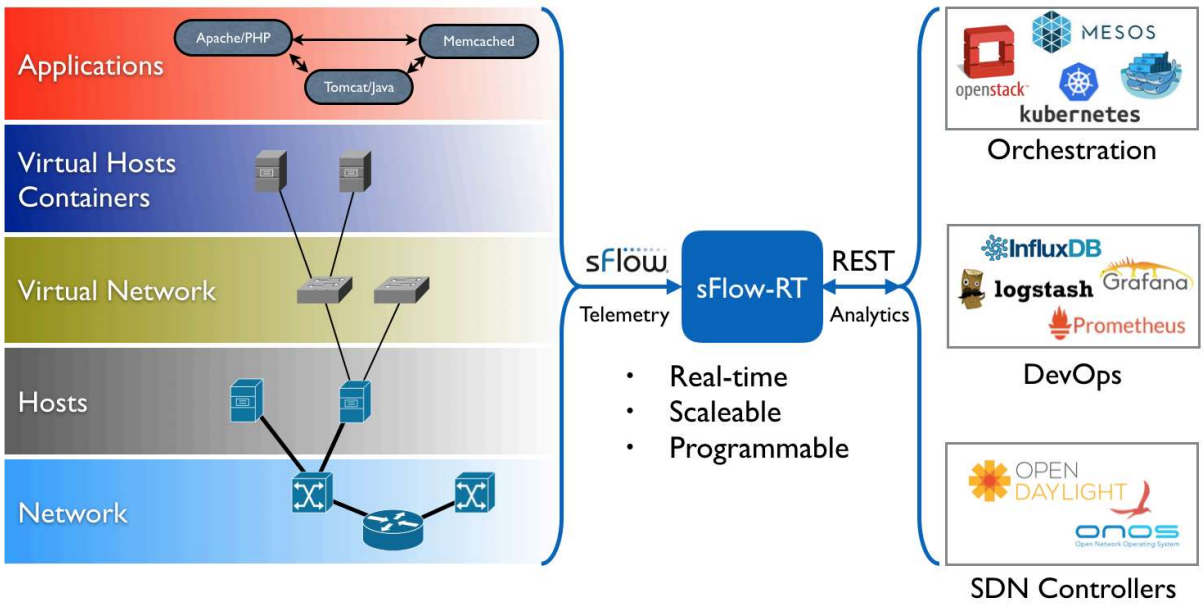
DDoS Attack Detection using SFlow in Software Defined Network

1. Objective:

- Detect the DDoS Attack using Sflow.

Sflow : it's an industry standard technology for monitoring high speed switched networks.It gives complete visibility into the use of networks enabling performance optimization, accounting/billing for usage, and defense against security threats.



This demonstration uses the sFlow-RT real-time analytics engine to process standard sFlow streaming telemetry from the network switches.

1.1. Download sFlow-RT:

- wget https://inmon.com/products/sFlow-RT/sflow-rt.tar.gz
- tar -xvzf sflow-rt.tar.gz

1.2. Install the Mininet Dashboard application:

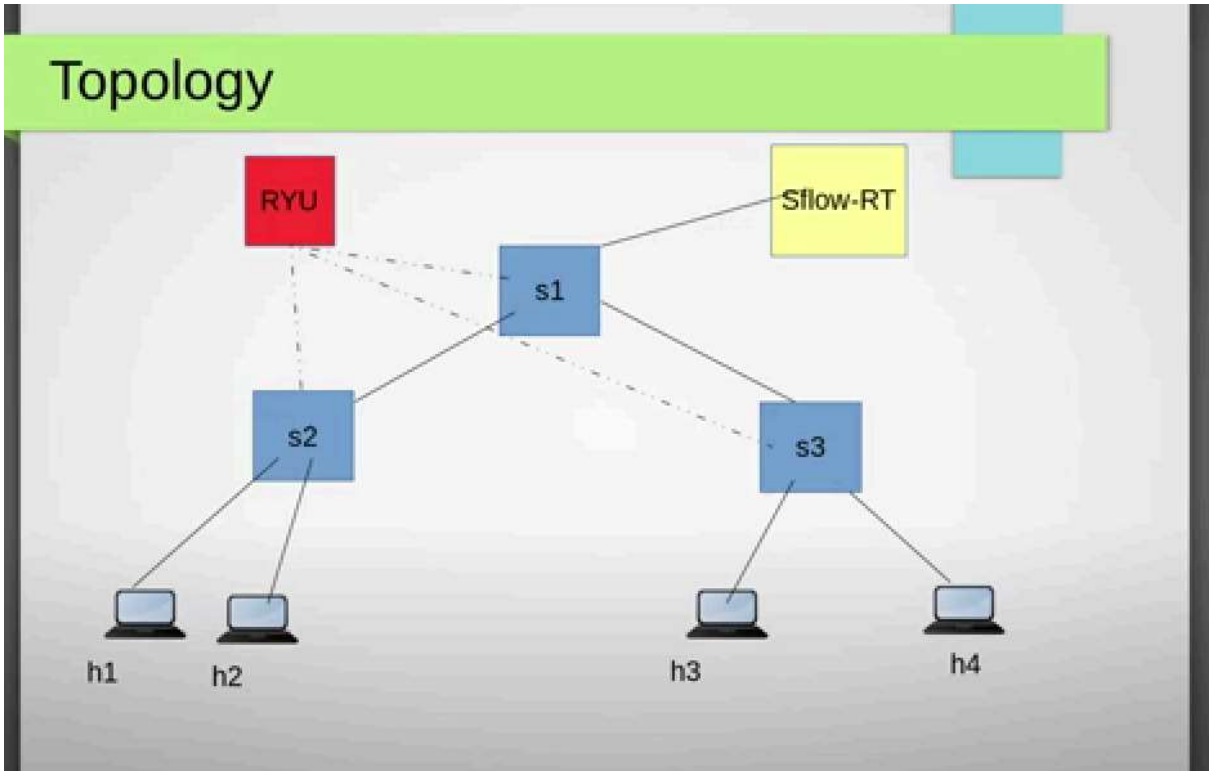
- sflow-rt/get-app.sh sflow-rt mininet-dashboard

1.3. start sFlow-RT :

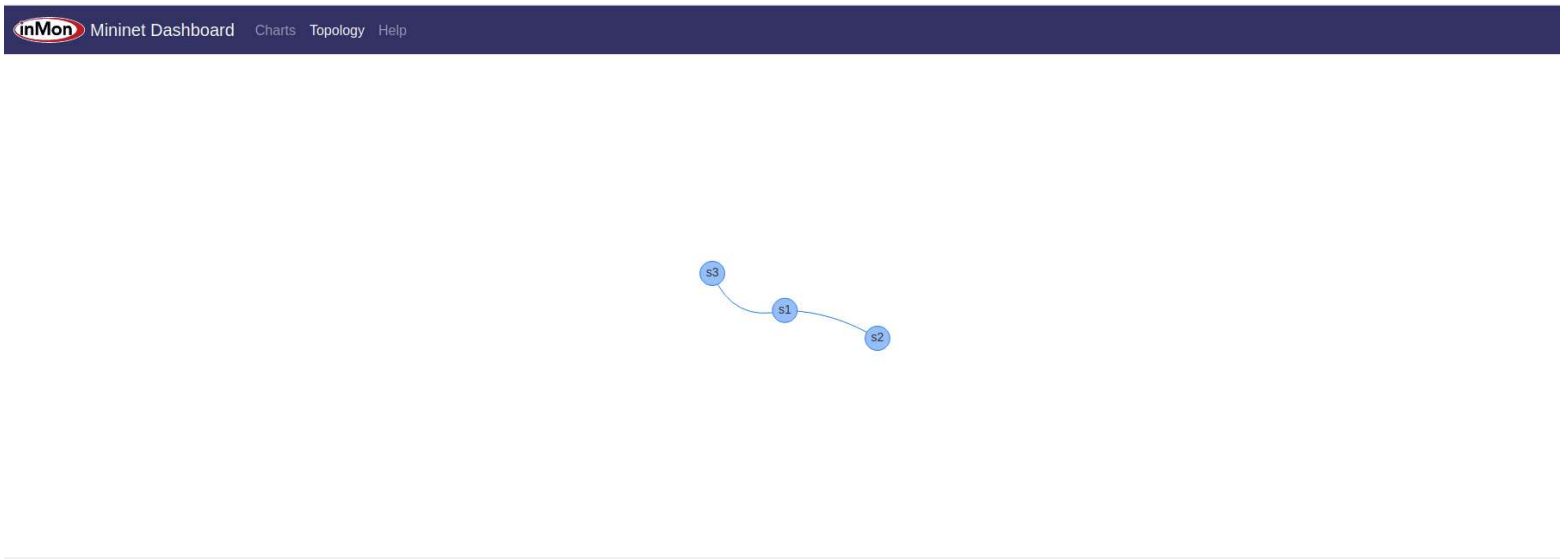
- ./sflow-rt/start.sh

We are going to use hping3 to simulate a DDoS attack, so install the software using the following command:
sudo apt install hping3

2. Topology :



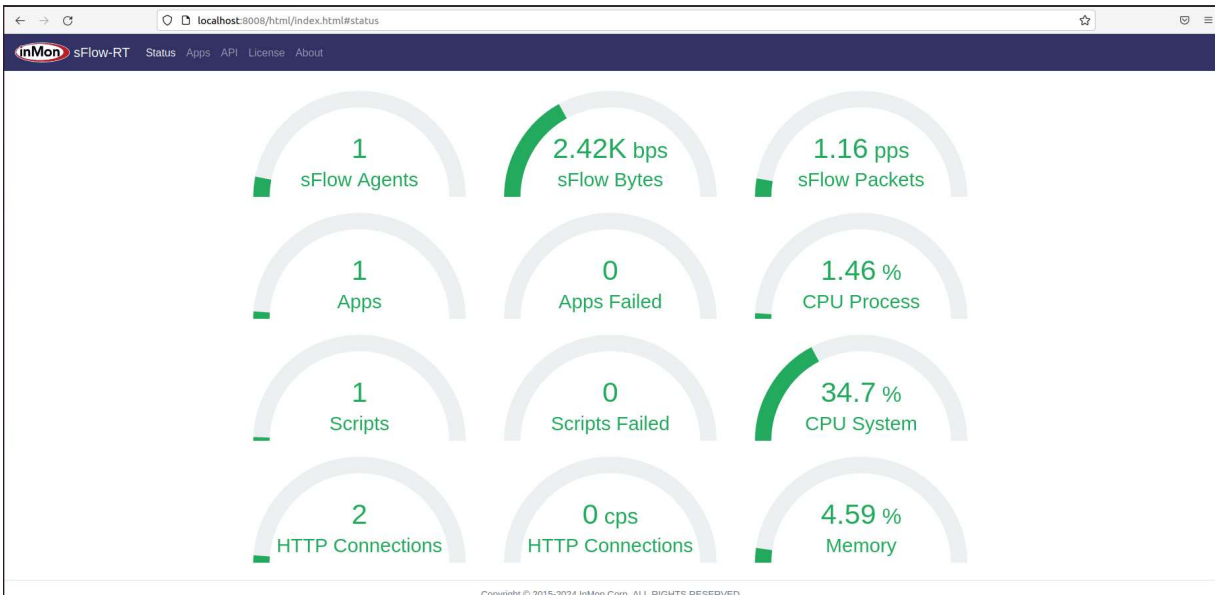
start Mininet:
sudo mn --custom sflow-rt/extras/sflow.py --link tc,bw=10 \
--controller=remote,ip=127.0.0.1 --topo tree,depth=2,fanout=2

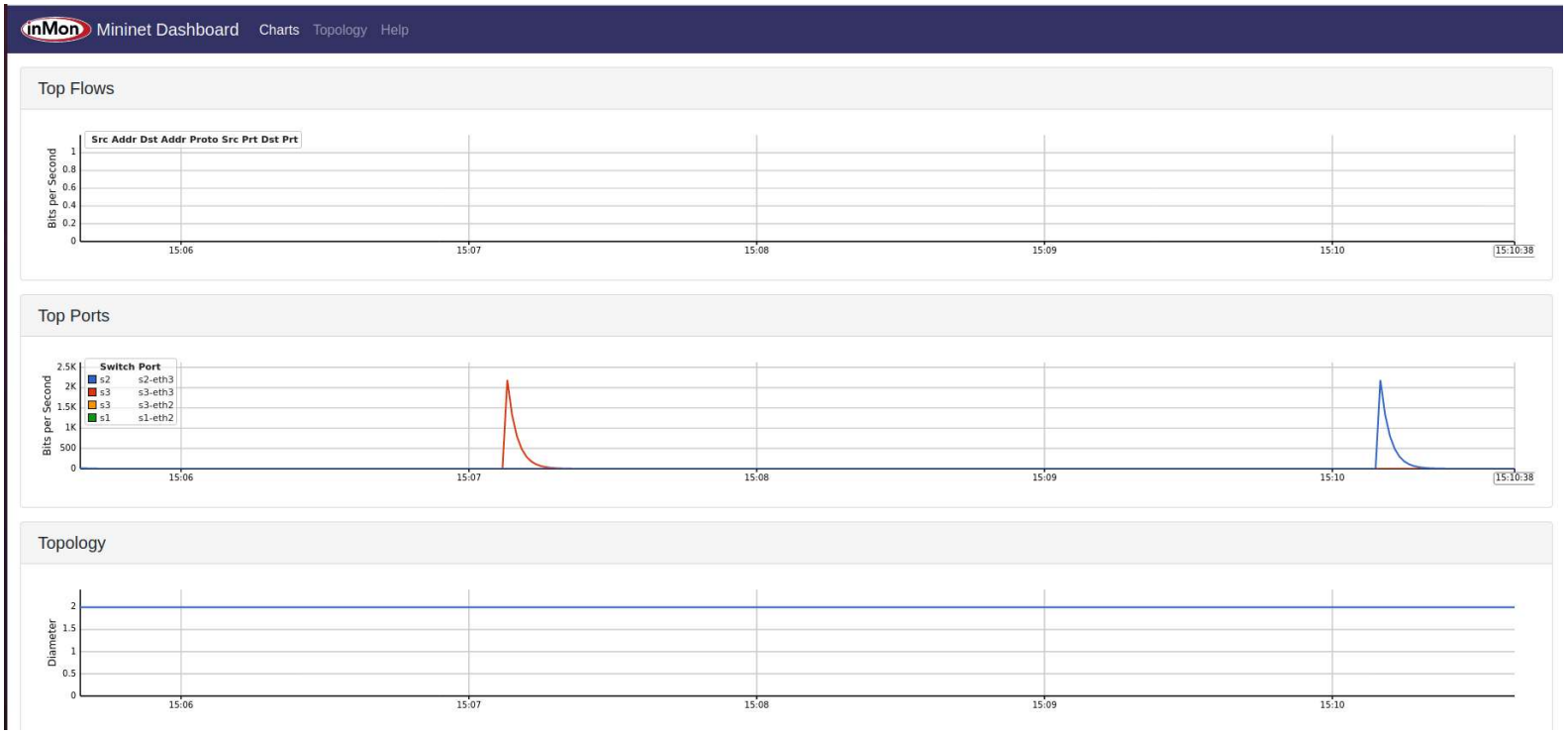


2.1. Logic :

- Switch s1 enabled Sflow, and configured to talk to the SFLOW-RT app.
- Sflow-RT monitors the switch traffic.
- Sflow-RT Detects the DdoS attack, and calls RYU REST API to /mitigate the attack.

Generate normal traffic between hosts *h1* and *h3*: iperf h1 h3





2.2. Generate an attack:

We use the hping3 tool to generate the attack.

```
mininet> h1 hping3 --flood --udp -k -s 53 h3
```