Contribution ID: **56** Type: **not specified**

# Topic 1: Issues capturing ALL traffic with Zeek?

*Wednesday 6 November 2024 13:30 (30 minutes)*

We have some sites that have question/potential issues concerning the traffic measurements from Zeek vs SNMP.
- Should be expect that the Zeek traffic estimate should be close to the SNMP counters from the corresponding switch ports?
- Is some kind of NIC/hardware offloading hiding traffic from Zeek?
- Do we have best practice recommendations regarding configurations?
- What should sites expect regarding Zeek traffic monitoring and traffic estimations?

**Presenters:** SHARMA, Aashish (LBNL); Dr CROOKS, David (UKRI STFC); JORDAN, David (University of Chicago (US)); MC KEE, Shawn (University of Michigan (US))

**Session Classification:** SOC Hackathon