Passive monitoring in GEANT3 network

Aleš Friedl, Sven Ubik
CESNET

NA3 Monitoring Workshop, Belgrade, 21-22 October 2009

Monitoring approaches

Active monitoring:

- send and receive test packets

Passive monitoring:

- capture and analyze real traffic

Network infrastructure monitoring:

- collect information from network equipment

Passive monitoring

Advantages:

- non-intrusive
- provides information about real traffic, e.g.:
  - load dynamics
  - protocols and applications used in the network
  - anomalies, attacks
  - real packet loss (difficult to test actively)

Difficulties:

- processing large volumes of traffic
- high cost of monitoring cards

Pilot deployment in GN2

Partners

- ACAD (BG), CESNET (CZ), PIONIER (PL), SWITCH (CH)

GEANT2-NREN border links

- 3x 10G, 1x 1G

Monitoring applications

- ABW, Packetloss, Burst, Tbwtools, *Perfmon+Servmon*

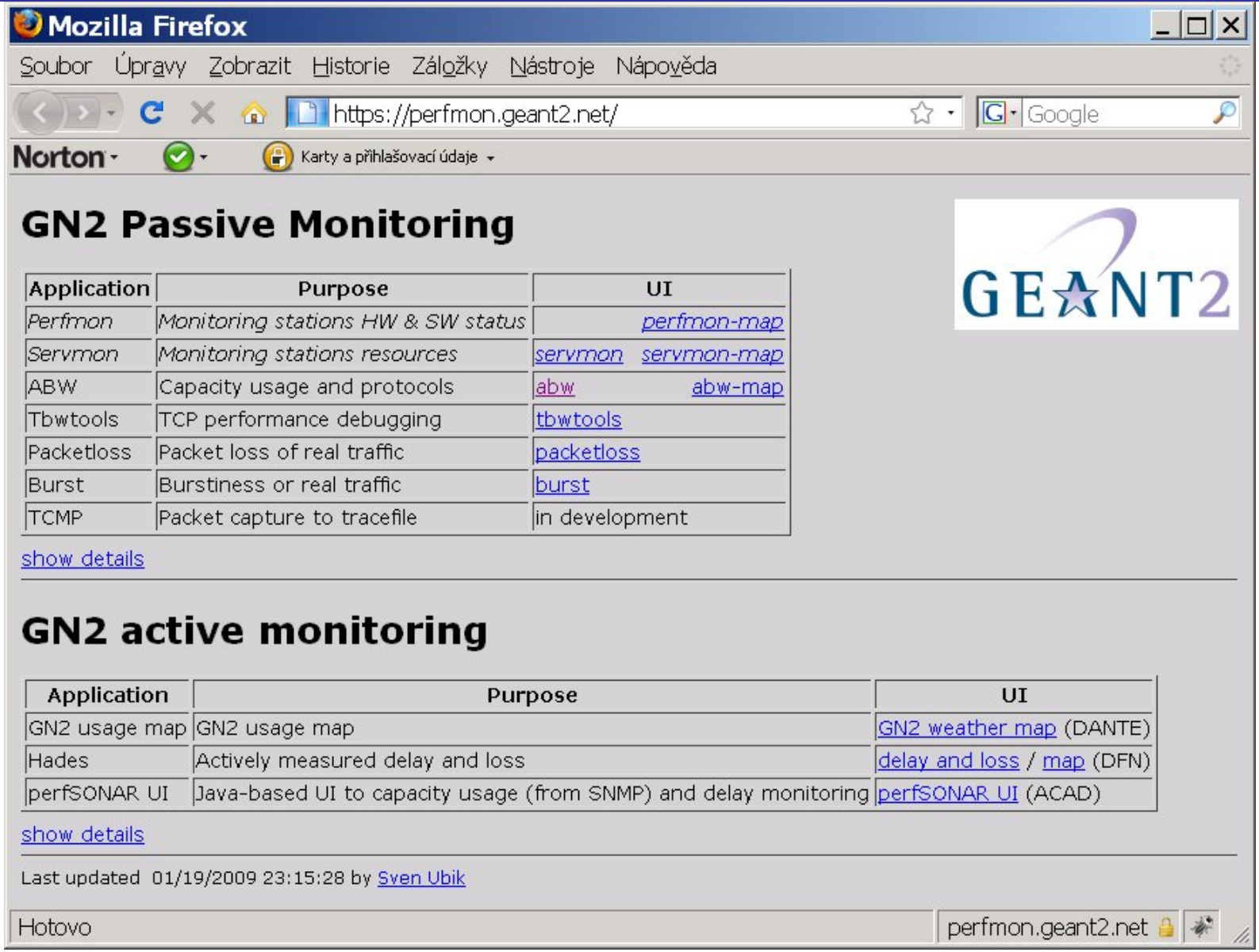
Central user interface

htpps://perfmon.geant2.net

Username and password:

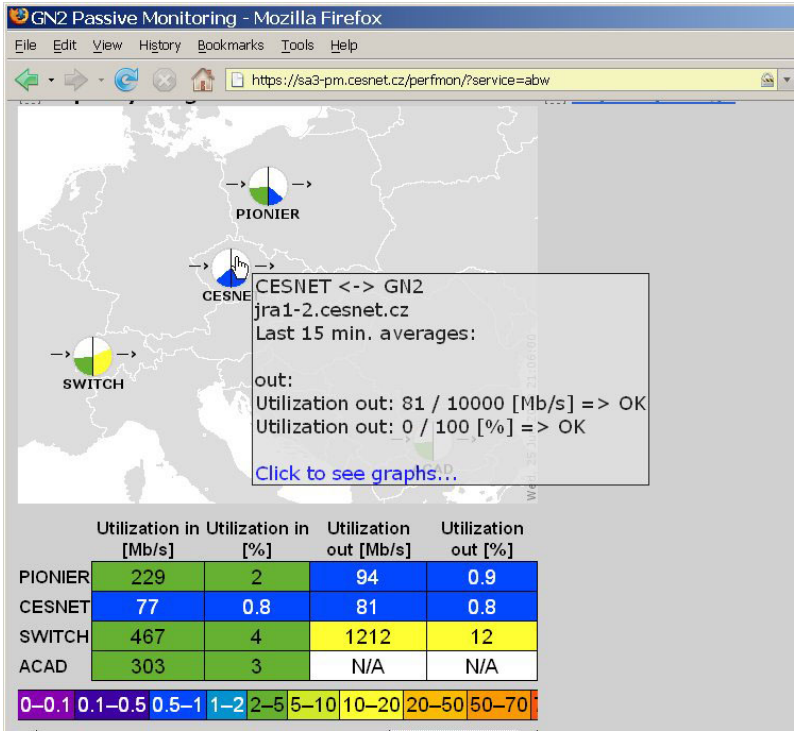
http://wiki.geant2.net/bin/view/JRA1/Jra1WorkingArea

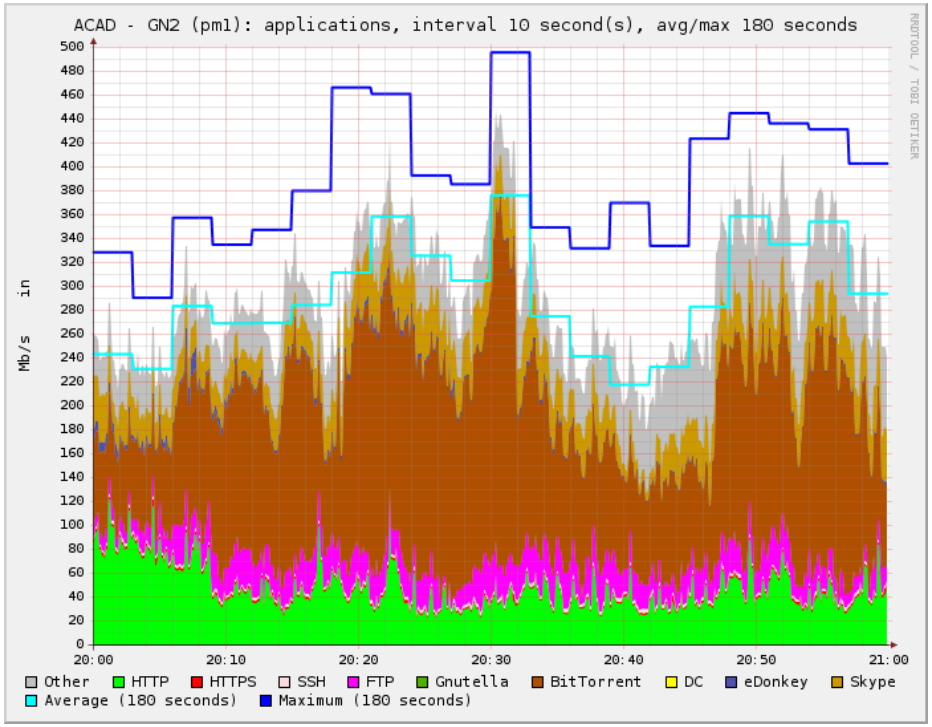
Web access to monitoring



ABW

- traffic composition from protocols and applications
- short-term load peaks
- payload pattern searching => gradually decreasing reliability
- new lightweight detection library being developed in JRA2 GN3





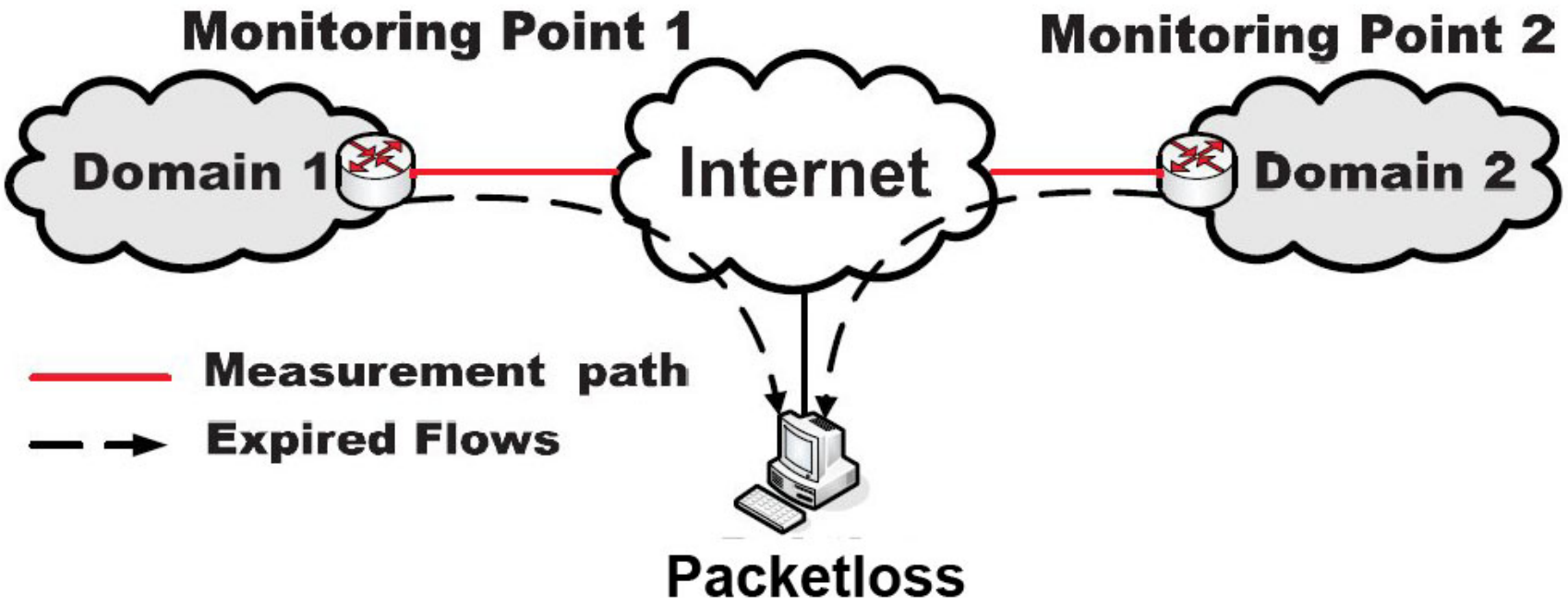
Packet loss monitoring

Problem illustration:

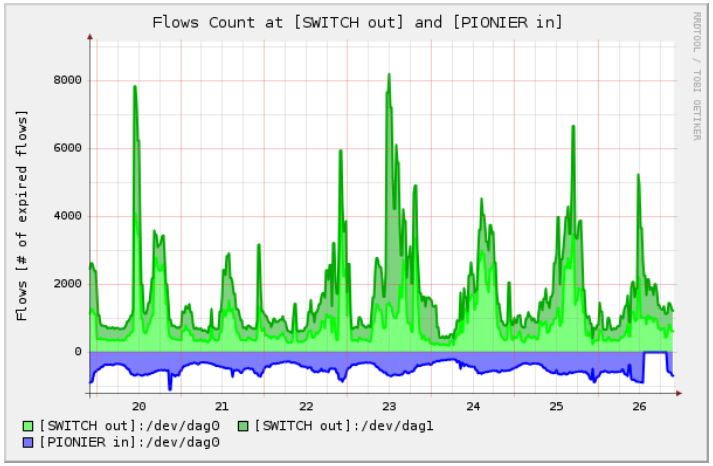
- Packet loss ~10^{-5} can affect TCP and applications seriously
- If we send 100 test packets / second (quite a lot), it takes ~1000 seconds to detect such loss!
- How to measure full-mesh (scalability)?
- What applications and what users were affected by loss?
- How to measure loss bursts?

Realistic packet loss measurements with identification of affected applications and users can only by done by analysis of real traffic by passive monitoring.

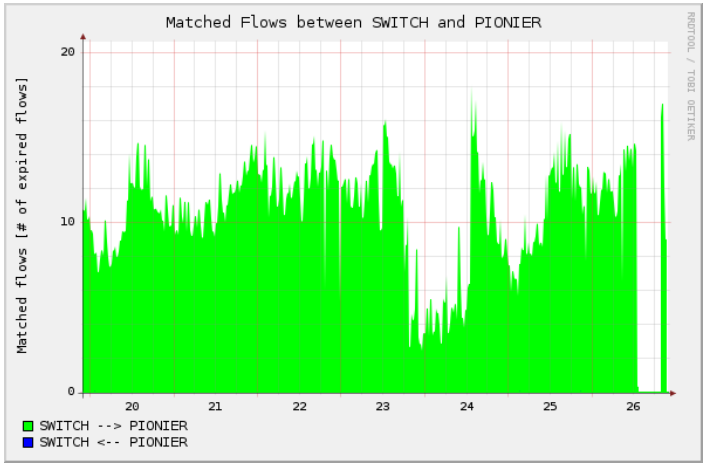
Packetloss - idea



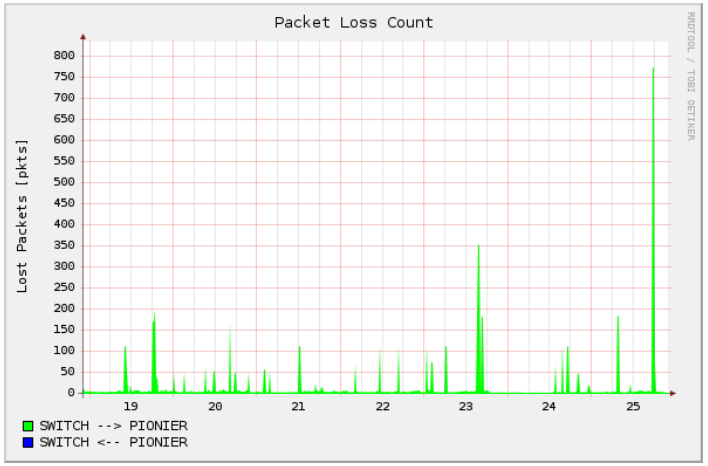
Packetloss - results



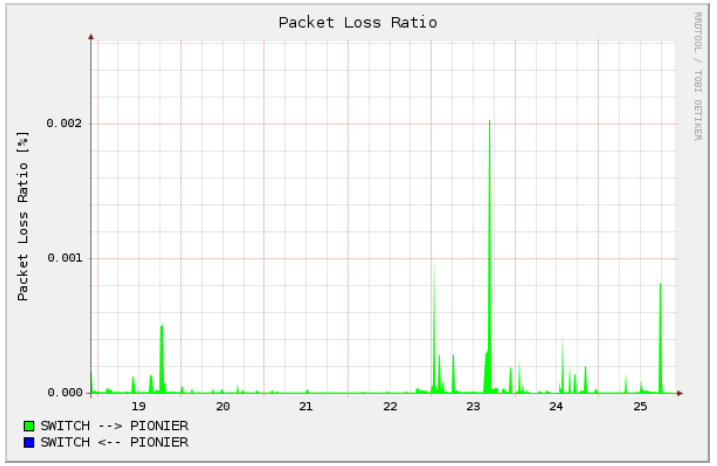
Flow count (1 station)



Matched flows (2 stations)



Lost packets



Loss rate

Extension in GN3

Research (JRA2):

- Lightweight application protocol detection based on machine learning and protocol behaviour patterns
- Packetloss running over regular Netflow

Development and deployment (SA2):

- More GN3-NREN points
- Higher stability
- “Business case” submitted to GN3 management

http://wiki.geant.net/pub/SA2/PassiveMonitoring/GN3_SA2_T3_pm.doc

User groups

We aim at the following user groups, in aproximate order of priority:

- PERT
- Networking researchers
- NOC
- Network planners
- General public

Questionnaire

- questions:
  - preference of network characteristics (detection of known protocols, blind classification, real packet loss, geographical characteristics)
  - user interface preferences
  - purposes of monitoring
- mark options as 1 to 5 (5=very useful, 1=least useful)
- responses obtained from: CARNET, LITNET, NORDUNET, RESTENA, ROEDUNET, SIGMANET

Summary of received responses

- All proposed applications were considered as very interesting by prospective users
- Network research as purpose is indicated with various importance (from lower to higher), whereas other purposes of use were indicated as highly important, particularly NOC
- Web-based user interface is strongly preferred over perfSONAR UI

Technology

- Monitoring cards are necessary for approx. > 300 Mb/s of live traffic
- Regular NICs have good throughput for large packets (for file transfers) but low throughput for small packets (frequently present in traffic) they consume a lot of CPU just for packet copying and cannot utilize multi-core CPUs
- Monitoring cards can copy line-rate traffic (10 Gb/s) zero-loss, zero CPU load, with splitting into multiple buffers to be served by multi-core CPUs
- We have practical experience with DAG and Napatech (both 1 Gb/s and 10 Gb/s)
- Cost per 10 Gb/s port approx. 8000 Eur (2-port Napatech card)

Technology (cont.)

We are investigating if standard Netflow can be used for proposed applications

- Current application-detection library, Packetloss as well as new lightweight application-detection currently need extra attributes (not in standard Netflow)

Roadmap

- Software (development, testing, integration)
  - 9/2009 – 8/2010
- Transition to service
  - 1/2010 – 8/2010
- Support setup (helpdesk, Wiki pages)
  - 4/2010 - 6/2010

Assuming task will be approved by end of November 2009

Thank you for your attention!