Adding a PIB to the MIB

Configuration and integration of 'advanced monitoring'

Steven Van den Berghe

1st Scampi Workshop

Amsterdam - 27 January 03

What I think I'll be talking about

- Demand for measurements is growing:
  - complexity is growing
  - diversity is growing
- Options:
  - one device for every task
  - one part of a device for every task
  - flexible and powerful usage
- Requirements:
  - unify measurement representation, configuration
  - unify usage
- No religious war

What to measure

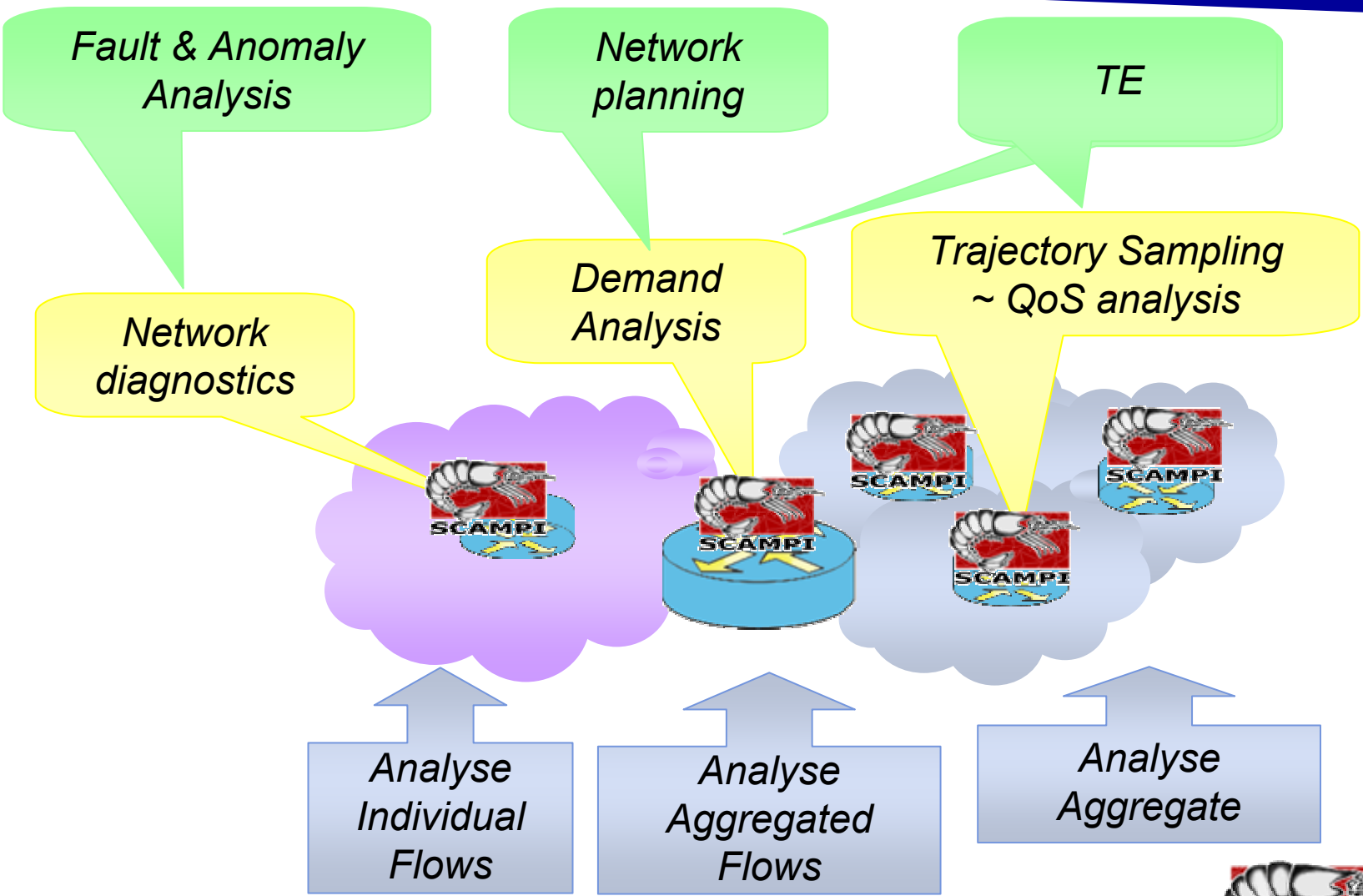
Functionality: observation => diagnostic monitoring

- Basic monitoring functionality available for ages:
  - *ping*: calculate round-trip delay and loss by injecting packets in a network
  - *SNMP/MIBs/RMoN*: add counters etc. to network elements to passively monitor what passes
  - Snort, Ntop: Diagnostics/stats on ‘streams’

Functionality: reaction => operational measurement

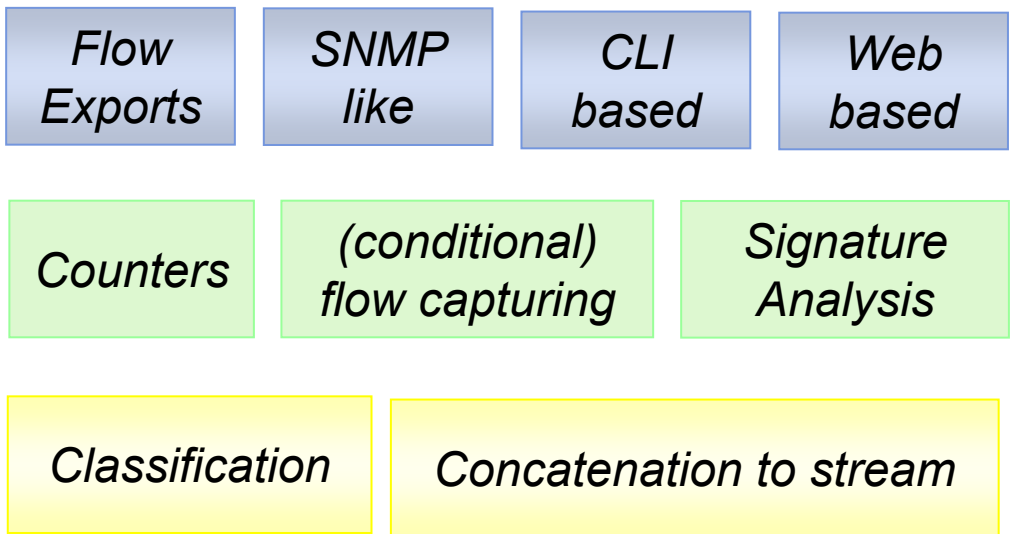
- One step beyond: automated reaction to monitoring results
  - Policy based management: if <event> then <action>

Unification?



Integrating Monitoring In the Device

- Network Monitoring Device
  - configuration
  - reporting
- New ‘type’ of measurements
  - complete new top-down part in device



Requirements

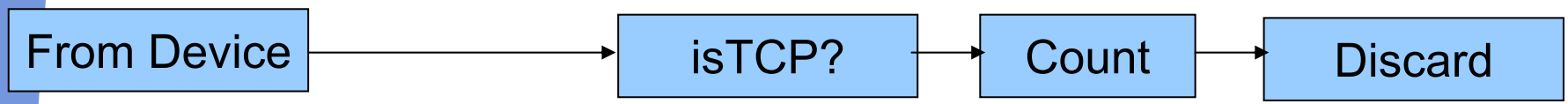
What I Have

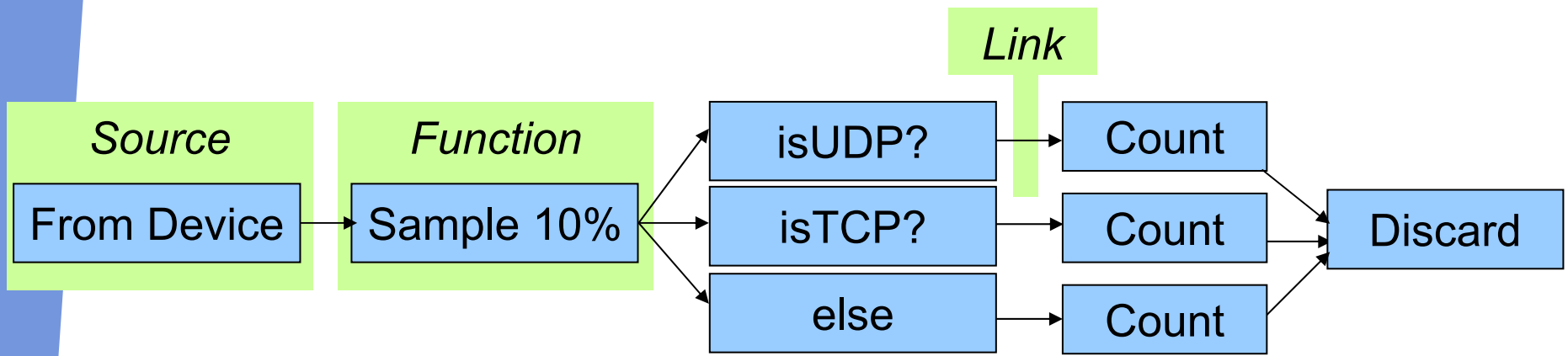
- Application Stats
- Intrusion Detection
- Packet Sampling

What I Want to Have

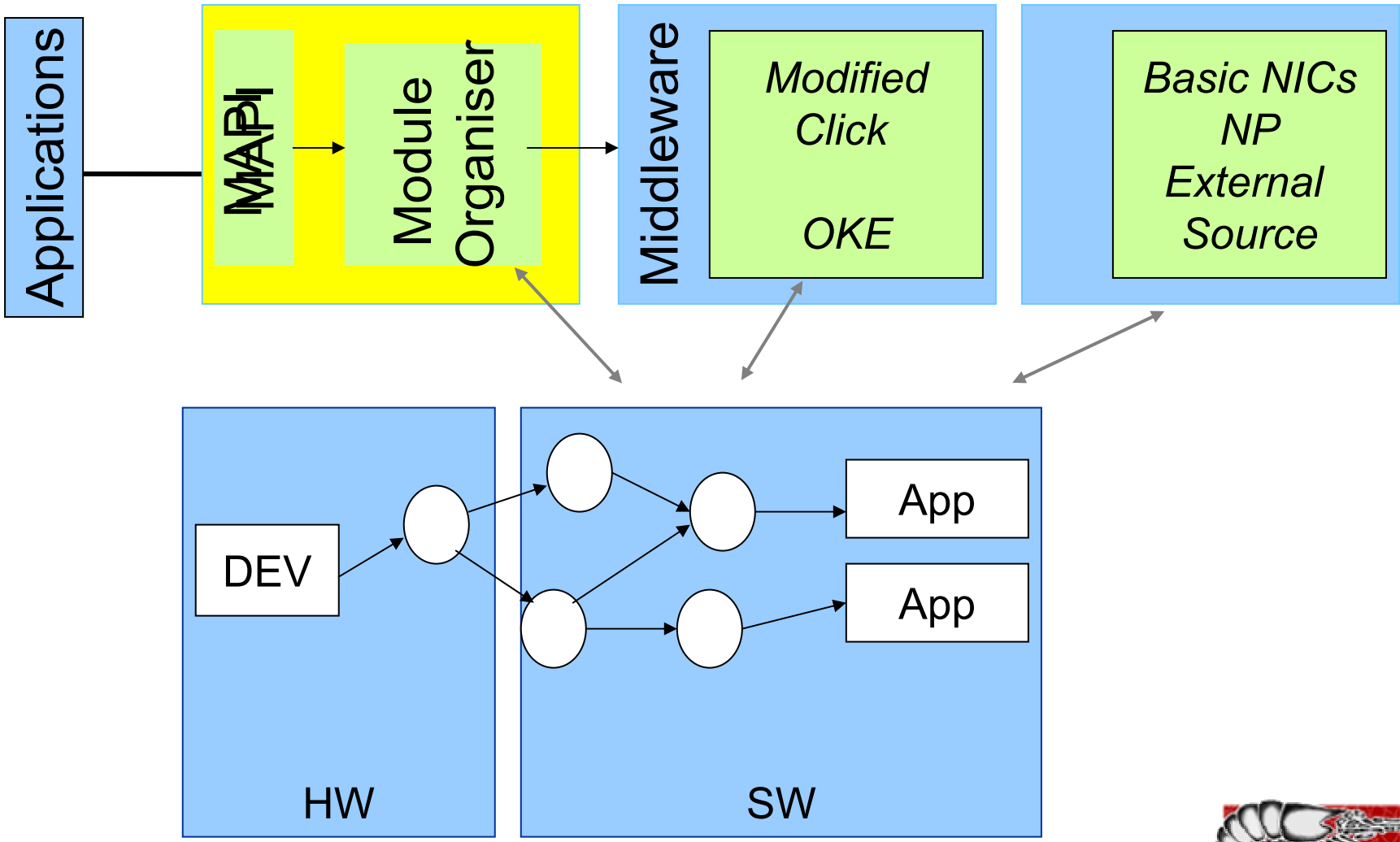
- A Single Way to
  - configure
  - report
  - act upon reports

Big job & Small Blocks

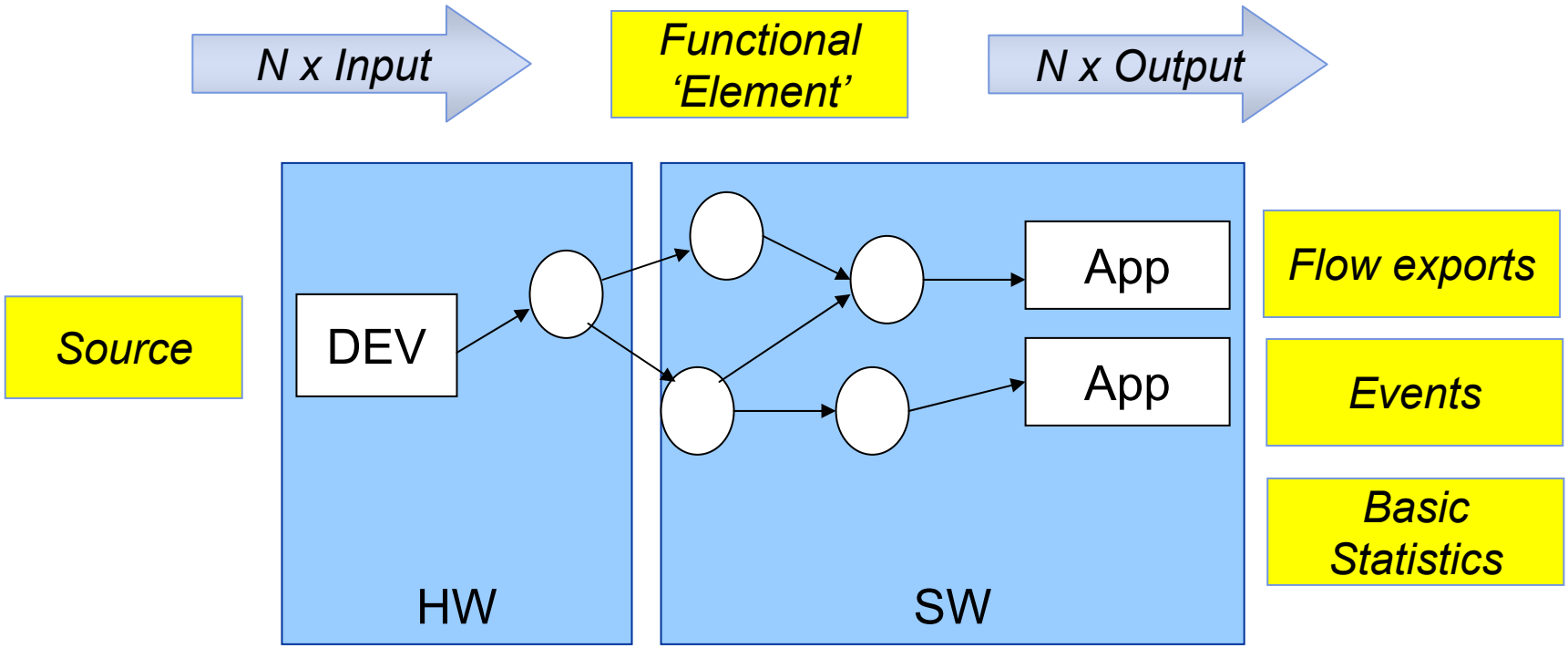




Unified Access: SCAMPI



Functionality Summary



- Build powerful monitoring constructs from simple elements
  - classifier, sampling (incl. Hashing), flow export
  - optimize intermediate graph
- object-oriented better suited than functional ?

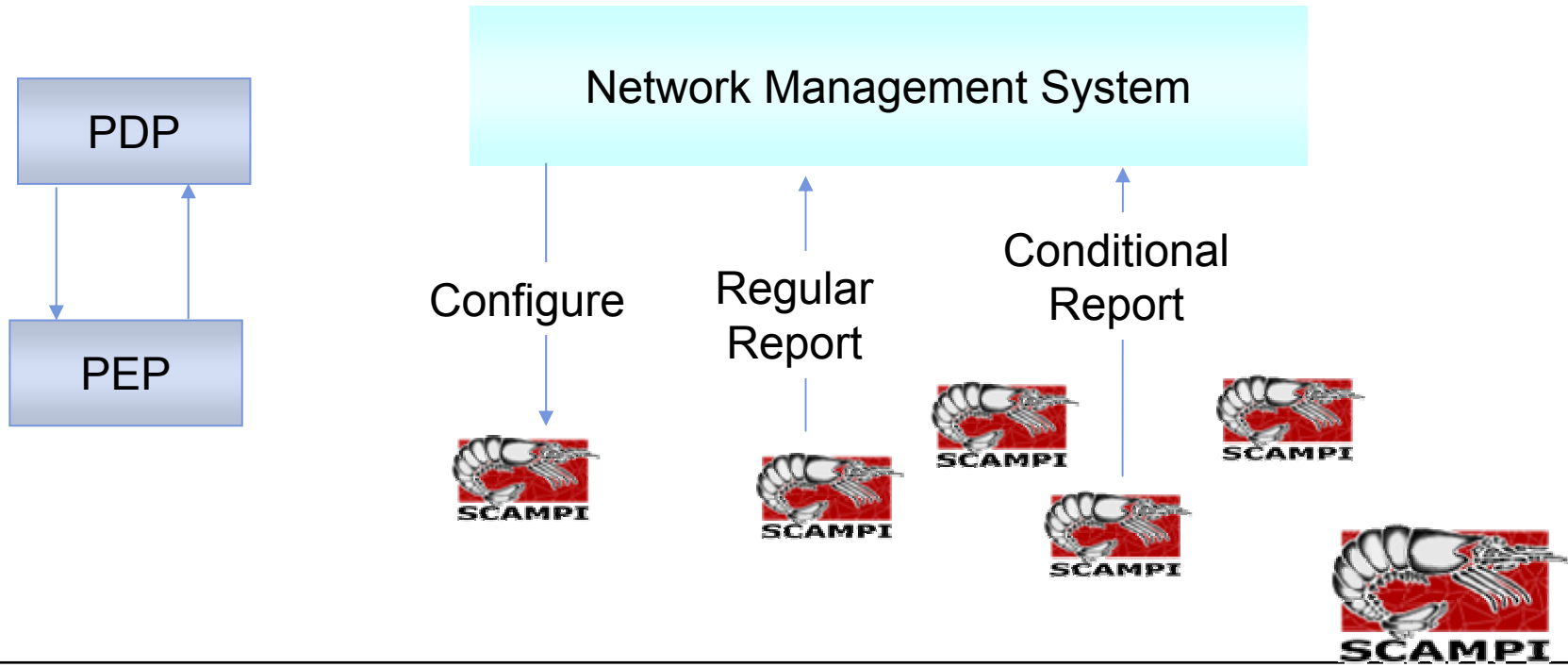
Case: TE

- Multi-Service Traffic Engineering (TE): accommodate a maximum of multi-service traffic requests by optimally using the available network resources
  - One new “keyword”: Service monitoring
  - + “Old” functionality: e.g. driving GUIs for management (e.g. for failure detection and human network analysis etc.)
- Requires
  - Demand analysis (passive, sampling)
  - QoS-measurements (active, passive, sampling)
  - Network status (passive)
- Observation + automated operation

- `draft-ietf-tewg-measure`

ietf-rap-feedback

- Given provisioned ‘objects’ part of configuration
- Check stats and report
  - regularly
  - on change
  - on threshold crossing

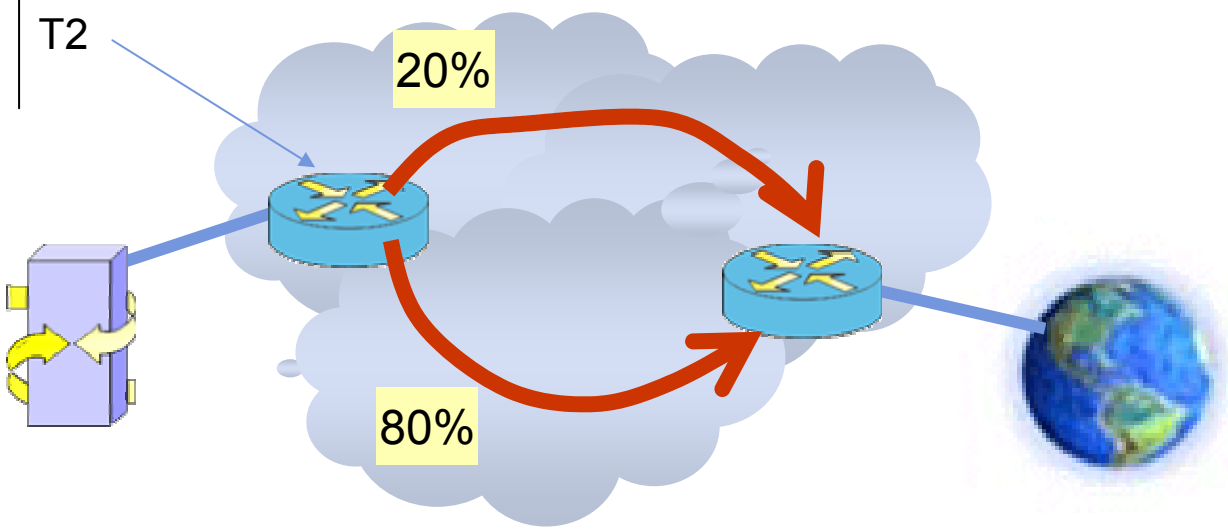


Tunnel Management

Set-up monitoring of subnet B — *demand > 20%*

On Alarm — *Re-map and re-configure*

Subnet A	T1
Subnet B	T2



Thank You

- Any (remaining) questions ?

  - steven.vandenberghe@intec.rug.ac.be

  - http://www.ist-scampi.org

What I think I'll be talking about

- Demand for measurements is growing:
  - complexity is growing
  - diversity is growing
- Requirements:
  - unify measurement representation, configuration
  - unify usage
- Implemention using a 'basic-building-blocks' method vs. a table-based method.