Hardware-Accelerated Framework for Flow Monitoring of 10Gbit Networks

Vojtěch Krmíček
CESNET, z.s.p.o.
krmicek@liberouter.org

Pavel Čeleda
CESNET, z.s.p.o.
celeda@liberouter.org

Radek Krejčí
CESNET, z.s.p.o.
krejci@liberouter.org

Introduction and Motivation
Monitoring of multi-gigabit networks is a challenging problem due to growing speeds of modern links and huge amount of transferred data.

- Networks are complex and prone to failures and attacks.
- Networks are difficult to understand without monitoring.

Flow Monitoring
IP flow monitoring is an effective way how to supervise high-speed networks. It is based on collecting statistical information about transferred data between IP flow endpoints - source and destination IP addresses, port numbers, protocol and other features like an amount of transferred bytes, packets, TCP flags.

Flow Monitoring Framework
The flow monitoring framework was developed by the JRA2 activity of the GEANT2 project for the purposes of security monitoring. It consists of hardware-accelerated FlowMon probes and open-source NfSen collector. Hardware acceleration provides maximal performance and stability for large networks and backbone links.

FlowMon Probe Features
- Mobile network appliance, no fixed network position.
- Based on Linux, which means unlimited potential for extensions.
- Low system load for unsampled traffic.
- Observes whole network traffic.
- NetFlow v5/9 and IPFIX support.
- NetFlow v9 and IPFIX user templates.
- Simultaneous export to multiple collectors.
- Secure configuration through a web interface via NETCONF over SSH.

FlowMon Probe Hardware
- Support for 2×1 Gb/s or 1×10 Gb/s.
- IPv4, IPv6, VLAN, MPLS support.
- Flow cache for 512 000 flow records.
- Static, random or adaptive sampling.
- Media convertor - SFP, XFP transceivers.

FlowMon Probe Network Connection
The probe has one management and several monitoring ports. The probe can be connected to the monitored network in:

- TAP mode - fiber or copper TAP
- Inline mode - COMBO card built-in TAP
- SPANI mode - router/switch mirror port

FlowMon Probe Remote Configuration
The remote configuration system is based on NETCONF protocol and provides platform independent and user friendly interface to configure the probe. The system contains:

- Web frontend
- NETCONF subsystem
- Configuration daemon

Deployment Results
The following graphs represent the measurement results achieved by FlowMon probe deployed on the edge of a large campus network. The NetFlow data are stored on a dedicated NfSen collector.

NfSen is capable of handling more NetFlow data sources simultaneously and display them in one or more graphs. Other features include:

- Various types of graphs
- Traffic profiles
- Advanced filtering
- Triggers and alerts
- User defined plugins

The presented framework is suitable for research or operational purposes in high-speed networks. The FlowMon probe is well integrated with NfSen collector.

Acknowledgement
This work is supported by the research intent MSM6383917201 and EU FP6 project GEANT2 (contract No. 511082).

References