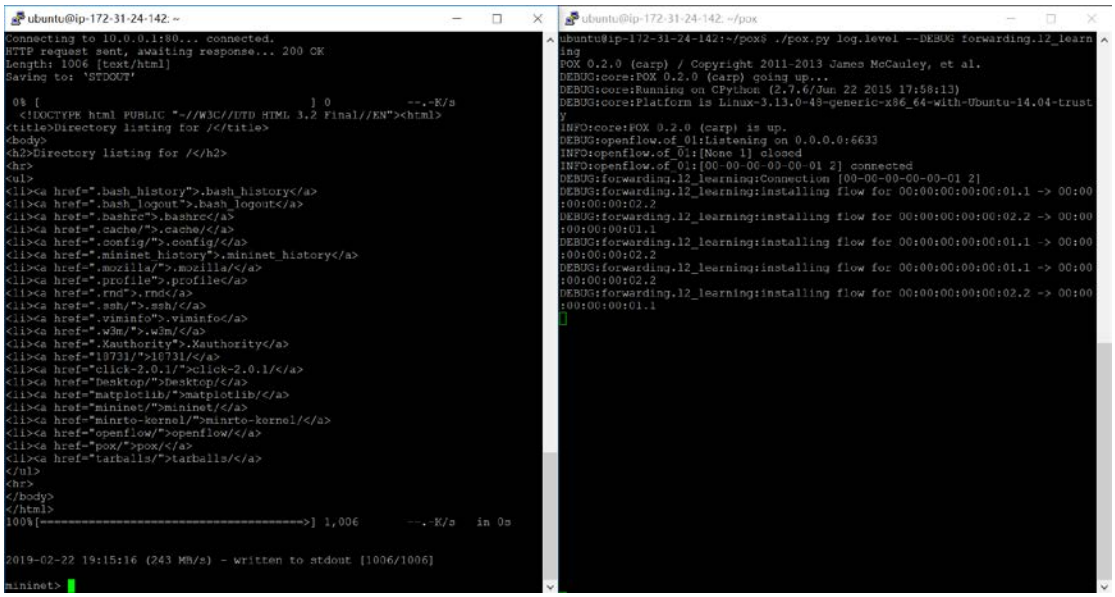
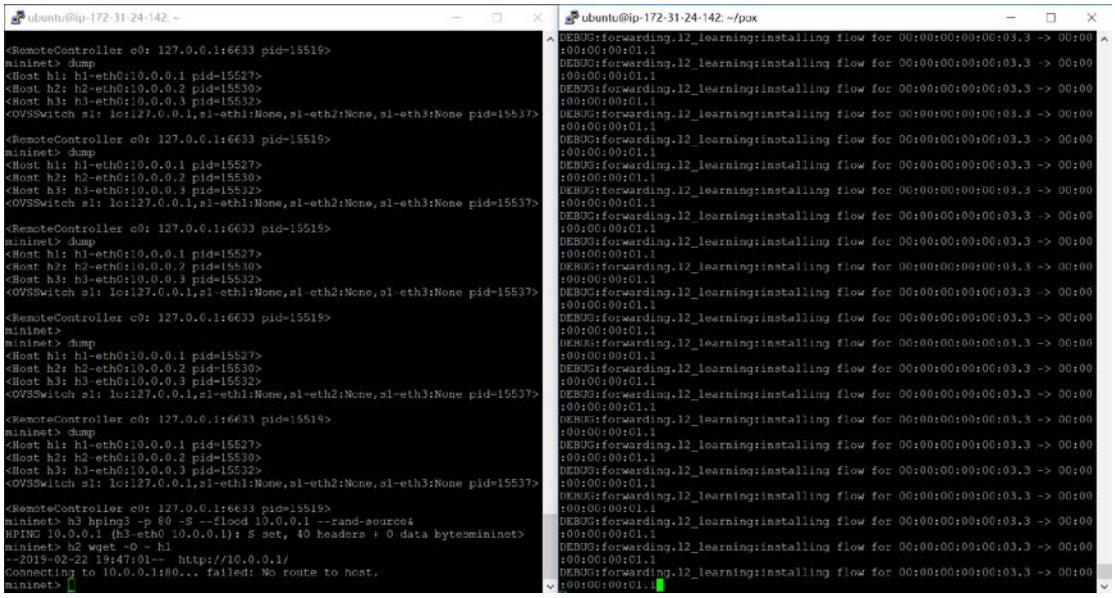
Reactive controller under SYN flood

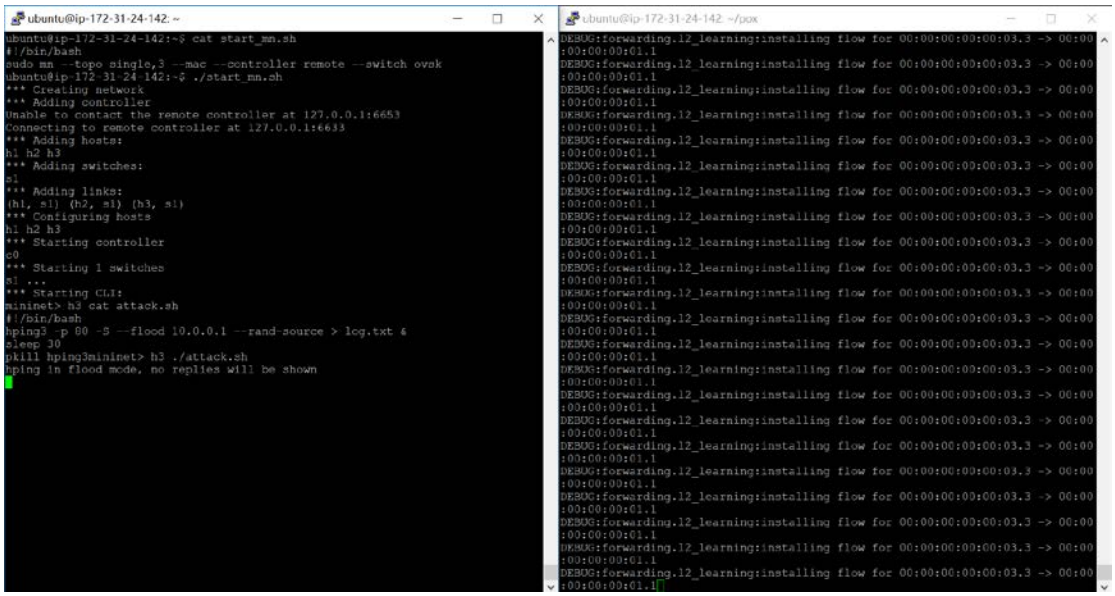
HTTP request, without DoS, reactive controller:



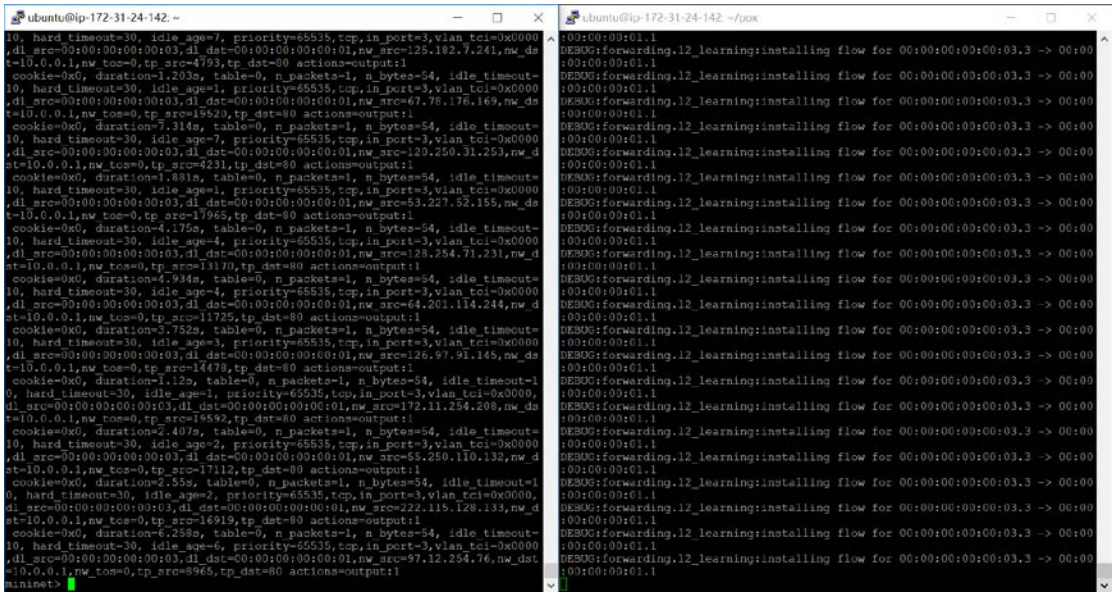
HTTP request, with DoS, reactive controller - request failed:



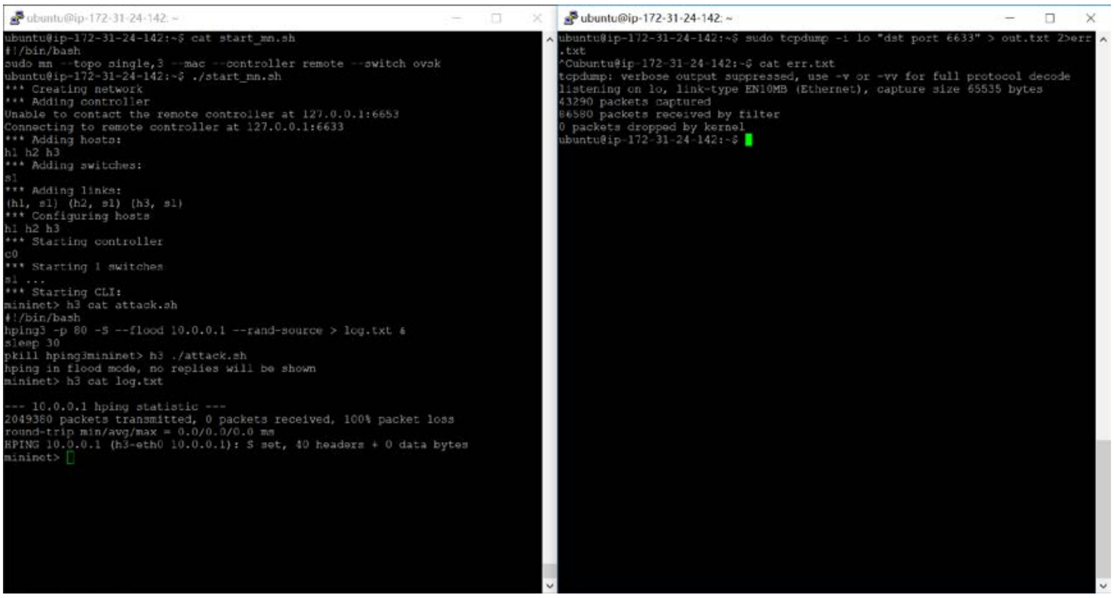
hping3 running:



A huge number of flows are inserted:

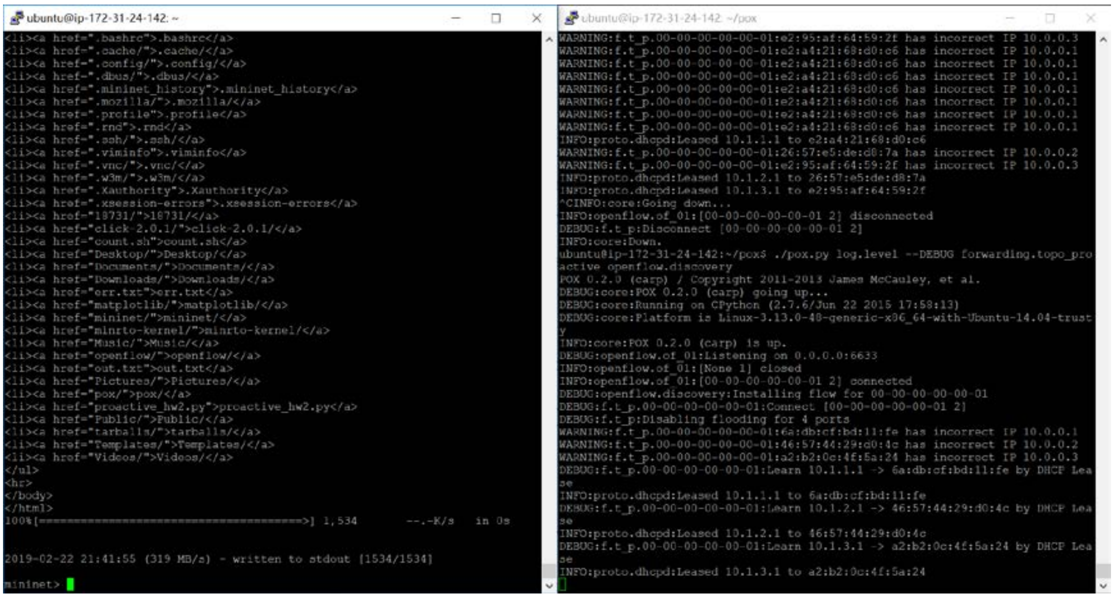


hping3 generated 2049380 TCP SYN packets in 30s, resulting in 43290 PACKET_IN to the controller:

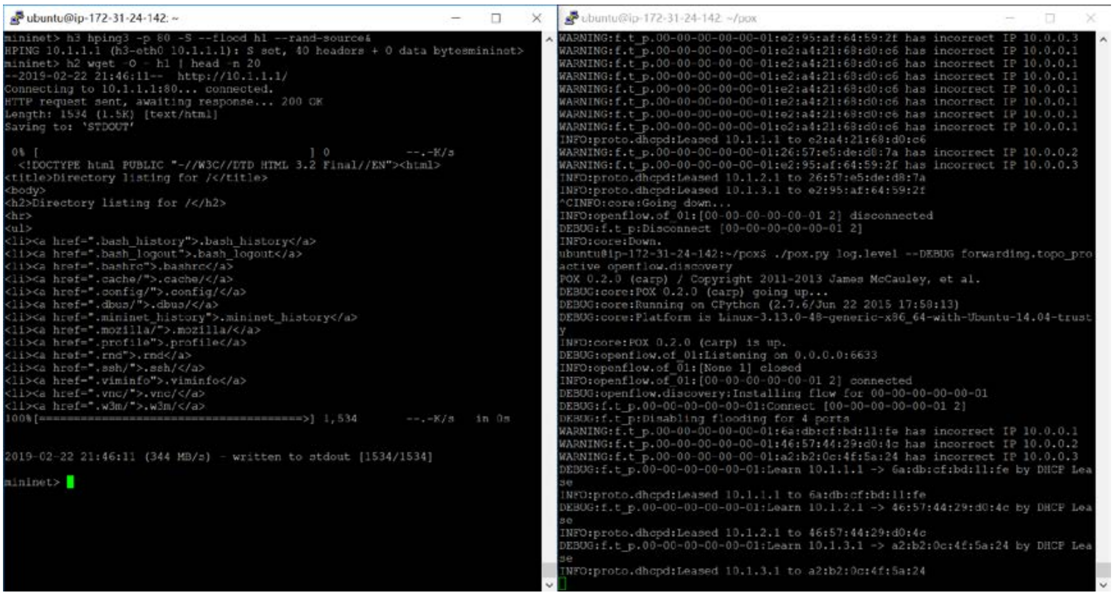


Proactive controller under SYN flood

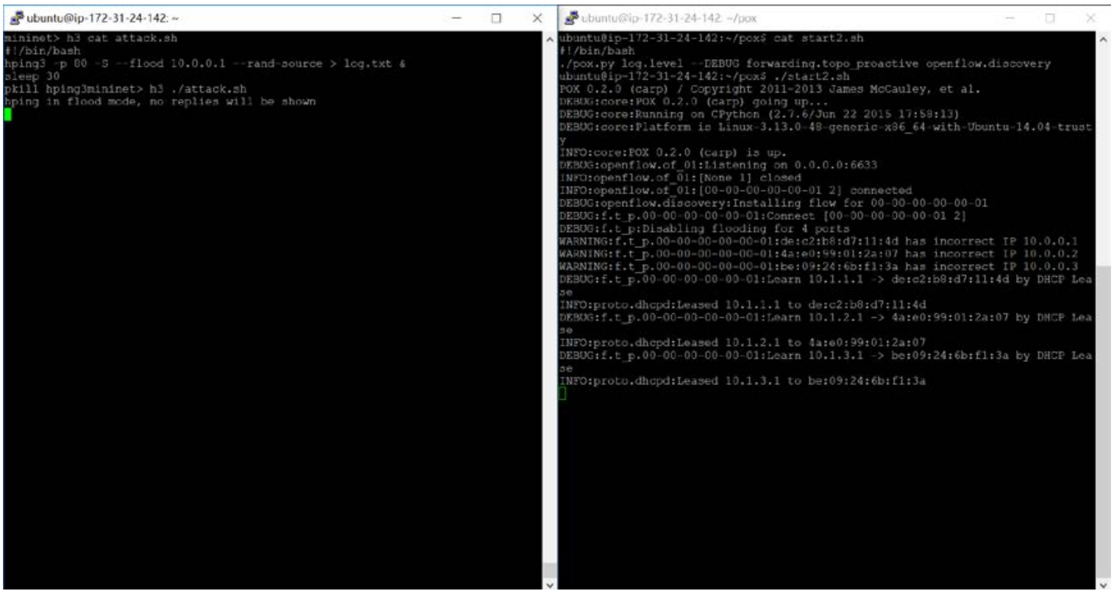
HTTP request, without DoS, proactive controller:



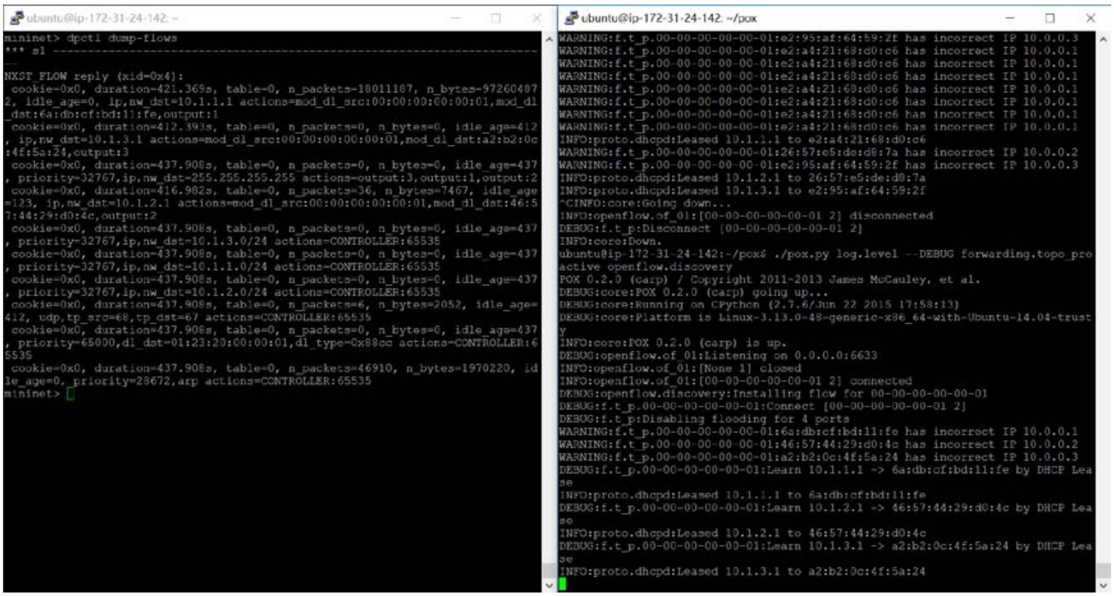
HTTP request, with DoS, proactive controller - request succeeded despite SYN flood attack:



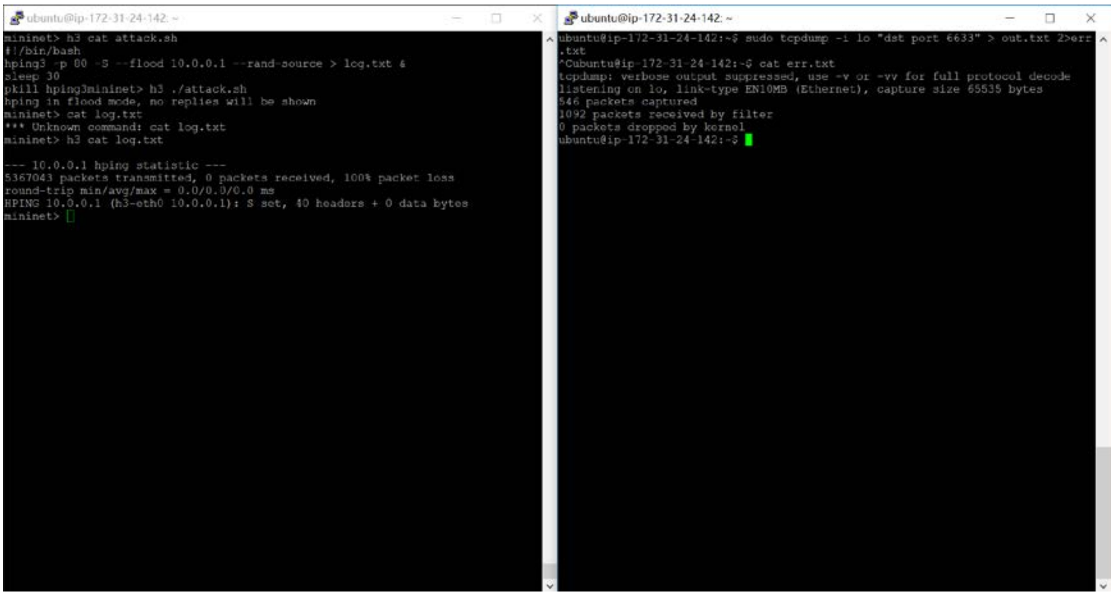
hping3 running, however, no flow is generated:



The flow table remains clean despite SYN flood attack:



hping3 generated 5367043 TCP SYN packets, but only 546 OpenFlow messages received by the controller:



Attack code explained

```
#!/bin/bash
hping3 -p 80 -S --flood 10.0.0.1 --rand-source > log.txt &
sleep 30
pkill hping3
```

The above script invokes hping3 to generate a SYN flood (lasting for 30s) to 10.0.0.1:80 with random source IPs. The frequency of SYN packets are ~100000 per second (from the stats in log.txt).

Difference between reactive and proactive controller:

With reactive controller, during a SYN flood attack, a huge number of requests are sent to the controller, and a huge number of flows are inserted, and the http request is completed blocked.

With proactive controller, during a SYN flood attack, the number of requests sent to the controller is limited, the flow table remains clean, and the http request goes unhindered.