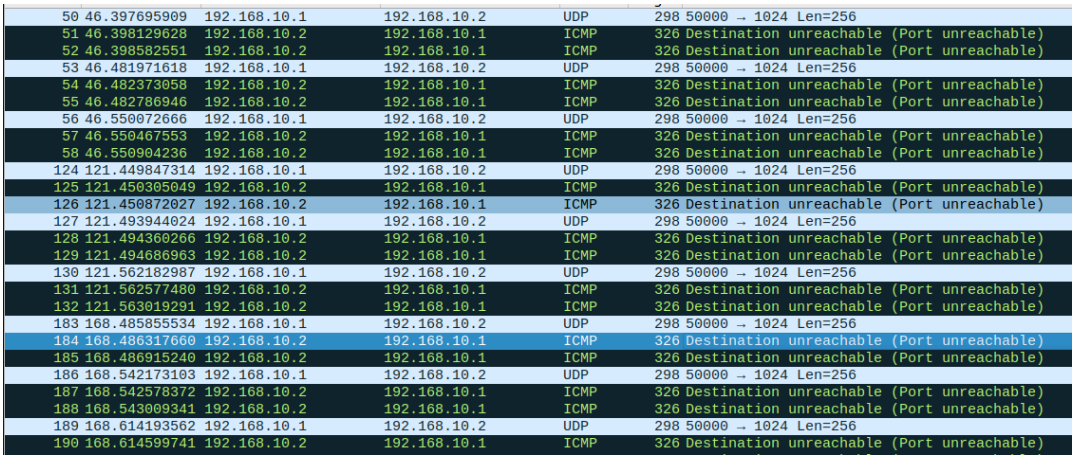
Running P4 Program

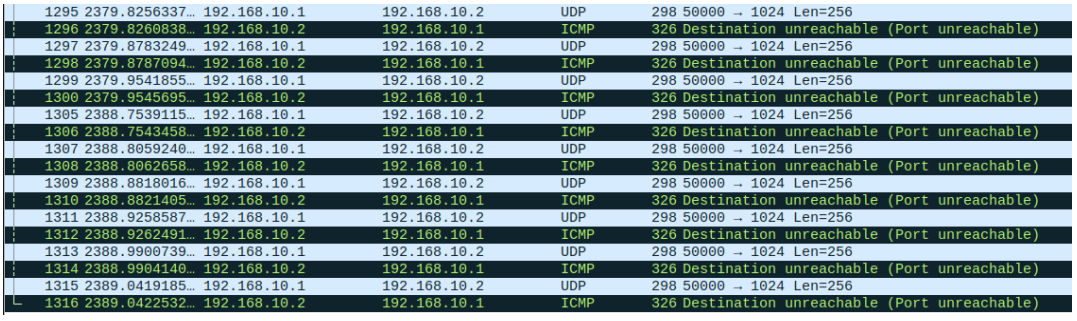
Q: Can you add table entries so the program will drop the packets you send? Yes. We can accomplish this by adding the mac address of the lab machine to the table of the reflector P4 program.



50	46.397695909	192.168.10.1	192.168.10.2	UDP	298 50000 → 1024 Len=256
51	46.398129628	192.168.10.2	192.168.10.1	ICMP	326 Destination unreachable (Port unreachable)
52	46.398582551	192.168.10.2	192.168.10.1	ICMP	326 Destination unreachable (Port unreachable)
53	46.481971618	192.168.10.1	192.168.10.2	UDP	298 50000 → 1024 Len=256
54	46.482373058	192.168.10.2	192.168.10.1	ICMP	326 Destination unreachable (Port unreachable)
55	46.482786946	192.168.10.2	192.168.10.1	ICMP	326 Destination unreachable (Port unreachable)
56	46.550072666	192.168.10.1	192.168.10.2	UDP	298 50000 → 1024 Len=256
57	46.550467553	192.168.10.2	192.168.10.1	ICMP	326 Destination unreachable (Port unreachable)
58	46.550904236	192.168.10.2	192.168.10.1	ICMP	326 Destination unreachable (Port unreachable)
124	121.449847314	192.168.10.1	192.168.10.2	UDP	298 50000 → 1024 Len=256
125	121.450305049	192.168.10.2	192.168.10.1	ICMP	326 Destination unreachable (Port unreachable)
126	121.450872027	192.168.10.2	192.168.10.1	ICMP	326 Destination unreachable (Port unreachable)
127	121.493944024	192.168.10.1	192.168.10.2	UDP	298 50000 → 1024 Len=256
128	121.494360266	192.168.10.2	192.168.10.1	ICMP	326 Destination unreachable (Port unreachable)
129	121.494686963	192.168.10.2	192.168.10.1	ICMP	326 Destination unreachable (Port unreachable)
130	121.562182987	192.168.10.1	192.168.10.2	UDP	298 50000 → 1024 Len=256
131	121.562577480	192.168.10.2	192.168.10.1	ICMP	326 Destination unreachable (Port unreachable)
132	121.563019291	192.168.10.2	192.168.10.1	ICMP	326 Destination unreachable (Port unreachable)
183	168.485855534	192.168.10.1	192.168.10.2	UDP	298 50000 → 1024 Len=256
184	168.486317660	192.168.10.2	192.168.10.1	ICMP	326 Destination unreachable (Port unreachable)
185	168.486915240	192.168.10.2	192.168.10.1	ICMP	326 Destination unreachable (Port unreachable)
186	168.542173103	192.168.10.1	192.168.10.2	UDP	298 50000 → 1024 Len=256
187	168.542578372	192.168.10.2	192.168.10.1	ICMP	326 Destination unreachable (Port unreachable)
188	168.543009341	192.168.10.2	192.168.10.1	ICMP	326 Destination unreachable (Port unreachable)
189	168.614193562	192.168.10.1	192.168.10.2	UDP	298 50000 → 1024 Len=256
190	168.614599741	192.168.10.2	192.168.10.1	ICMP	326 Destination unreachable (Port unreachable)

Figure 1: Traffic Capture of Modified Reflector

Notice that in the above traffic capture that for every UDP packet sent, we receive 2 ICMP error from the Rasberry Pi. One of the ICMP error is accounted for by the table dropping the packet, and the additional one is because we have set the send.py program with the lab machine's mac address and the Rasberry Pi's mac address, and this inflicts a systematic error within the Linux machine. If we had used completely random mac addresses, there would only be ICMP error message as shown in the below one.



1295	2379.8256337…	192.168.10.1	192.168.10.2	UDP	298 50000 → 1024 Len=256
1296	2379.8260838…	192.168.10.2	192.168.10.1	ICMP	326 Destination unreachable (Port unreachable)
1297	2379.8783249…	192.168.10.1	192.168.10.2	UDP	298 50000 → 1024 Len=256
1298	2379.8787094…	192.168.10.2	192.168.10.1	ICMP	326 Destination unreachable (Port unreachable)
1299	2379.9541855…	192.168.10.1	192.168.10.2	UDP	298 50000 → 1024 Len=256
1300	2379.9545695…	192.168.10.2	192.168.10.1	ICMP	326 Destination unreachable (Port unreachable)
1305	2388.7539115…	192.168.10.1	192.168.10.2	UDP	298 50000 → 1024 Len=256
1306	2388.7543458…	192.168.10.2	192.168.10.1	ICMP	326 Destination unreachable (Port unreachable)
1307	2388.8059240…	192.168.10.1	192.168.10.2	UDP	298 50000 → 1024 Len=256
1308	2388.8062658…	192.168.10.2	192.168.10.1	ICMP	326 Destination unreachable (Port unreachable)
1309	2388.8818016…	192.168.10.1	192.168.10.2	UDP	298 50000 → 1024 Len=256
1310	2388.8821405…	192.168.10.2	192.168.10.1	ICMP	326 Destination unreachable (Port unreachable)
1311	2388.9258587…	192.168.10.1	192.168.10.2	UDP	298 50000 → 1024 Len=256
1312	2388.9262491…	192.168.10.2	192.168.10.1	ICMP	326 Destination unreachable (Port unreachable)
1313	2388.9900739…	192.168.10.1	192.168.10.2	UDP	298 50000 → 1024 Len=256
1314	2388.9904140…	192.168.10.2	192.168.10.1	ICMP	326 Destination unreachable (Port unreachable)
1315	2389.0419185…	192.168.10.1	192.168.10.2	UDP	298 50000 → 1024 Len=256
1316	2389.0422532…	192.168.10.2	192.168.10.1	ICMP	326 Destination unreachable (Port unreachable)

Figure 2: Traffic with Random Mac Address

Q: What is cwm command? The cwm command is a shell scripting script, and compose of the command to call reflector.p4. It is similar to any command in linux such cat or awk. chmod u+x gives user the execution permission of cwm. I modified the directory inside the command and the

name of the file to call the correct reflector.p4 file, and the effect is the same as executing the commands given in the notes.

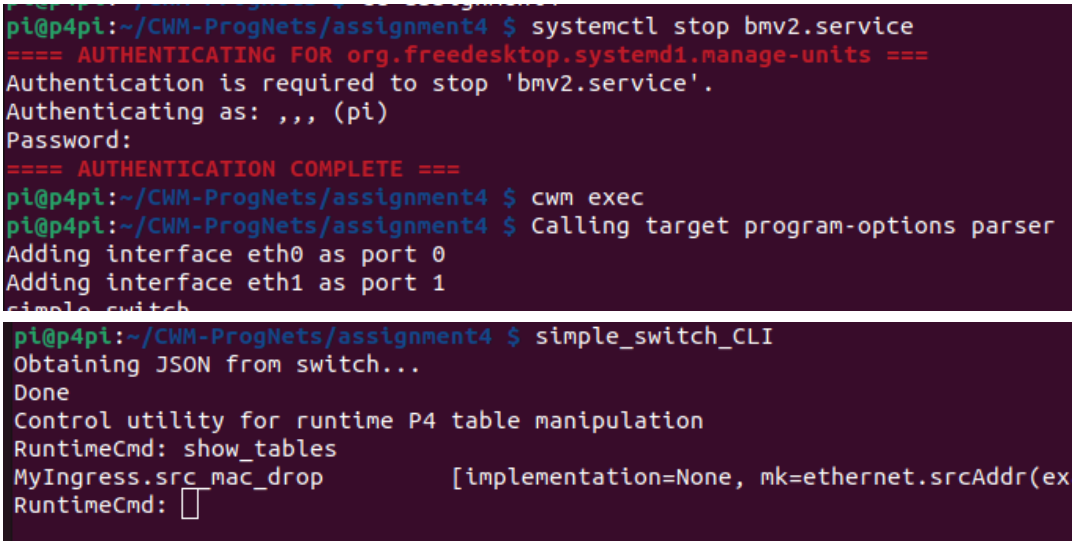


Figure 3: Effect of Excuting cwm Command