

Using IPFIX for NG Ethernet Monitoring: First Results

Rick Hofstede

Outline

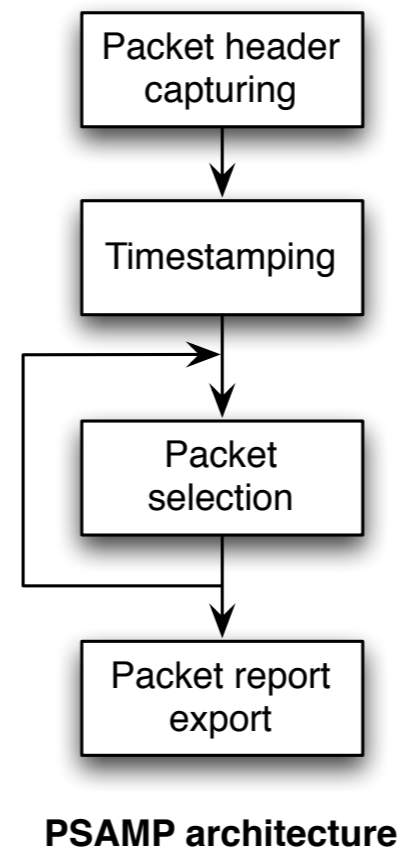
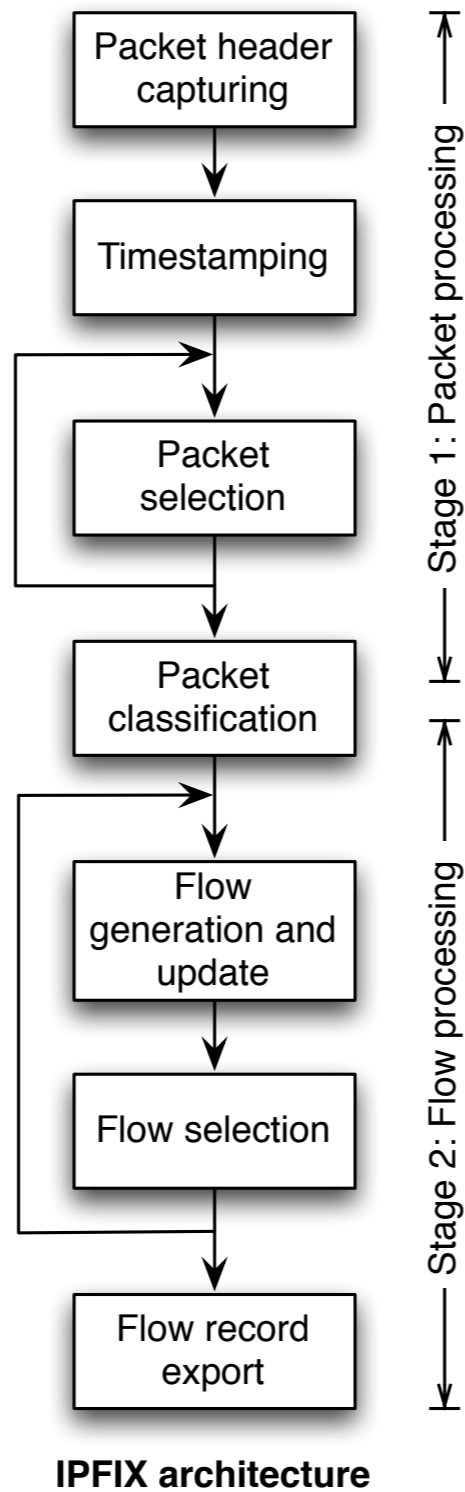
- Introduction
- NetFlow, IPFIX, PSAMP
- IPFIX for NGE monitoring
- INVEA-Tech FlowMon Probes
- Conclusion

Introduction

- University of Twente is involved in SURFnet RoN for the following topics:
 1. Report on state-of-the-art for Next-Generation Ethernet management (completed)
 2. Research on bandwidth measurements and allocation, using flow data (ongoing)
 3. Using IPFIX for Next-Generation Ethernet (NGE) monitoring (ongoing, topic of today)

NetFlow overview

- Provides a summary of network activity on the IP layer
- Helps to understand sources / destinations of traffic, applications generating traffic, etc.
- Overcomes scalability problems of packet-level capture
- NetFlow v5: fixed data structures, IPv4
- NetFlow v9: templates, IPv6
- Flexible NetFlow/IPFIX: allows user selection of flow keys and records



Source: RFC 5476

IPFIX architecture

IPFIX for NGE monitoring

- IPFIX Information Elements (IEs) have been defined by IANA
- IEs for (NG) Ethernet:

sourceMacAddress	destinationMacAddress	ethernetHeaderLength
dot1qVlanId	dot1qCustomerVlanId	ethernetPayloadLength
dot1qPriority	dot1qCustomerPriority	ethernetType
metroEvcID	metroEvcType	

- IPFIX is flexible enough to cope with different formats
- Our goal: evaluate the use of IPFIX for NGE flow monitoring

INVEA-Tech

FlowMon Probes

- Probes support IP flow export using NetFlow v5/v9/IPFIX
- INVEA-Tech developed a special Ethernet-plugin
 - Allows Ethernet flow export
 - Expired flows (by active or inactive timeouts) are exported by using NetFlow v9 (for early deployment)
 - Native Ethernet flow export to be supported in future
- New plugin: IPFIX 'immediate' flow export (RFC 5470)

INVEA-Tech

FlowMon Probes: hands-on

- Two INVEA-Tech FlowMon probes have been purchased (supported by SURFnet)
 1. FlowMon Probe 10000 SFP+ (1x 10GbE SFP+)
 2. FlowMon Probe 2000 (2x 1GbE copper)
- Both probes have been installed in the UT (non-NGE) network, in order to
 - Get experience
 - Understand their behavior
 - Test their stability

INVEA-Tech

FlowMon Probes: hands-on

- Impressions:
 - Easy to install
 - Great administration interface
 - Promising performance
 - Integrated solution: internal NetFlow collector available
 - Excellent customer support!

INVEA-Tech

FlowMon Probes: hands-on

- Connecting probes to SPAN/mirror-ports can lead to artifacts
 - J. Zhang and A. Moore - *Traffic Trace Artifacts due to Monitoring Via Port Mirroring*
 - Optical splitters will be needed in order to avoid monitoring artifacts
- Ethernet-plugin is still in 'fine-tuning' phase, in close cooperation with INVEA-Tech

INVEA-Tech

FlowMon Probes: performance

- Day-to-day traffic in UT network (FP10000):

Flows	Packets	Octets
7.0 k/s	615 k/s	4.5 Gbps

- A UT host was targeted by a DDoS attack last month
 - 1,500 attackers, 370 mln. flows, 22 GB, 13 minutes
 - UT core router (Cisco 6509) had a flow record loss of 90%
 - INVEA-Tech FP10000 probe was able to record all the flows

Conclusions

- INVEA-Tech's FlowMon Probe is a promising platform for flow monitoring
- Device performance is promising!
- Importance of having a dedicated flow collection device has been demonstrated
- Devices are in 'fine-tuning' phase now, although NGE monitoring cannot be tested yet
- Plan is to move the FPI0000 to SARA in Q2 2011

Thanks for your attention!

Rick Hofstede

r.j.hofstede@student.utwente.nl

INVEA-Tech

FlowMon Probes

- Ethernet-plugin uses the following IE mappings:

Key fields		Non-Key fields	
sourceMacAddress	→	srcIPv6	ethernetHeaderLength → srcAS
destinationMacAddress	→	dstIPv6	ethernetPayloadLength → dstAS
dot1qVlanId	→	srcPort	dot1qPriority → ToS
ethernetType	→	dstPort	dot1qCustomerPriority → TCP flags
0 (unused)	→	I3.proto	dot1qCustomerVlanId → port.out
0 (unused)	→	I4.proto	First Ethernet frame seen → flow start
FP monitoring port ID	→	port.in	Last Ethernet frame seen → flow end
			frames
			bytes