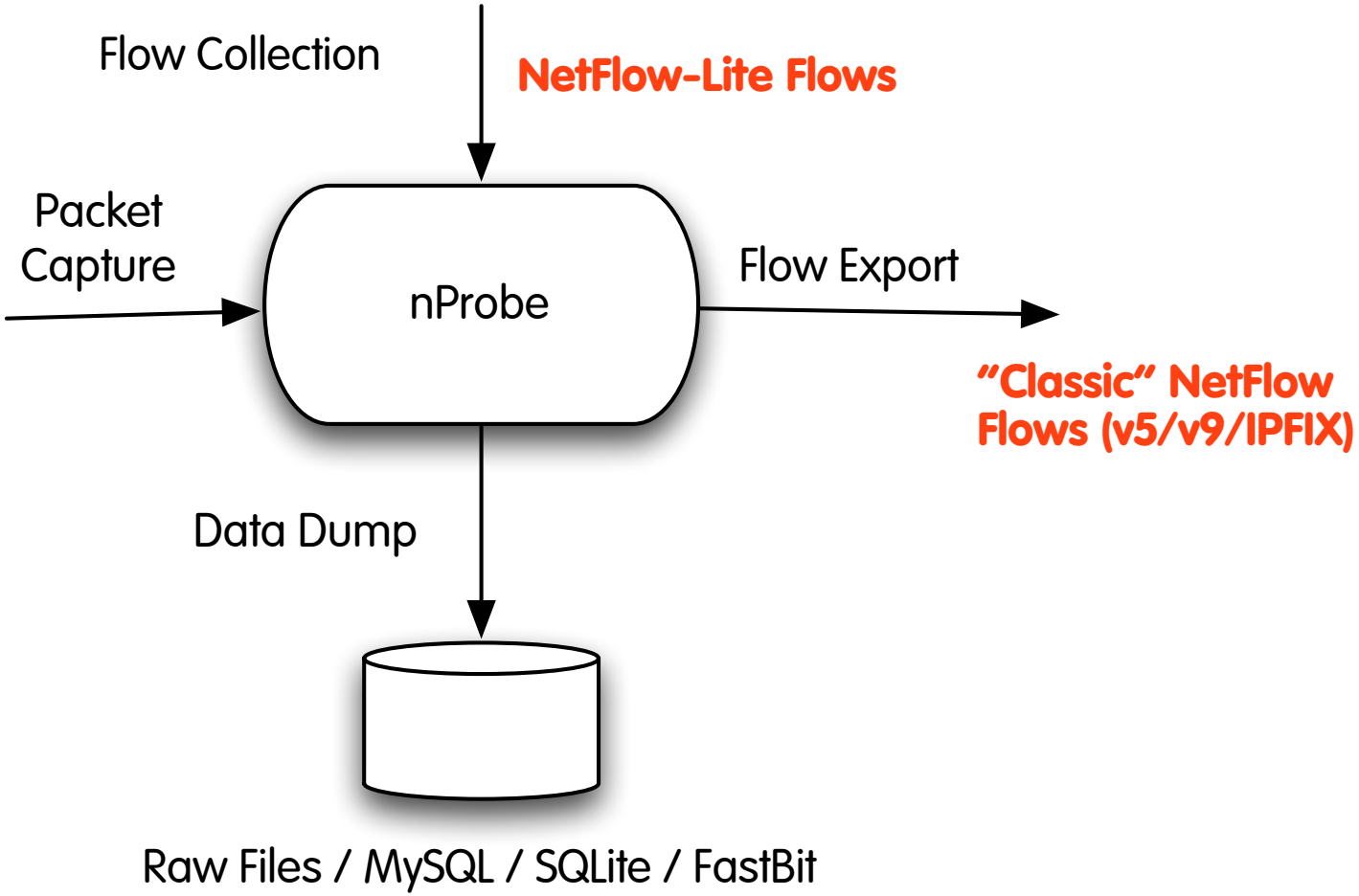
Using nProbe as NetFlow-Lite Aggregator

Luca Deri <deri@ntop.org>

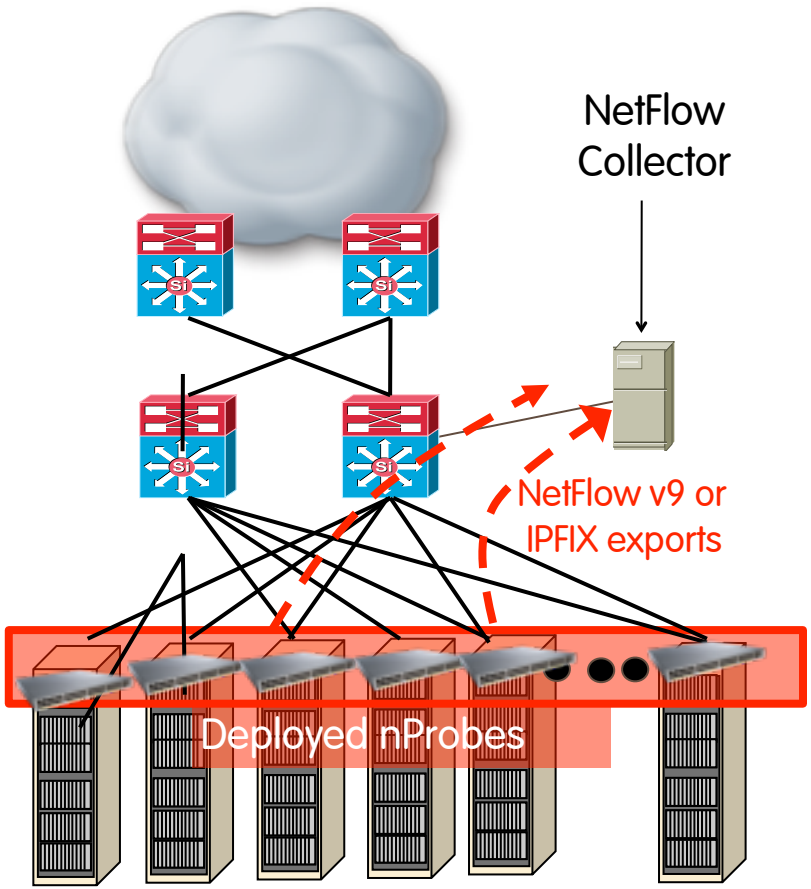
Problem Statement

- NetFlow-Lite brings visibility to switched networks.
- NetFlow-Lite are exports in v9/IPFIX format and contain packets sections.
- Legacy NetFlow collectors need additional support to understand and analyze NetFlow-lite flows.

What is nProbe ?



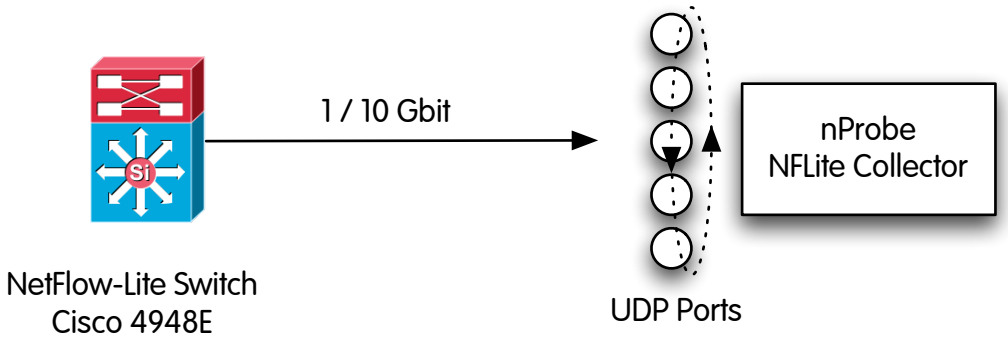
Typical nProbe Deployment



- Insert nProbe/nBox on spanned or mirrored switch ports.
- Typically watch uplink traffic.

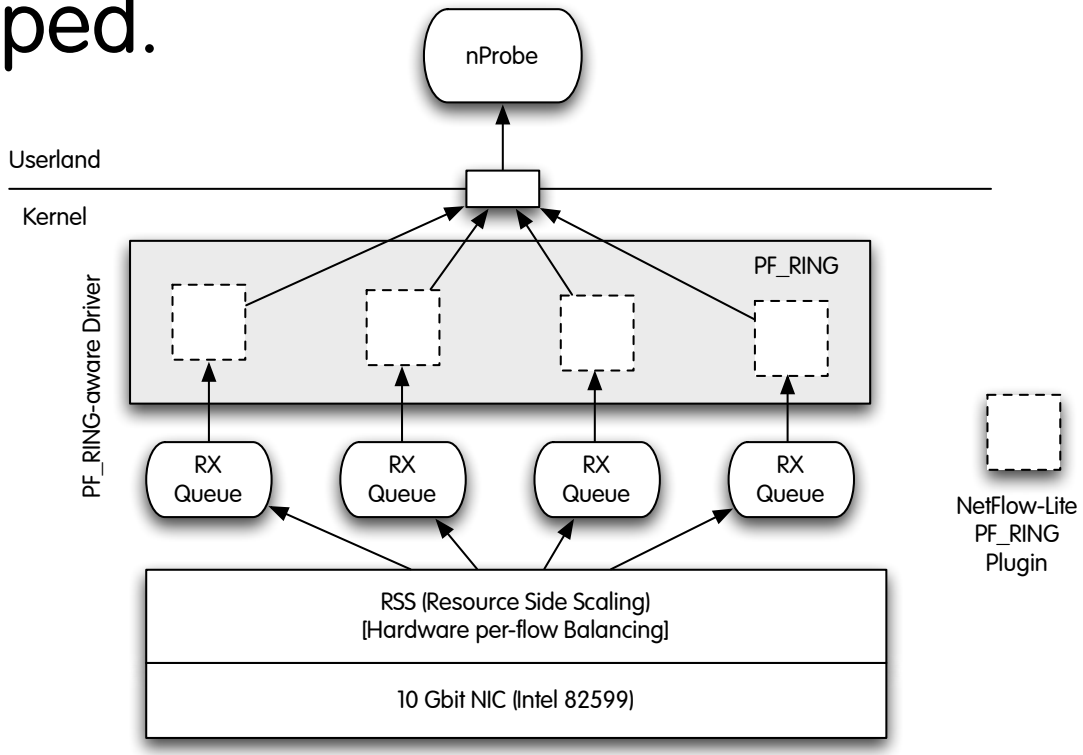
NetFlow-Lite Support in nProbe [1/2]

- nProbe collects NetFlow-Lite Flows over IPv4/IPv6 UDP.
- 4948E balances flows on multiple UDP destination ports



NetFlow-Lite Support in nProbe [2/2]

- For collecting large number of NetFlow-Lite Flows a kernel plugin (Linux only) has been developed.



Final Remarks

- nProbe supports NetFlow-Lite since version 6.5.
- It is available for both Windows and Unix.
- Typical NetFlow lite conversion speed range from 250k to 1M flows/sec (Linux only using the kernel plugin).
- nProbe supports transparent IP address spoofing for impersonating the 4948E switch.