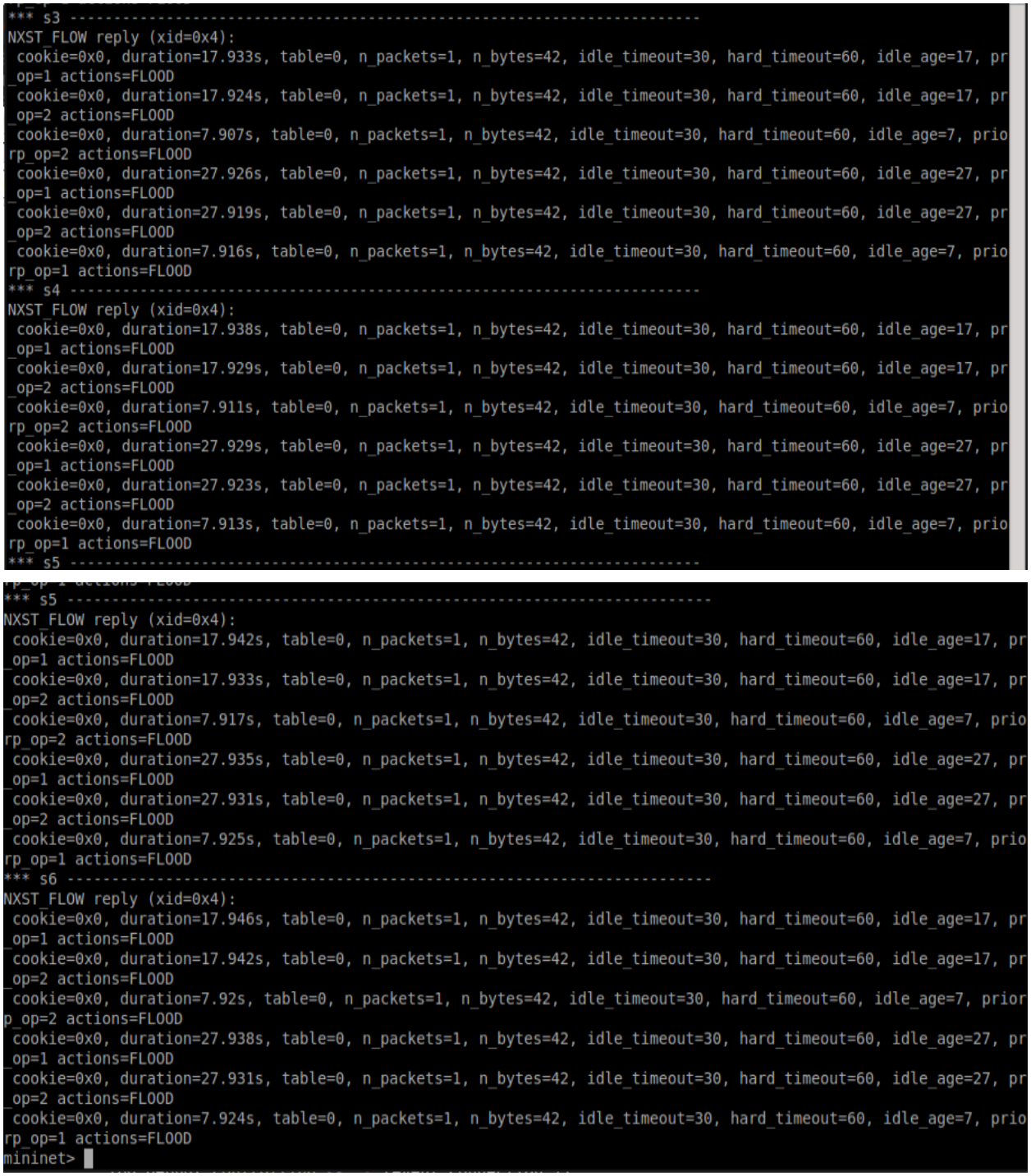
```
mininet> pingall
*** Ping: testing ping reachability
h10 -> h20 h30 h40 X X X X h_server h_trust X
h20 -> h10 h30 h40 X X X X h_server h_trust X
h30 -> h10 h20 h40 X X X X h_server h_trust X
h40 -> h10 h20 h30 X X X X h_server h_trust X
h50 -> X X X X h60 h70 h80 h_server X X
h60 -> X X X X h50 h70 h80 h_server X X
h70 -> X X X X h50 h60 h80 h_server X X
h80 -> X X X X h50 h60 h70 h_server X X
h_server -> h10 h20 h30 h40 h50 h60 h70 h80 X X
h_trust -> h10 h20 h30 h40 X X X X X X
h_untrust -> X X X X X X X X X X
*** Results: 56% dropped (48/110 received)
mininet>
```

I used pingall to check the ICMP traffic between each host. Pings that succeed show a correct connection using ICMP. Department A is unable to send ICMP messages to Department B. Department B cannot send ICMP packets to Department A either. The trusted host can only

send ICMP messages to Department A. the untrusted host cannot send packets to anyone because it cannot send IP or ICMP packets anywhere. The external hosts outside our networks h_trust and h_untrust cannot receive a ping from each other because IP traffic is blocked. The untrusted host cannot send ICMP traffic to hosts 10 through 80. The untrusted and trusted hosts cannot send any traffic to the server. The trusted host cannot send ICMP traffic to hosts 50 through 80. Hosts 10 through 40 cannot send ICMp traffic to hosts 50 through 80.

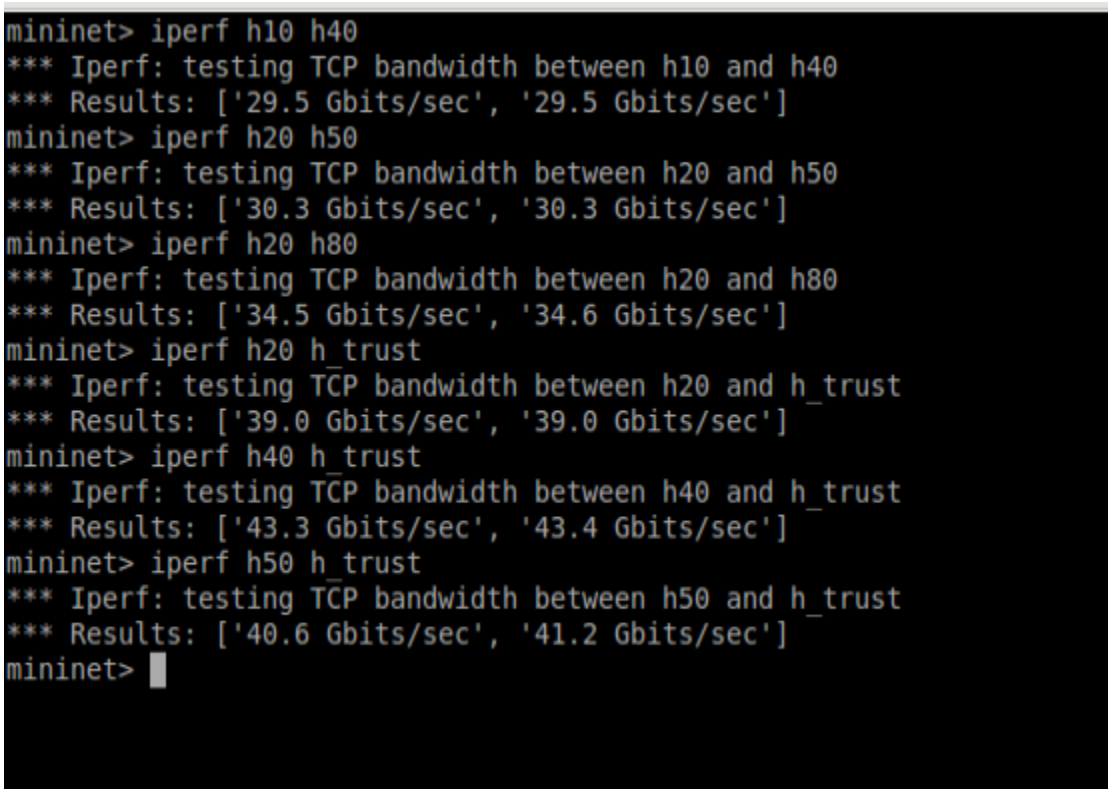
Flow table
dpctl dump-flows



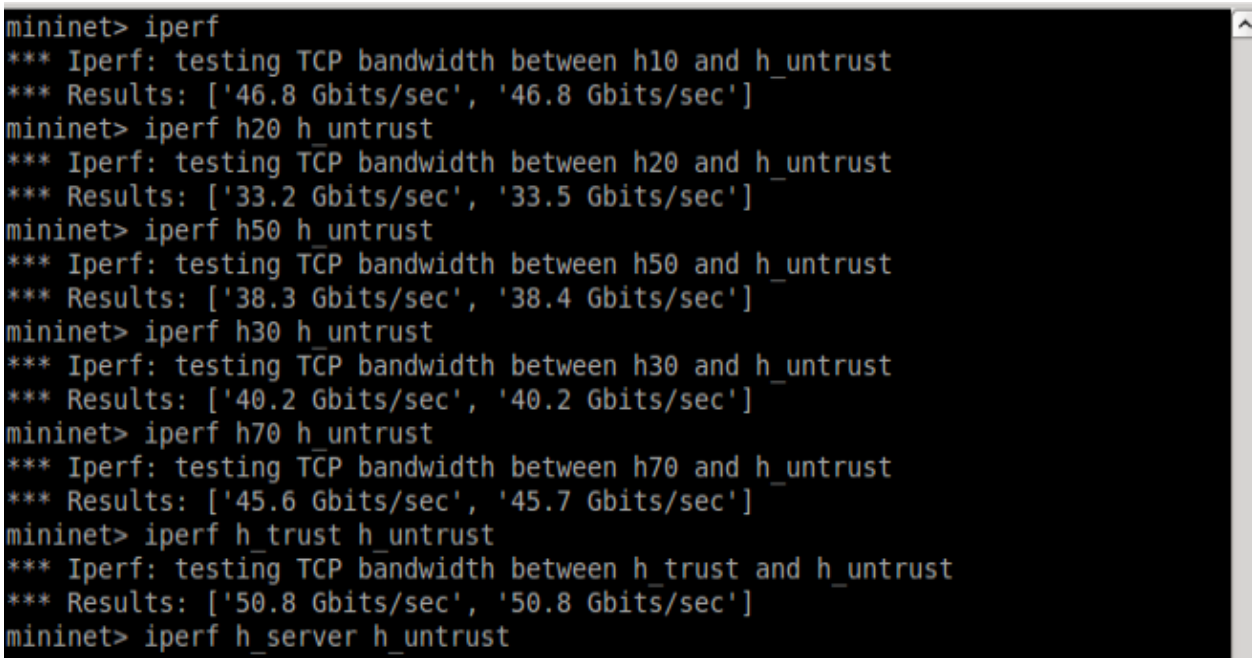


After running pingall, I ran the dpctl dump-flows command to see the installed flow mods in the table of each switch according to the rules specified in the lab document. For example, ICMP from the hosts in Department A (Host 10, 20, 30, 40) to the hosts in Department B (Host 50, 60, 70, 80) is blocked and vice versa. These table entries were installed to the switches when the switches got the first packets. The switches don't know how to process the first packets they receive, which is why these table entries need to be installed on the switches.

IP
Iperf



I used iperf to check the IP protocol access that was denied by the pingall command due to ICMP traffic control. Iperf can create a connection between Department A and B nodes. The trusted host can send TCP packets to both departments rather than just department A. Iperf uses TCP and TCP packets are allowed through the firewall in the channels shown above, so iperf succeeds.



The untrusted host is allowed to send TCP traffic to the hosts even though ICMP traffic from the untrusted host to the other hosts is blocked by the firewall.