

NetFlow Principle

The monitoring is based on collecting IP flows. In general, IP flows are sets of packets which share a common property. The most important such properties are the flow's endpoints. The simplest type of flow is a 5-tuple, with all its packets having the same source and destination IP addresses, port numbers and protocol.

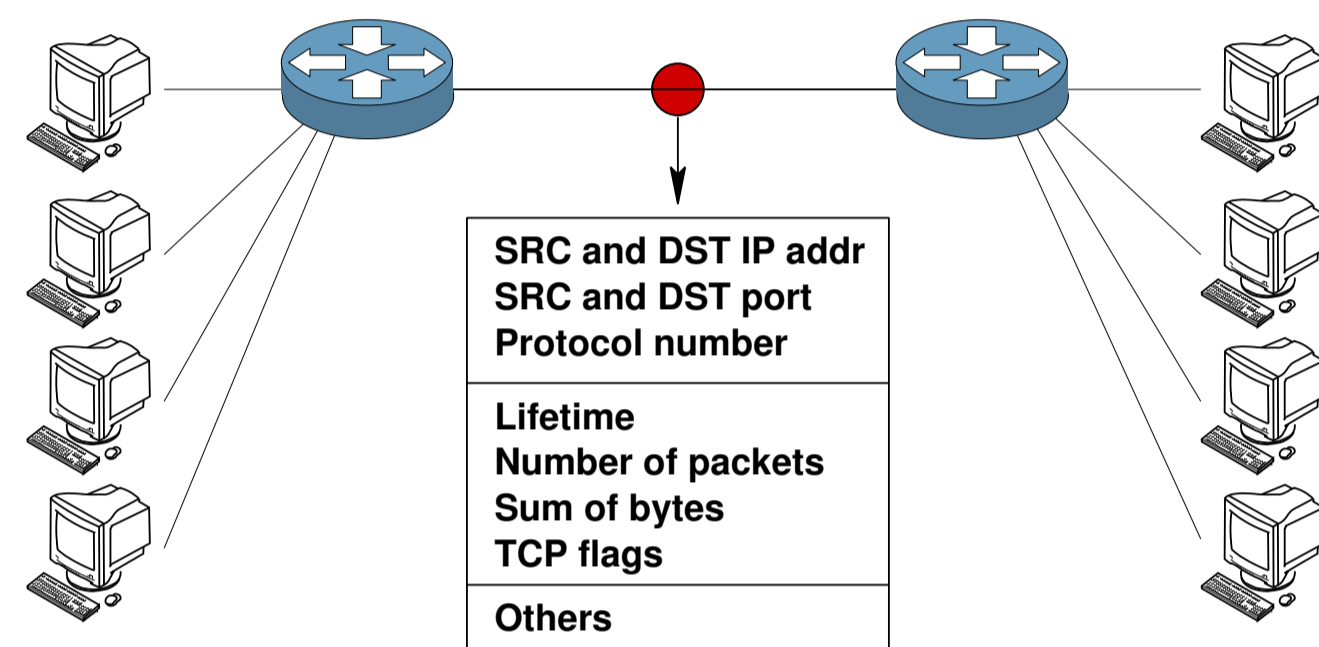


Figure 1: Collecting statistics about endpoints communication

FlowMon Probe

The standalone FlowMon probe [3] introduces new monitoring approaches and provides network statistics about IP flows in NetFlow version 5 and 9 formats.

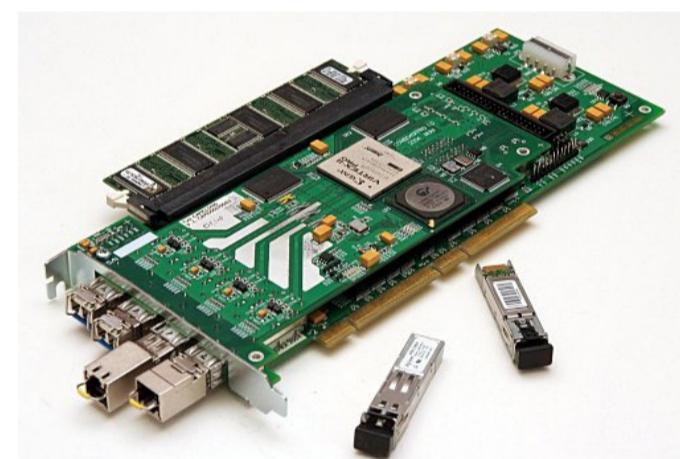


Figure 2: COMBO6X - network acceleration card

The probe is composed of PCI-X acceleration card and personal computer with open-source software. The card is equipped with FPGA chips (reloadable firmware). The card supports either 1 Gbps or 10 Gbps network interfaces.

Advantages

- High performance
- Advanced functions
- Invisible on L2 and L3
- IPv4, IPv6 and MPLS support

The card accelerates the time critical parts of the flow monitoring and aggregation process. The PC is responsible for the export of the collected flow statistics and additional flow record processing.

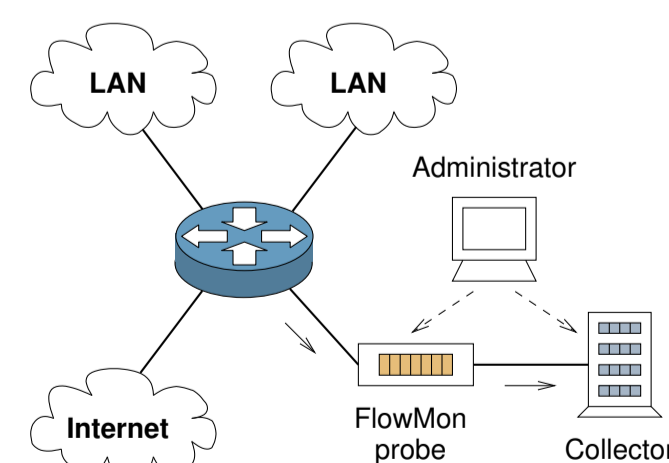


Figure 3: FlowMon probe connected in the network

Firmware

The firmware is composed of several units which are chained into processing pipeline. Incoming packet is assigned with timestamp. Then it is processed at network layer L2 and L3 to verify CRC, extract information about IP addresses, ports, protocol, length of the packet and other fields. The corresponding flow record is found using hashing with consequent look-up. The flow record is updated or created. If the flow expires the flow record is transferred to PC memory.

Features

- Full 2 x 1 Gbps throughput
- Adaptive inactive timeout
- 256 K flow records
- HW IP address anonymization
- Adaptive sampling
- Repeater and splitter

Software

The probe software consists of several parts:

- Linux 2.4 and 2.6 kernel drivers
- User space libraries (libcsflow, libcombo)
- Terminal and web configuration programs
- NetFlow ver. 5/9 flow exporter program

The start-up programs load the firmware into acceleration card and initialize the probe. The kernel driver reads continuously the flow records from hardware and flow exporter encapsulates these records in NetFlow data and sends them to a collector.

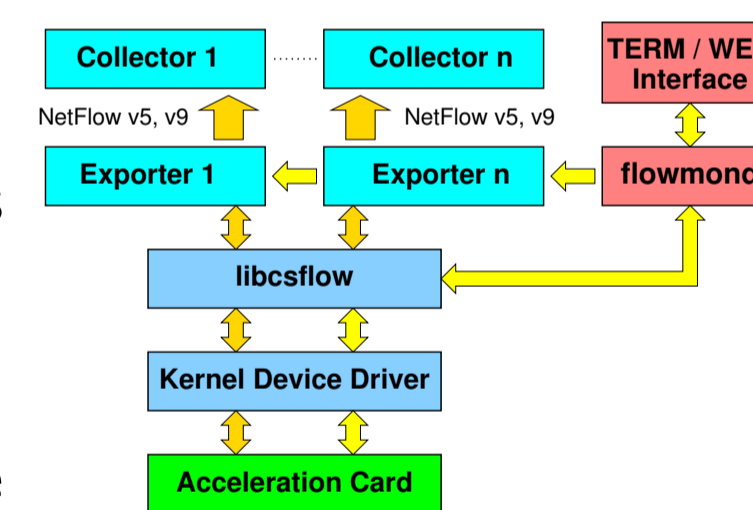


Figure 4: FlowMon probe software layers

Testing

To measure the performance of the network devices we use the Spirent AX/4000 broadband test system.

The tests provided estimates of one-way throughput of the NetFlow probes on Ethernet at a rate of a gigabit per second according to RFC 1944.

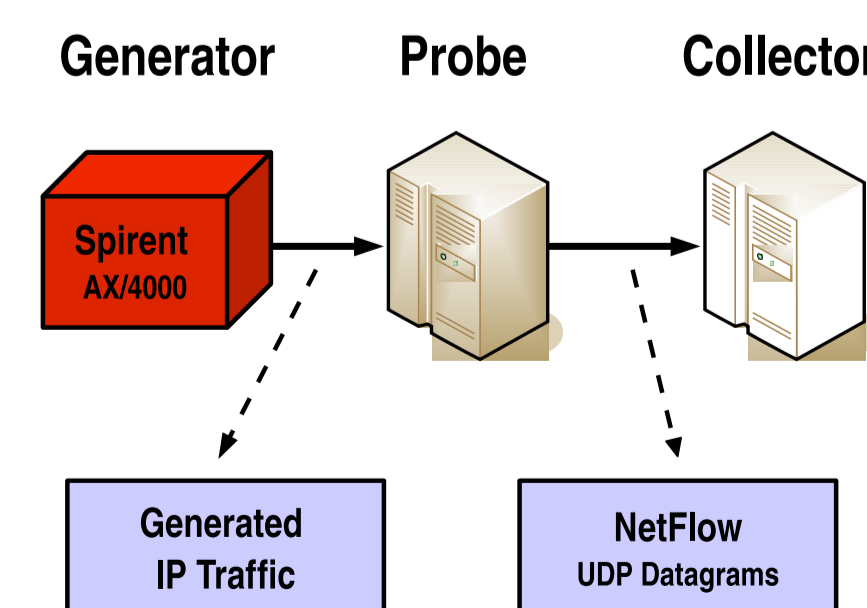


Figure 5: Connection of devices during test

The results in Fig. 6 indicate that the FlowMon probe is able to process 1 Gbps traffic at line rate without any packet losses, regardless of the packet size. In comparison, the nProbe software [1] suffers from massive losses for packet sizes below 400 B.

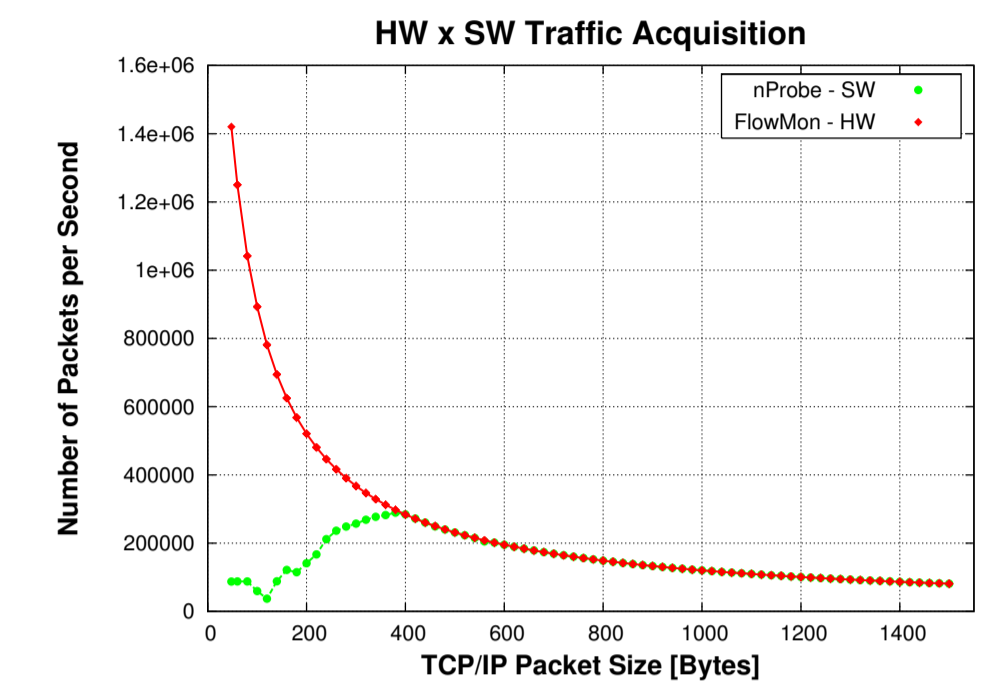


Figure 6: NetFlow probes comparison

Deployment

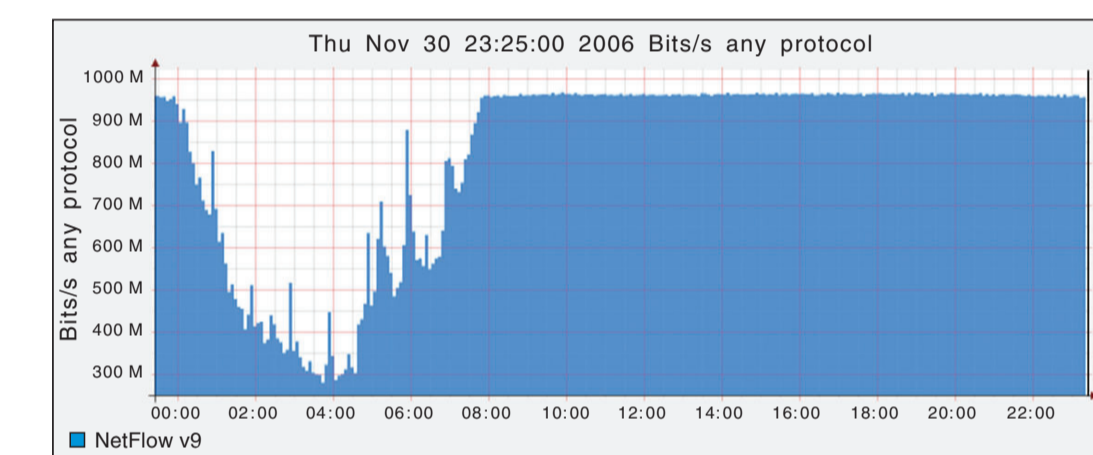


Figure 7: Statistics from NfSen collector

NRENs using FlowMon

- SWITCH (Switzerland)
- SURFnet (Netherlands)
- CESNET (Czech Republic)
- GRNET (Greece)
- Bulgarian Academy of Sciences

To develop, test and deploy FlowMon probes we use NfSen [2] collector, a graphical web based front end for the NFDUMP netflow tools. According to our practical experiences FlowMon can collaborate with NfSen without any problems.

Conclusion

The presented FlowMon probe is robust solution for all administrators who are interested in their flow data. The probe is able to provide data in several formats with optional sampling, filtering and anonymization. Currently we focus on development of 10 Gbps solution and on implementation of another export format IPFIX.

Acknowledgment

This work is supported by the research intent MSM6383917201 and EU FP6 project GN2 (contract No. 511082).

References

- [1] Luca Deri. nProbe an extensible Netflow v5/v9/IPFIX GPL probe for IPv4/v6. <http://www.ntop.org/nProbe.html>.
- [2] Peter Haag. NfSen - NetFlow Sensor. <http://nfsen.sf.net>.
- [3] Liberouter Project. Hardware Accelerated FlowMon Probe. <http://www.liberouter.org/flowmon>.