1. What is Flow Monitoring?

Flow monitoring offers an aggregated view of network activity.


Flexible NetFlow/IPFIX: allows user selection of flow keys and records.

Future: use flow monitoring in Carrier Ethernet networks?

2. IPFIX at the Ethernet Layer

Network operators are considering deployments of Carrier Ethernet networks.

Monitoring at the Ethernet layer provides an overview of active layer 2 protocols.

Our goal: evaluate the use of IPFIX for Next-Generation Ethernet (NGE) monitoring.

3. Probing Equipment

INVEA-Tech FlowMon Probes support IP flow export using NetFlow v5/v9/IPFIX. A special Ethernet-plugin was developed for exporting Ethernet flows.

Exported fields:

Start time, end time, source MAC address, destination MAC address, EtherType, sVLAN, cVLAN, sPriority, cPriority, header length, payload length, packets, octets

Two FlowMon Probes have been installed in our University's campus network.

4. Case 1: Misconfiguration

DECnet Phase IV traffic was found in our network. It was used in previous years for router configuration, but it was not disabled until now.

5. Case 2: Security

A misbehaving host generated a big amount of ARP traffic, which can cause serious damage to the health of the network.

Normal ARP traffic on campus network:

Erreorous ARP traffic on campus network:

Although most IPv4 campus traffic is generated during working hours, IPv6 flows behave differently:

Many small flows are generated by IPv6, especially during evenings. What will be the effect on probing equipment, when more hosts make use of IPv6?

6. Case 3: Profiling

Ethernet flow monitoring provides new insights into active traffic types in a network.

Besides profiling network activity, it can support network managers in detecting misconfigurations and security issues. Other use cases will be investigated as future work.

7. Conclusions

This work has been supported by SURFnet's 'GigaPort 3' project for Next-Generation Networks.