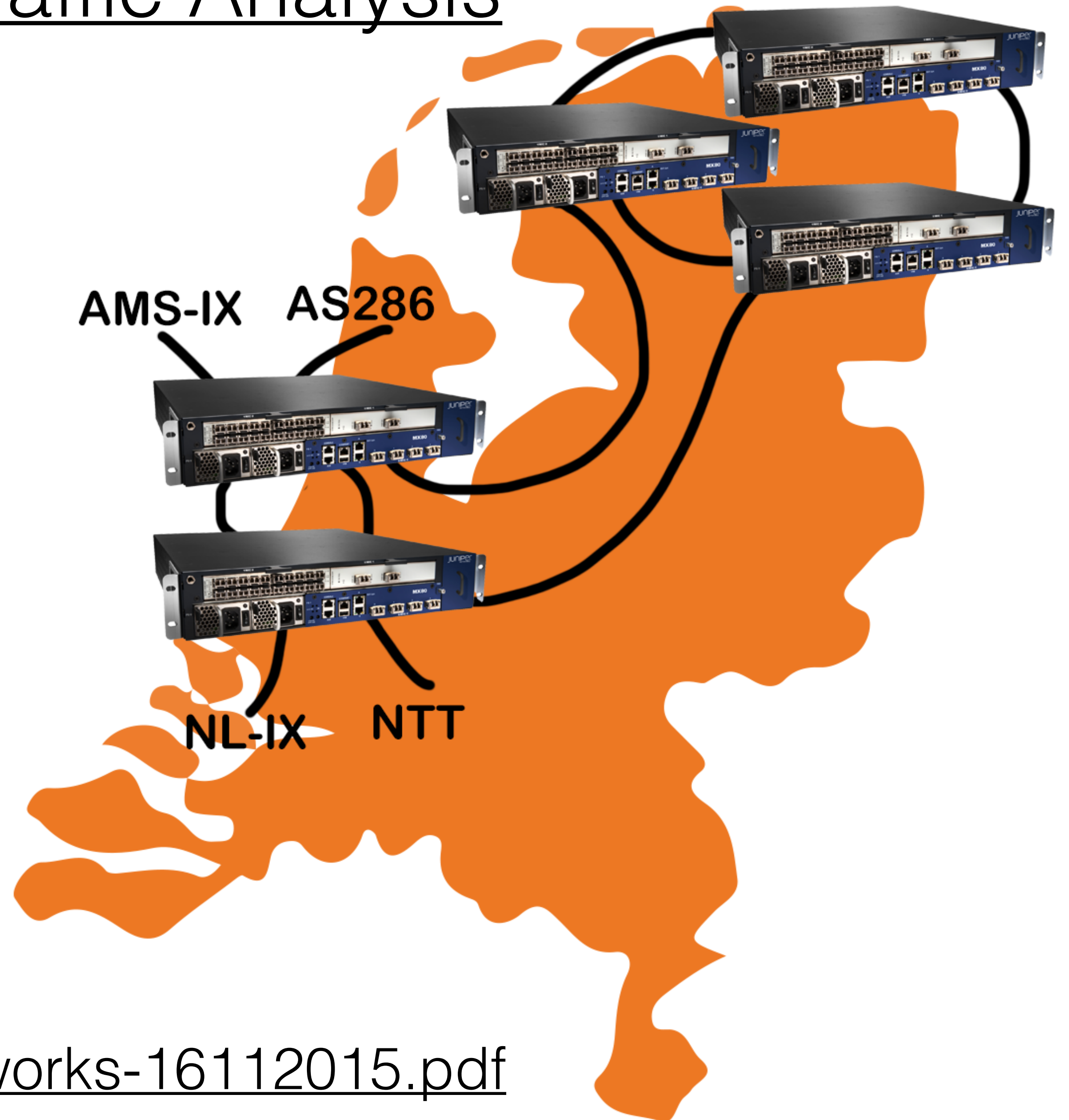


Cheap and Efficient DDoS Traffic Analysis

Fabian Labohm
f.labohm@duocast.nl
Duocast

Cheap and Efficient DDoS Traffic Analysis

- ASN: 31477
- Routing: Juniper MX80
- KRT Issue
Last major incident: 17-11-2015
Impact: 2x 20 mins *
- Netflow / Inline Jflow (ipfix)
- Fastnetmon implemenation

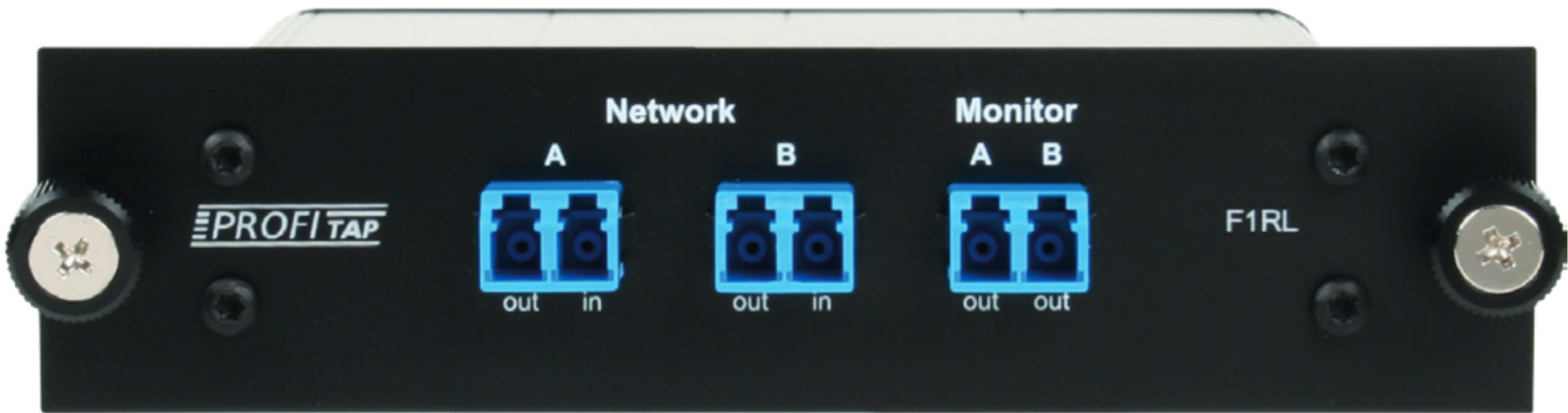
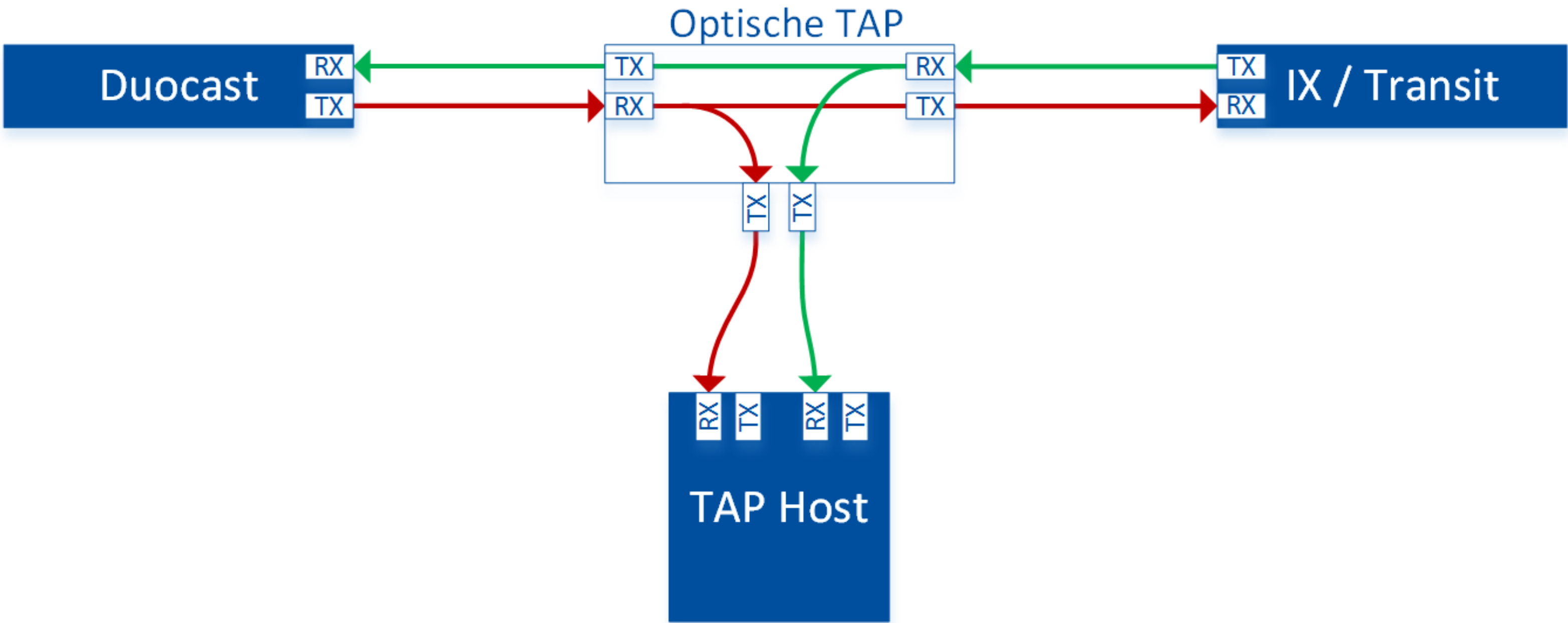


* <https://noc.duocast.net/rca-eunetworks-16112015.pdf>

Cheap and Efficient DDoS Traffic Analysis

- Doel:
 - Uitschakelen van Netflow, verlagen van load op routers
 - implementatie Fastnetmon
- Mogelijke oplossingen:
 - Portmirror op routers of aggregatie switches
 - Routers vervangen door MX240+
 - Optical taps

Cheap and Efficient DDoS Traffic Analysis

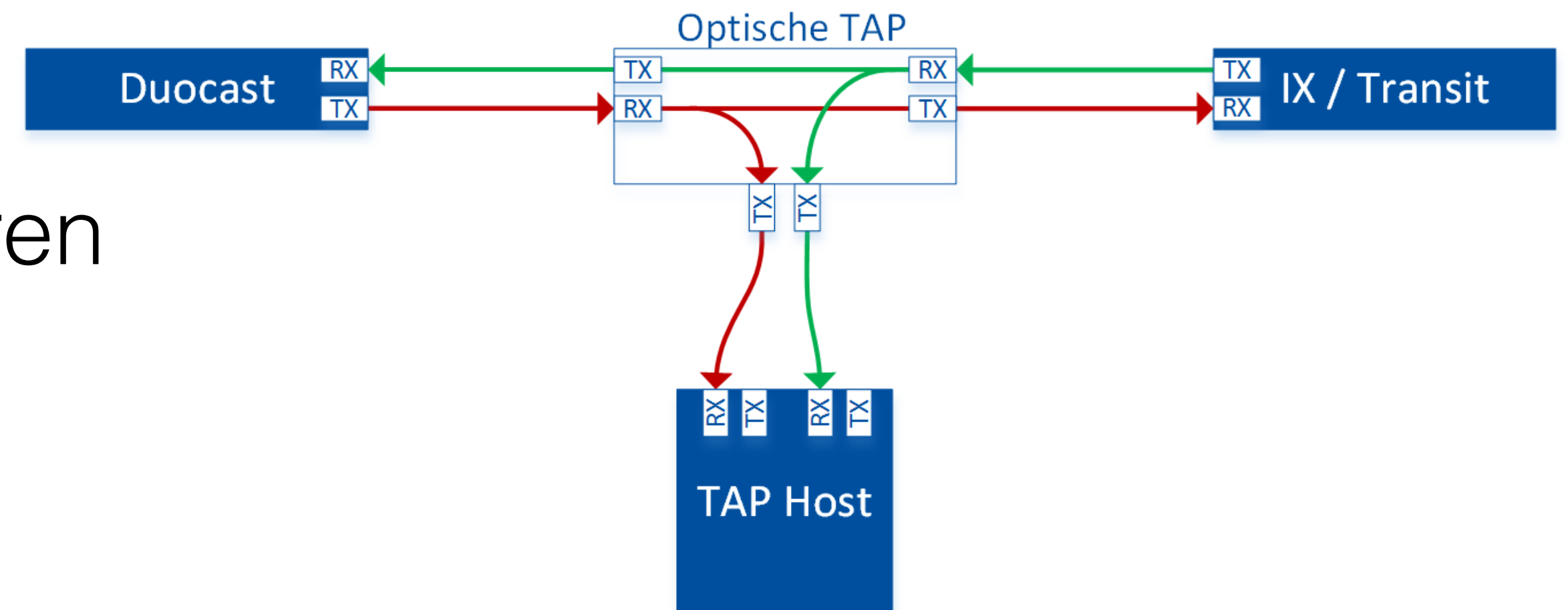


Rack-Mountable 1-Link LC TAP (F1RL)

Split ratio	50/50	60/40	70/30	80/20
Multi-Mode 50/62.5µm	4.0/4.0	3.0/5.0	2.4/6.3	1.8/8.1
Single-Mode 9µm	3.6/3.6	2.7/4.7	1.9/6.0	1.2/7.9

Cheap and Efficient DDoS Traffic Analysis

- 2 POPs in Amsterdam (Globalswitch, EuNetworks)
- 4 10Gbps uplinks (AMS-IX, NL-IX, NTT, KPN)
- 2 optische taps per POP
- 8 optische signalen om te monitoren

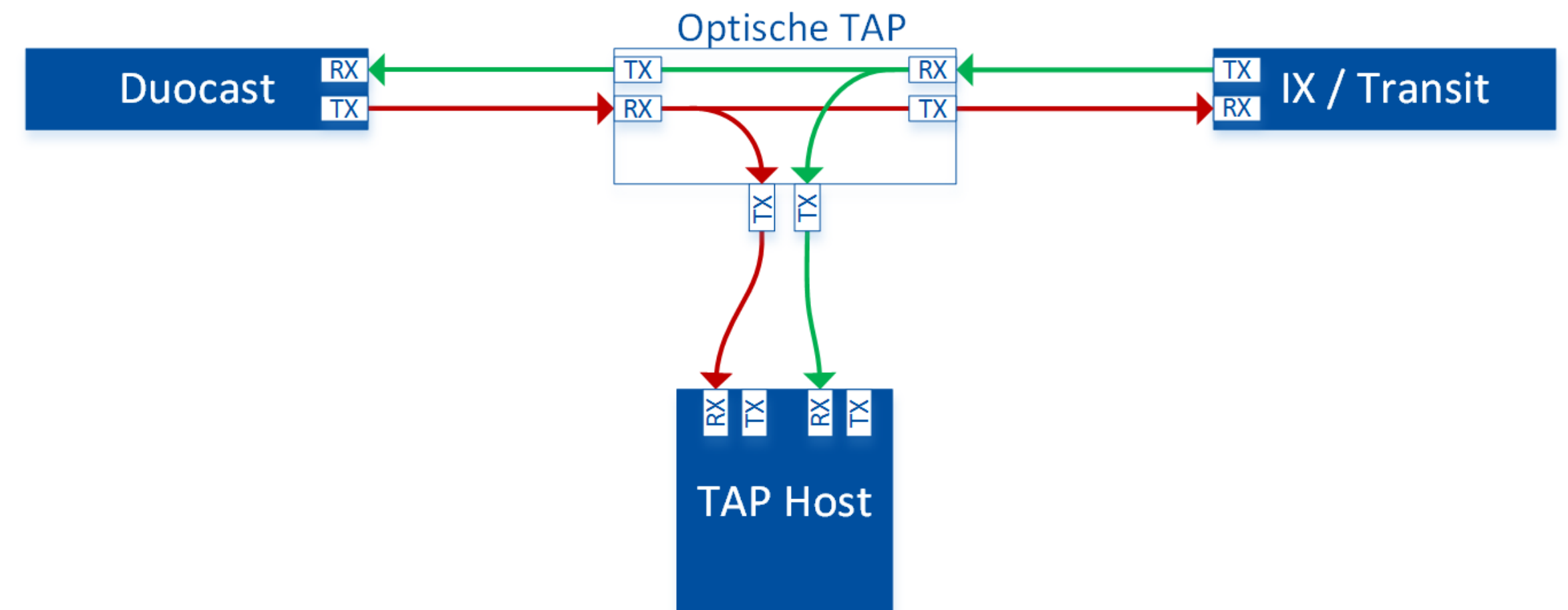


Cheap and Efficient DDoS Traffic Analysis

- TAP Host hardware
 - Supermicro met 2x E5-2620, 32GB, 2 disks raid1
 - 2x Intel X710-DA2 (dual port SFP+)
- Intel X710 NIC = 10GBase-SX en 10GBase-LX optics only

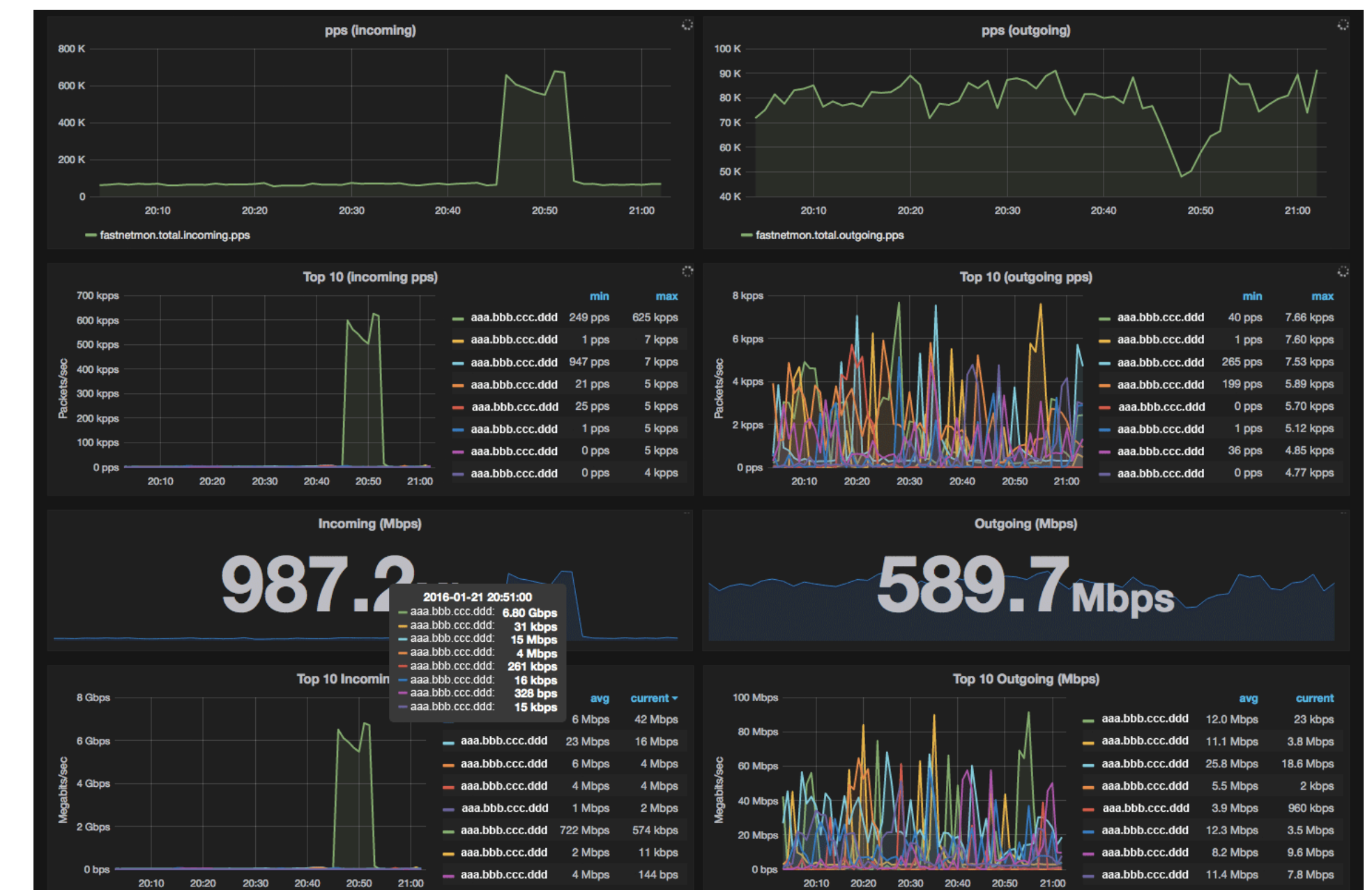
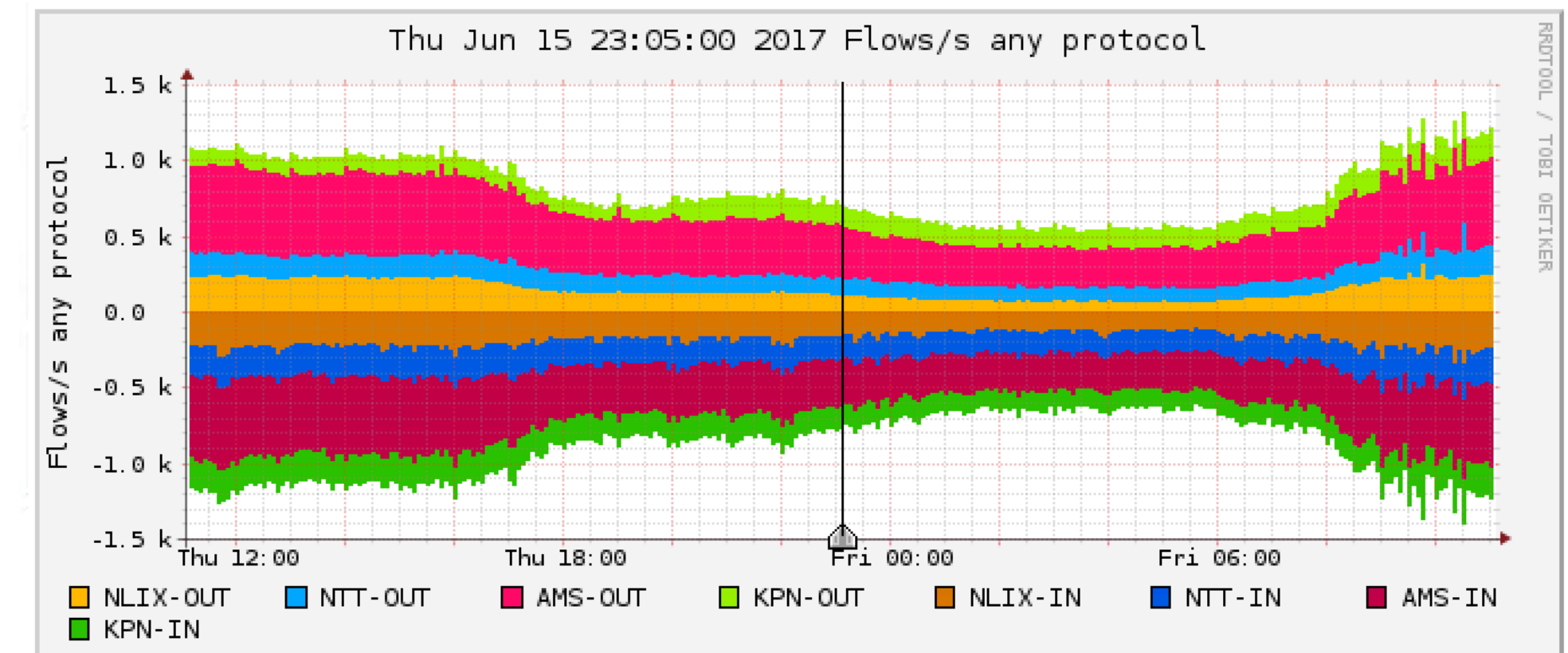
Cheap and Efficient DDoS Traffic Analysis

- Resultaat:
 - TAPHost per POP
 - 4 10Gbps poorten per host - alleen RX aangesloten
 - 4 NICs in OS (linux)
 - Netflow op beide MX80's uit



Cheap and Efficient DDoS Traffic Analysis

- Configuratie
- TAPHost 1
- iptables ipt_NETFLOW
- NFSen
- TAPHost 2
- iptables ipt_NETFLOW
- Fastnetmon + Grafana



Cheap and Efficient DDoS Traffic Analysis

- Ervaring tot op heden:
 - Full table laden in 6 minuten in plaats van 20
 - Fastnetmon werkt goed!
 - Minimale investering
- Nadelen:
 - Schaalbaarheid
 - Aggregatie van data

Cheap and Efficient DDoS Traffic Analysis

Feedback / Vragen ?