

Stager

TF-NGN, Lisboa
Olav Kvittem

30th September 2004

Stager

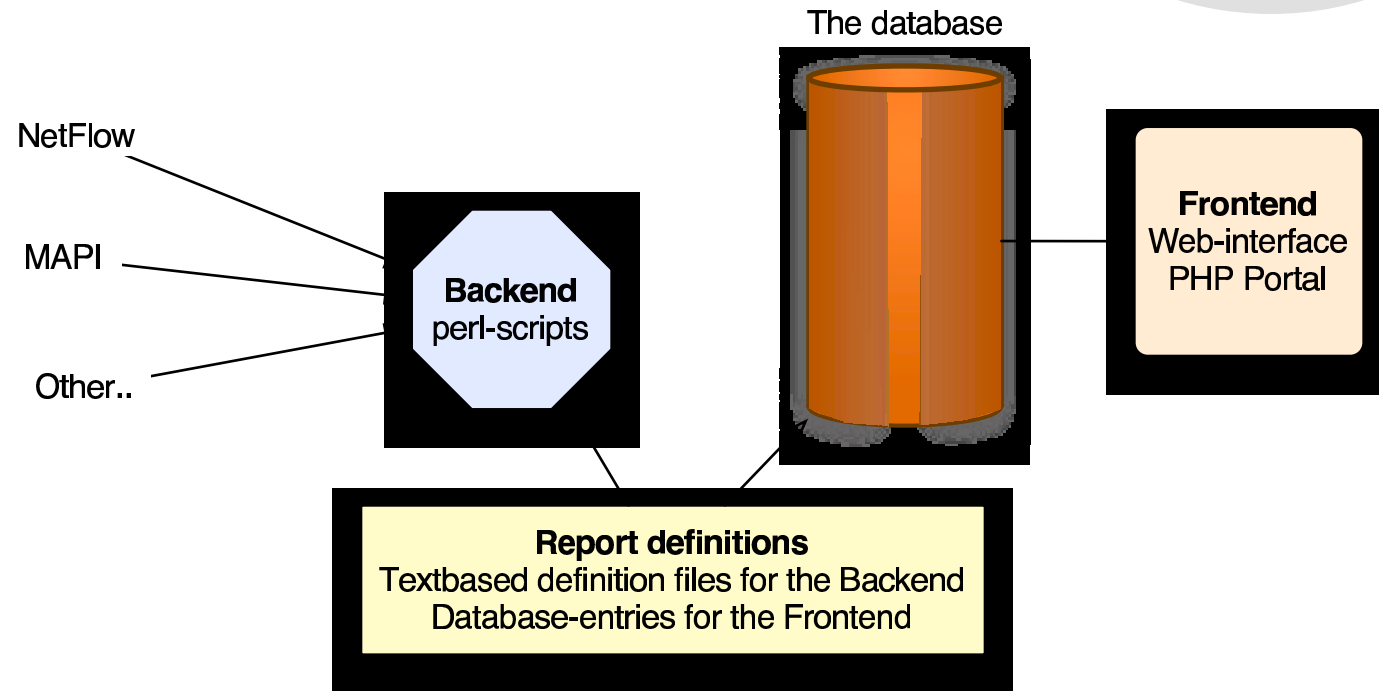
- Statistical Accumulating Graphing Extensible Reporting
- Collect and and aggregate in Postgresql
- Statistical analysis, standard deviation, distribution
- Comprehensive configurable reporting and graphing
- Open for threshold monitoring and anomaly detection by SQL
- Application made for Scampi

Scampi

Scampi - a EU-project with about 10 participants to develop a free and low cost

- high speed passive measurement platform(10Gbps)
- a 10Gbps passive monitoring card
- API in C - modular functions - filtering and statistics
- netflow analysis module IPv4/v6 netflow v5/v9 from ntop (Luca Deri)
- adapted “standard” open software (tcpdump, flow-tools)

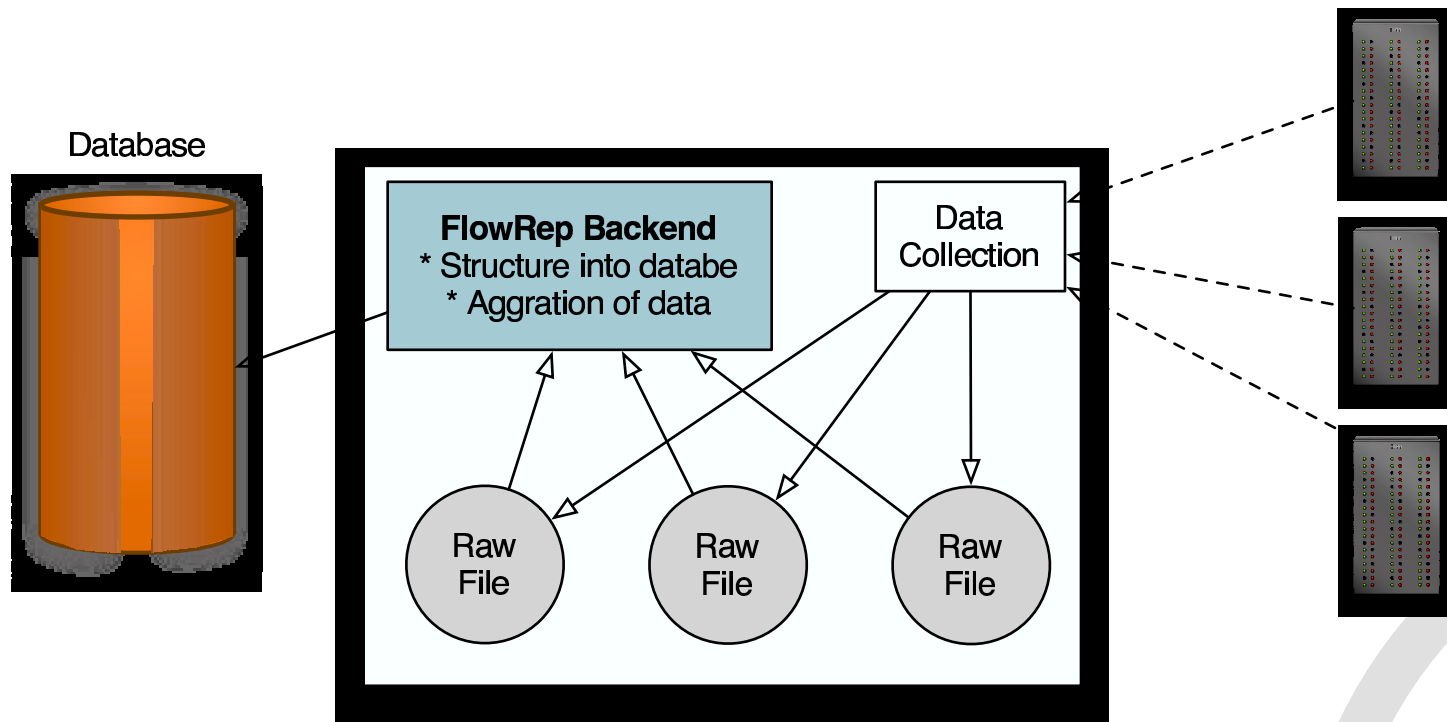
Stager structure



backend processing

Collect data and put into database

Periodic maintenance and aggregation



Stager Flow

- Flow reporting tool for Scampi
- Netflow v5, v9, IPv6, Ipfix?
- Flow-tools used for collection, preprocessing and detailed inspection
- In operation for UNINETT cisco routers
- 20 routers, 258 links

Report setup > Graph Source Port Simple Limit rows: 25 OK [Login]



Month Monday Day

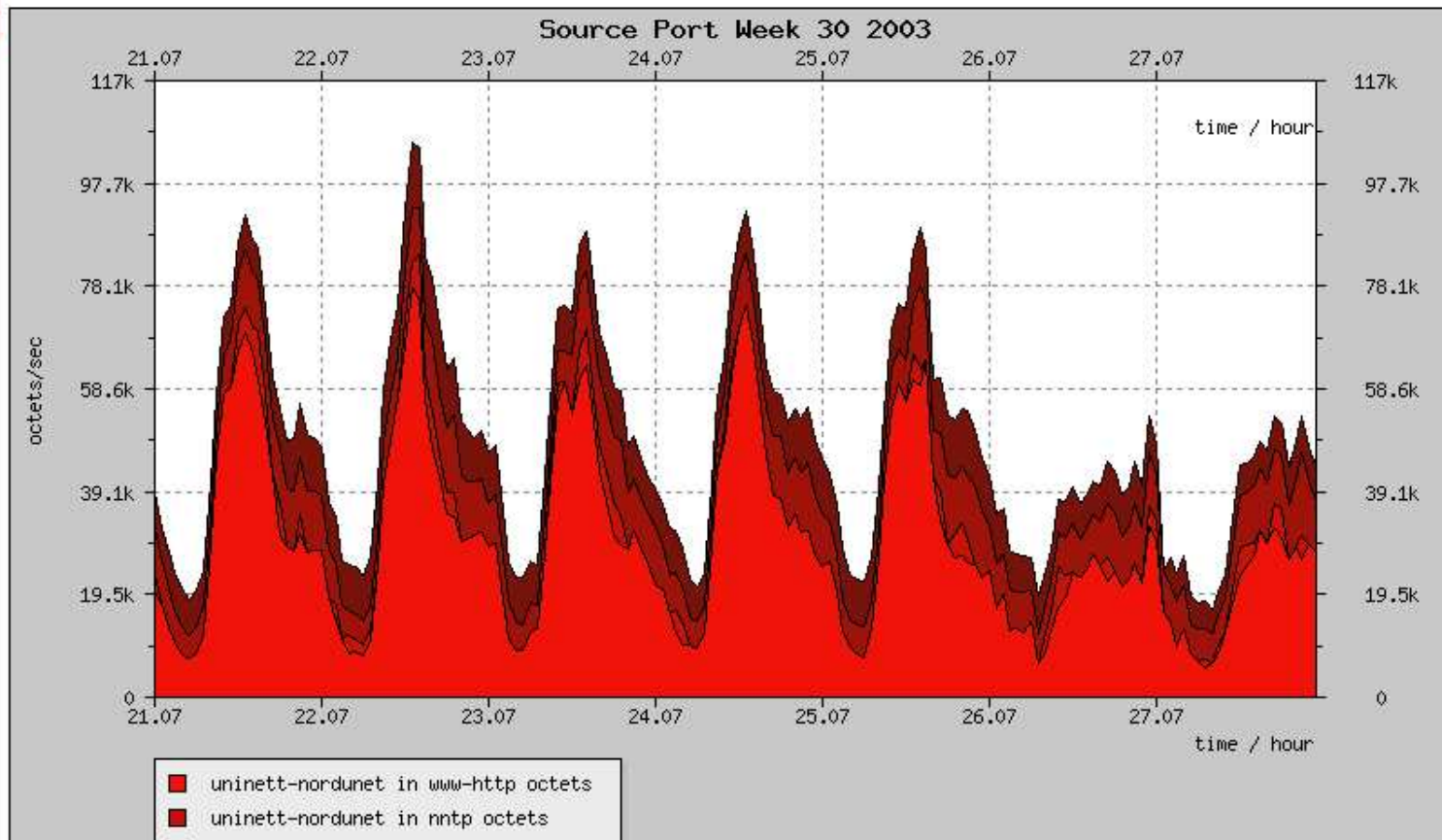
Show all Select Group
 uninett-nordunet Opposite
 Direction In Out
 Choose interface



Plot type: Area graph Y-scale: Linear Plot image size: 800x400 Omit other Replot

Source Port

Week 30 2003



Stager SQL experiences

- Now 40GB, 4 weeks, 258 links, 375K records per hour
- Swift response as far as 250GB
- 4 disk sw raid on dual 3GHz Xeon
- smaller queries locks up less
- index just when needed
- inserts limited by disk io
- turn off buffer flushing - data can be rebuilt