Monitoring the hidden: TimeMap

Claudio Allocchio (GARR)
And GN5-1 WP6 T3 team
TimeMap-dev@lists.geant.org

www.geant.org

Outline

- Why Timemap
- Current status
- Beyond observation: anomaly detection
- Further development

What are we talking about?

How is the road ahead today?

And how is it is in average?

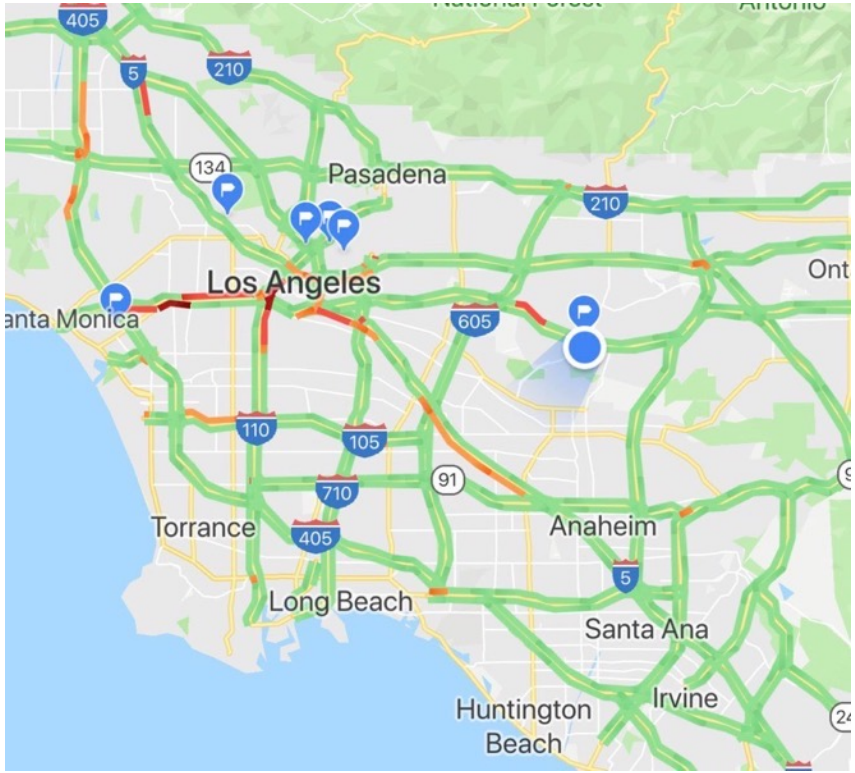
“Road report: on HWY 101 there are 364 vehicles per minute”

it may
Be nice
…

“Road report: on HWY 101 there are 364 vehicles per minute”

Or…
Lots of Stop & Go

“Road report: on HWY 101 there are queues at the red spots”



…but we also like to know transit times

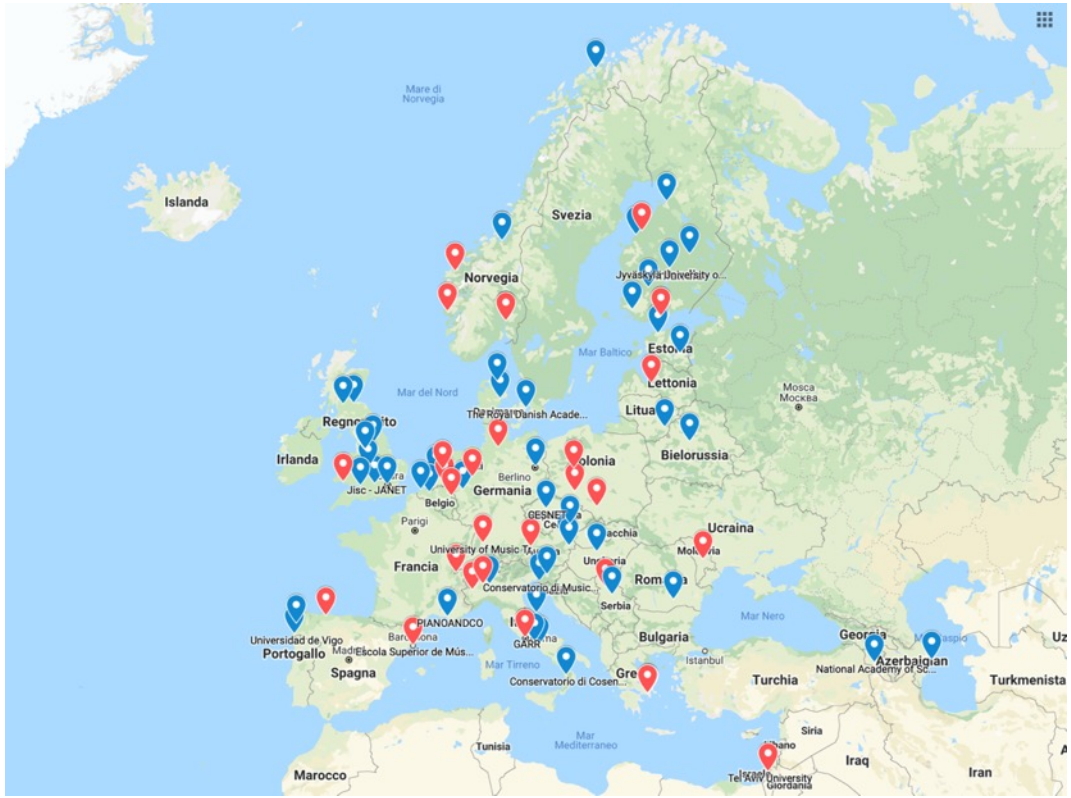
Network Traffic: what do we usually have?

But this is OK for bulk data transfers

NOT for real time applications which are sensitive to Latency & Jitter!

Can my application set the cruise control on and live happily?

Applications which need “cruise control” on are on fast rise!

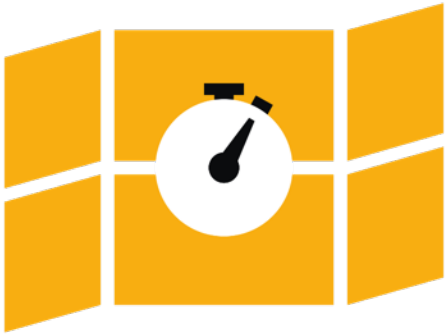


- LoLa

+ 30%

We need to monitor ”the hidden”:

- latency
- jitter



TimeMap

We need to keep track of ”the hidden”:

- historic series

We need to find anomalies in “the hidden”

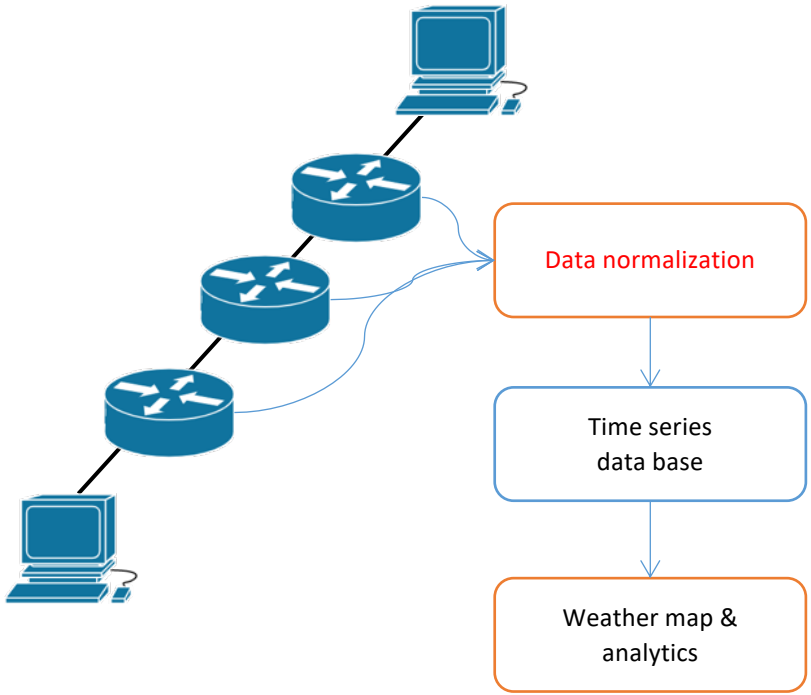
- machine learning
- alarms
- call the Police! … well, call the NOC people!

So in GN4-3, WP6 T1 we designed TimeMap!

Architecture requirements

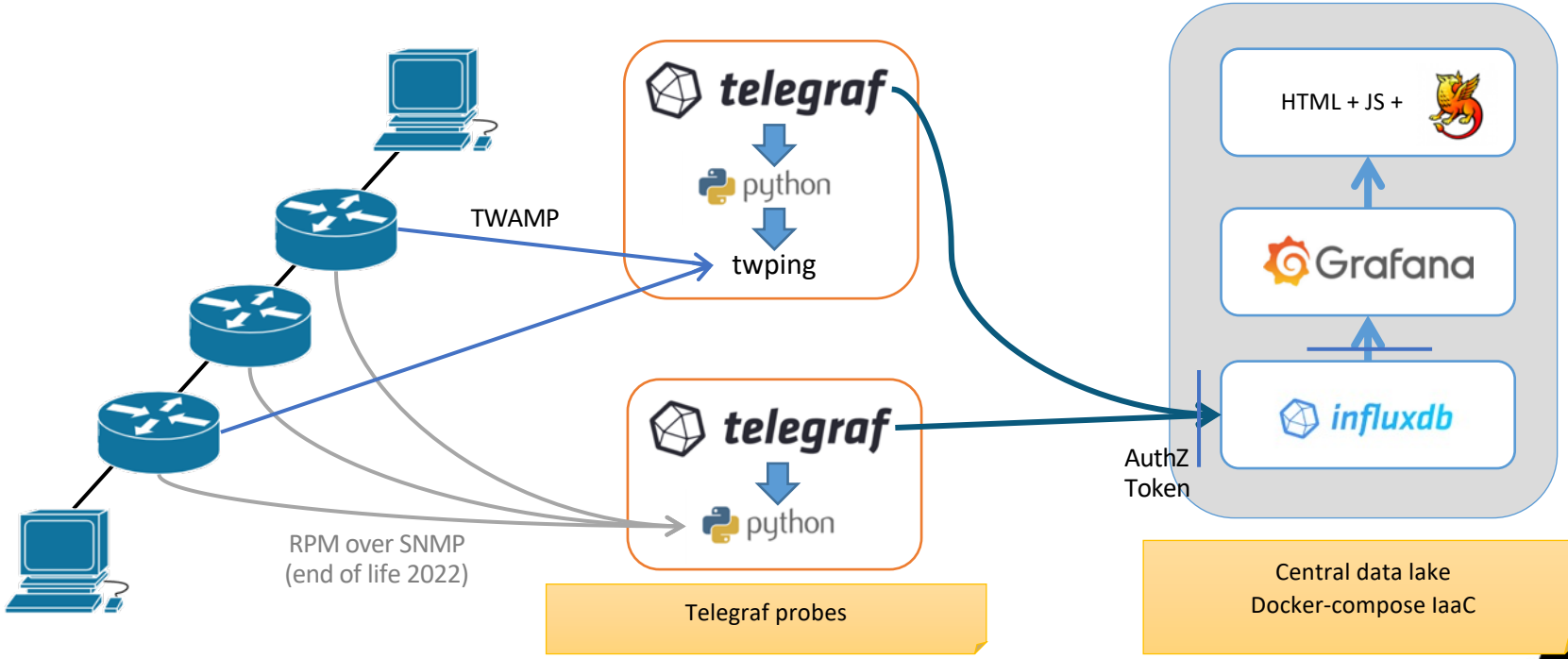
- Scalable and portable system
- Network architecture neutral
- Based on monitoring standard specifications
- Based on Open Source components
- Modular containerized system
- Easy to deploy
- With federated access control

TIMEMAP architecture and features

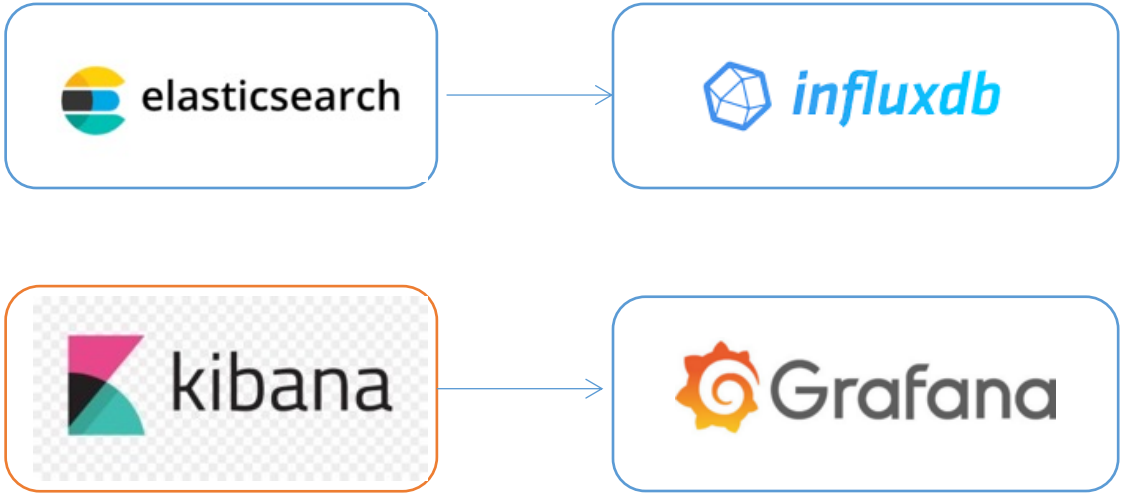


- Latency & Jitter data collection
  - TWAMP from all backbone routers
  - TWAMP from selected PerfSonar installations
  - RPM from all backbone routers (EoL 2022)
- Simplicity: almost zero footprint
  - Docker + Linux packages
  - Minimal custom code
  - Dynamic weather map GUI
- Security
  - eduGAIN authentication
  - Role Based Access Control
  - multi-tenancy

TIMEMAP v1 architecture – 1+ year of data taking

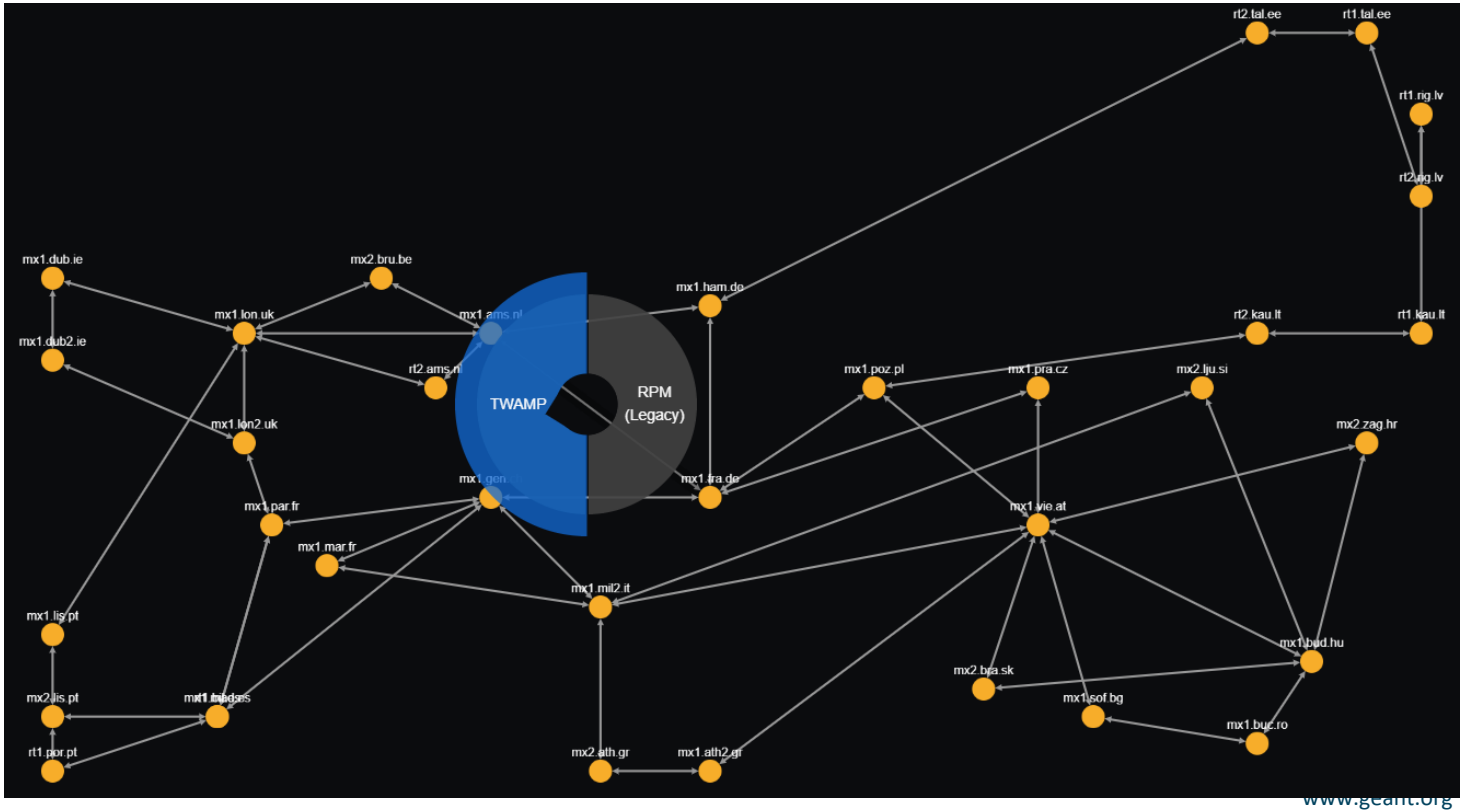


Flexibility: from prototype to production modules:

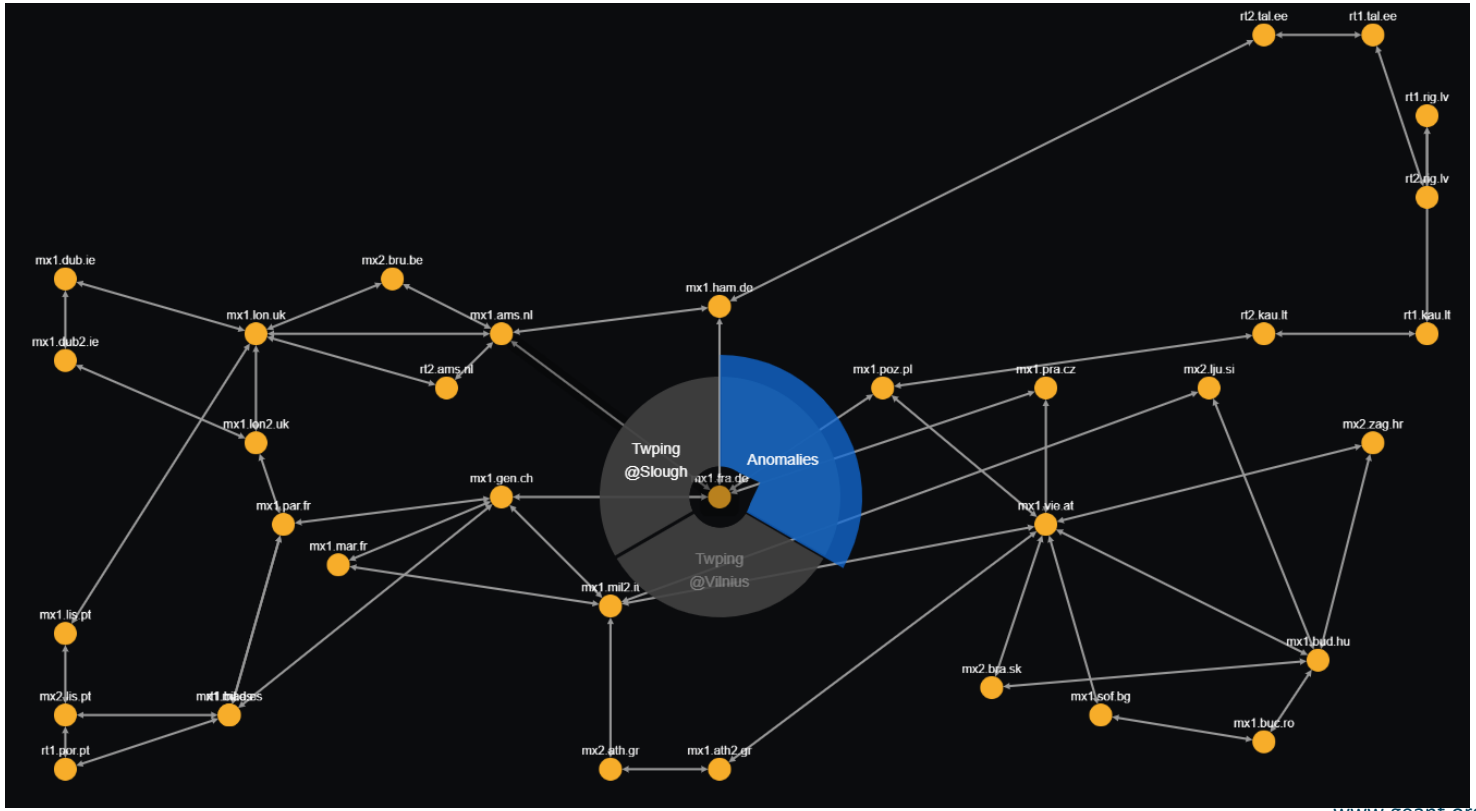


An “offline” view of the service (before we try go live!)

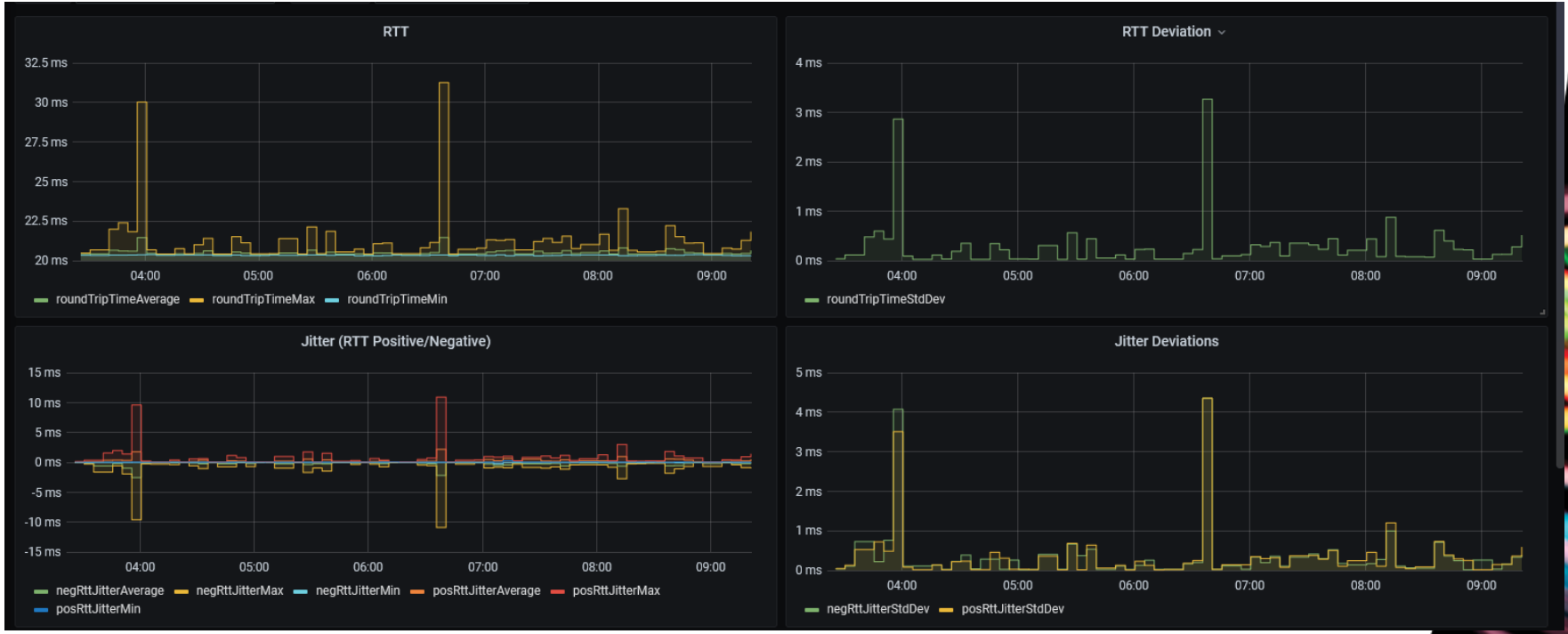
The entry map page: click on link



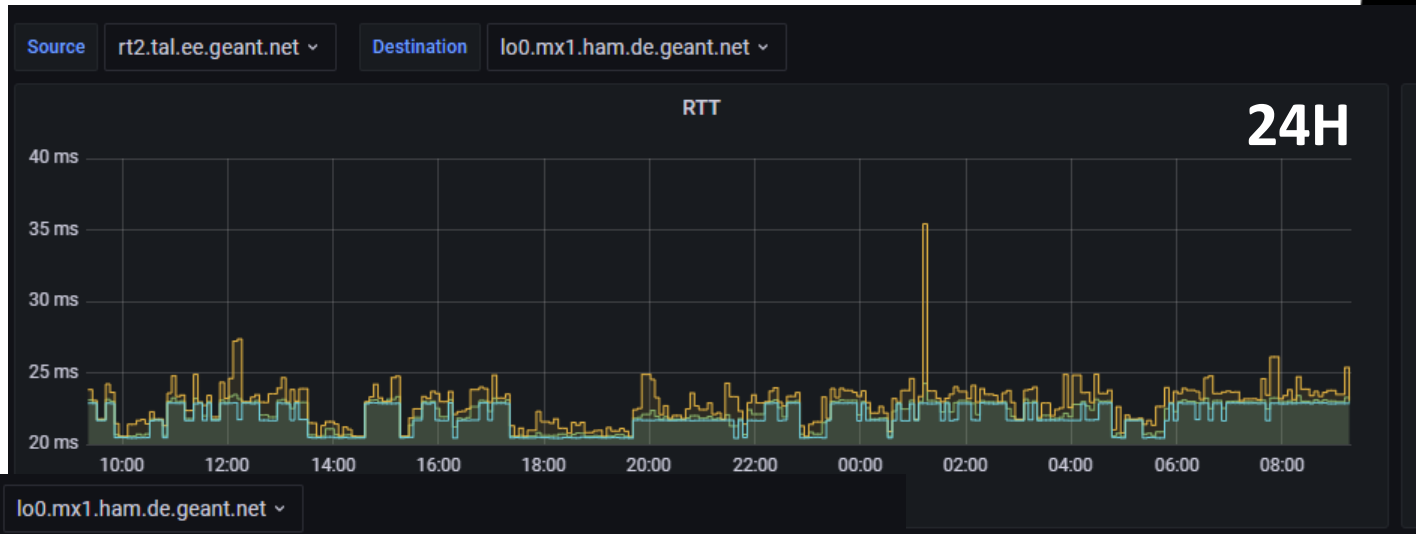
The entry map page: click on router

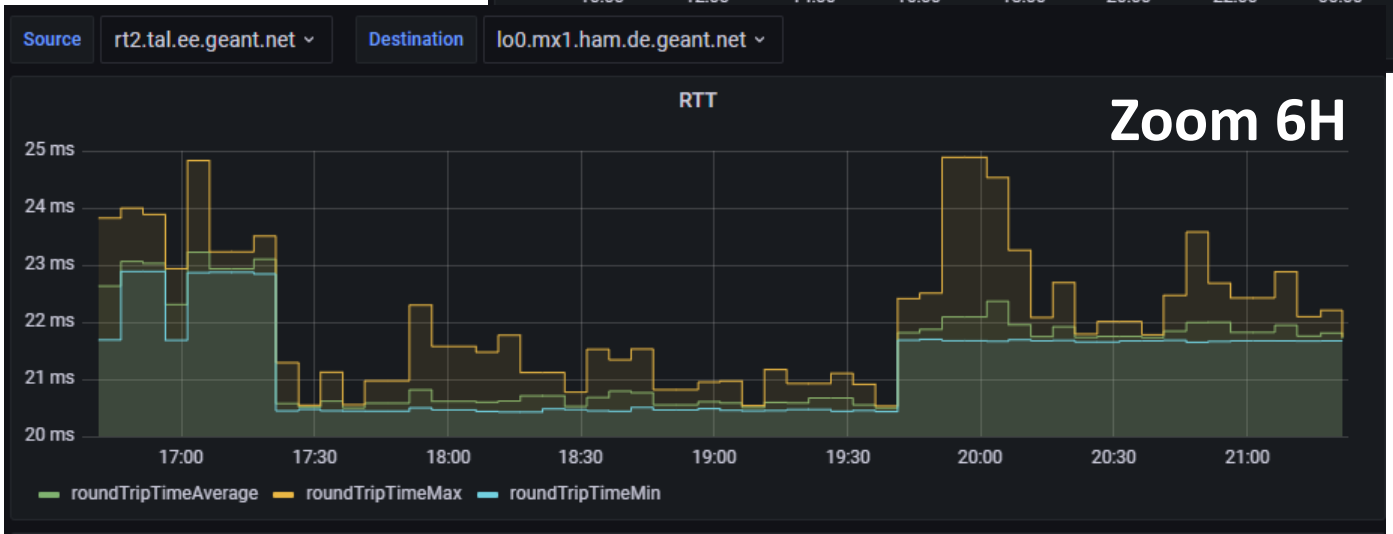


Periodic events

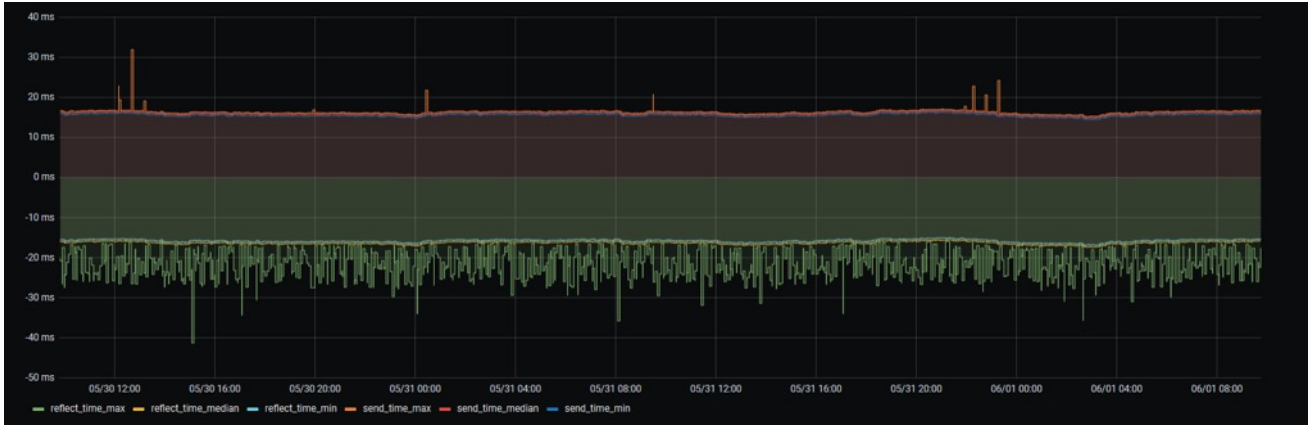


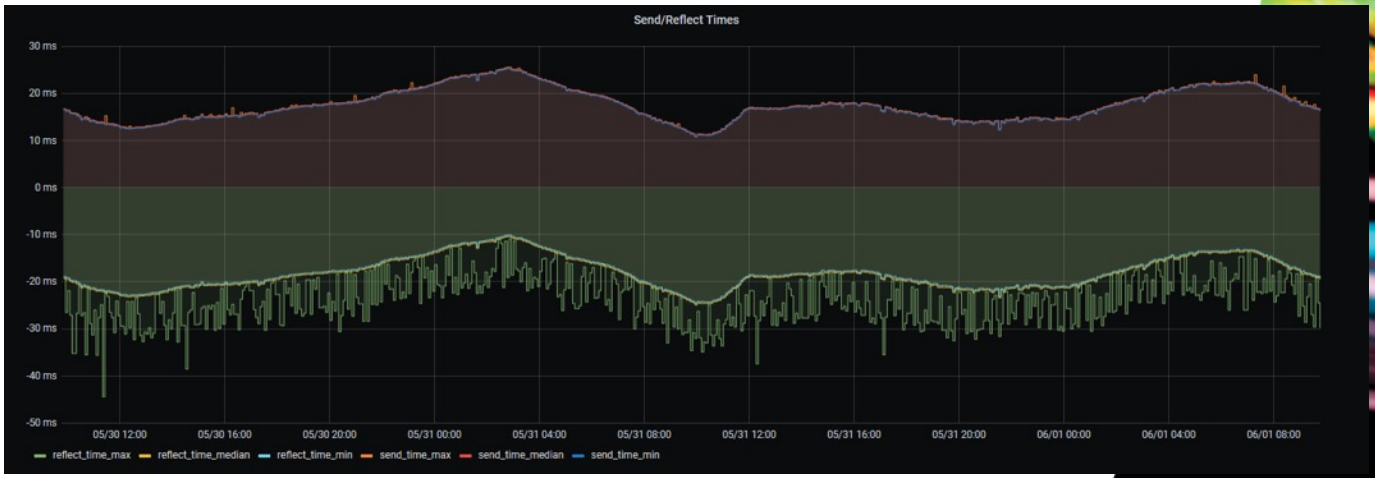
Re-routing


Source
rt2.tal.ee.geant.net
Destination
lo0.mx1.ham.de.geant.net
RTT
24H
40 ms
35 ms
30 ms
25 ms
20 ms
10:00
12:00
14:00
16:00
18:00
20:00
22:00
00:00
02:00
04:00
06:00
08:00

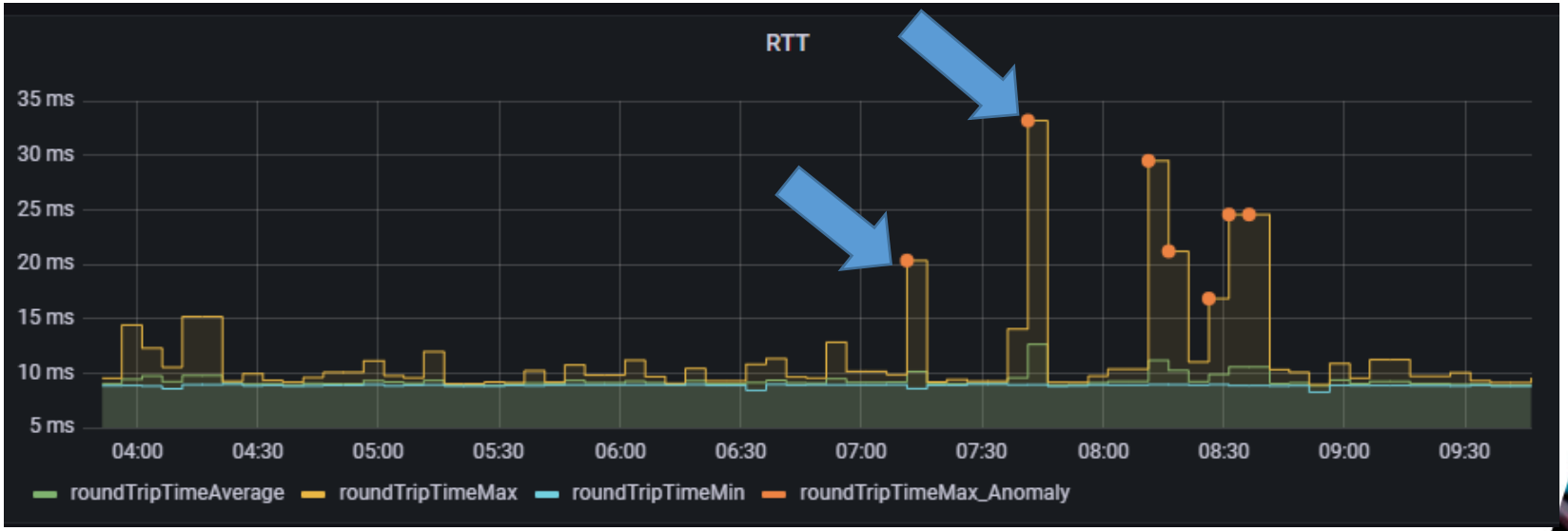

Source
rt2.tal.ee.geant.net
Destination
lo0.mx1.ham.de.geant.net
RTT
Zoom 6H
25 ms
24 ms
23 ms
22 ms
21 ms
20 ms
17:00
17:30
18:00
18:30
19:00
19:30
20:00
20:30
21:00
roundTripTimeAverage
roundTripTimeMax
roundTripTimeMin

Trends (clocks shifting?)

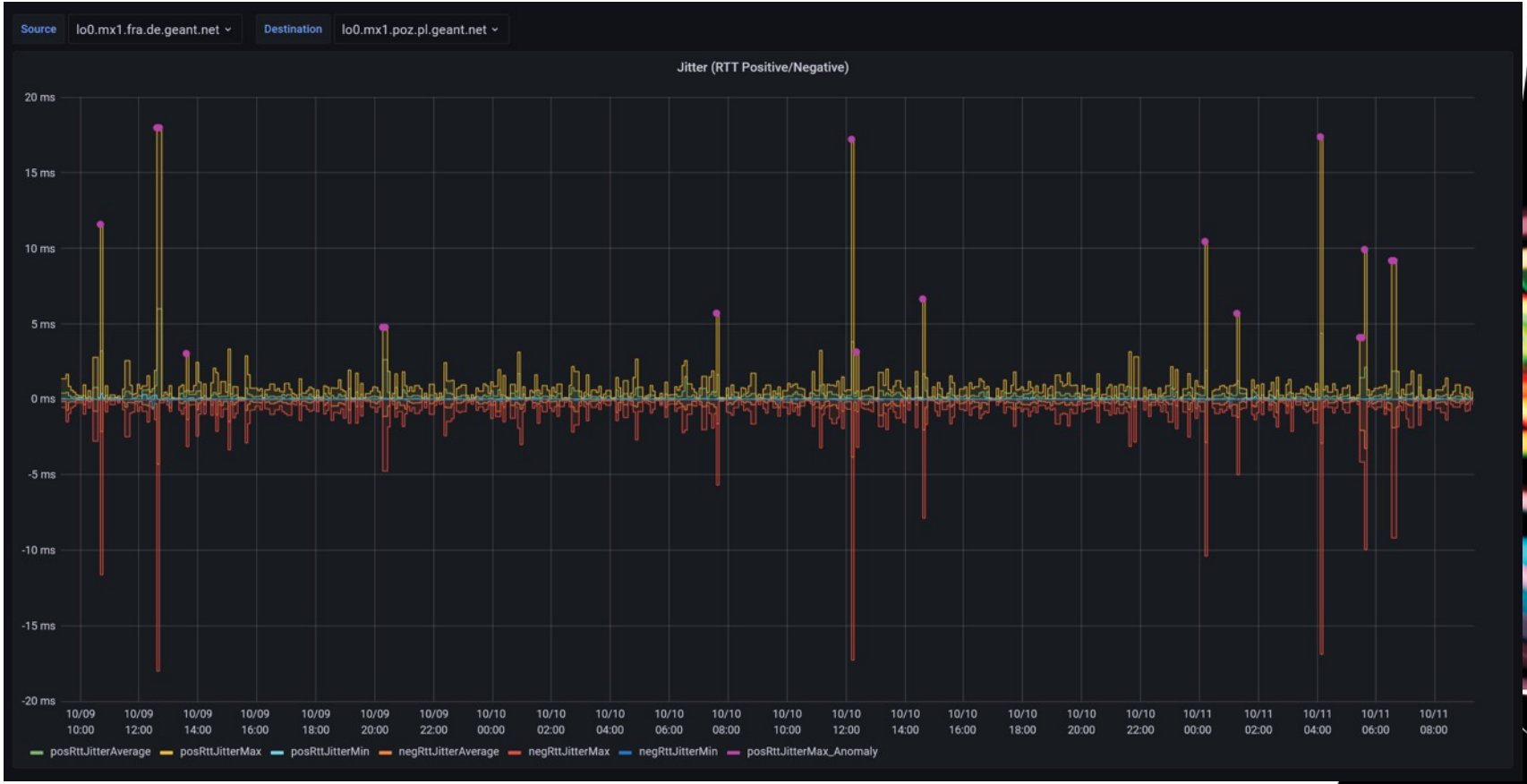




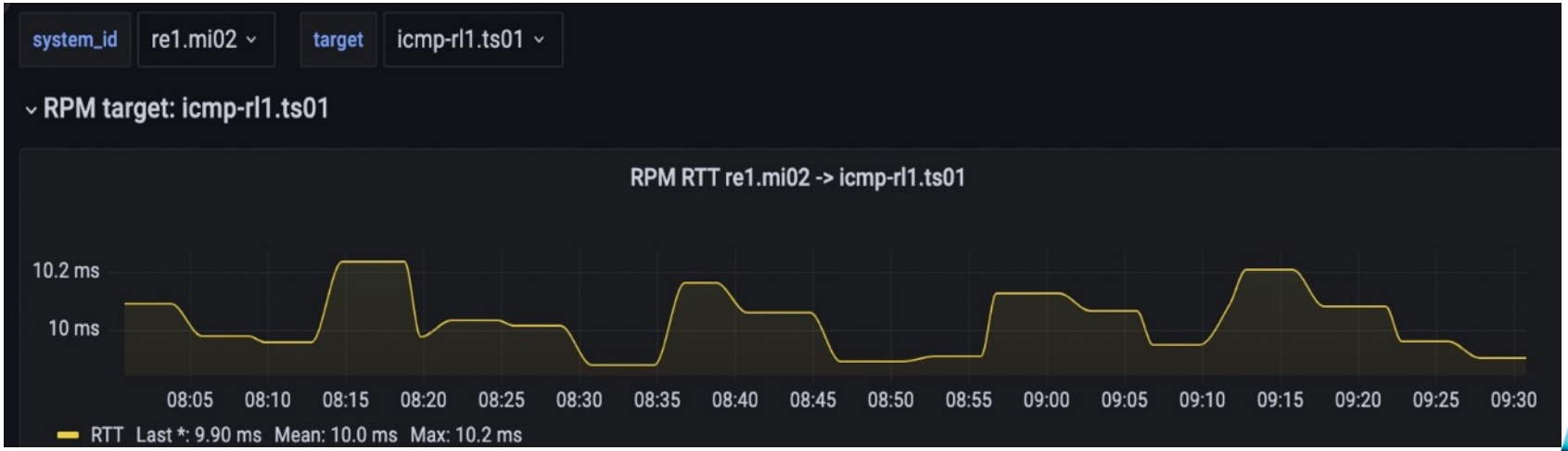
Anomaly Detection (AD) in Timemap



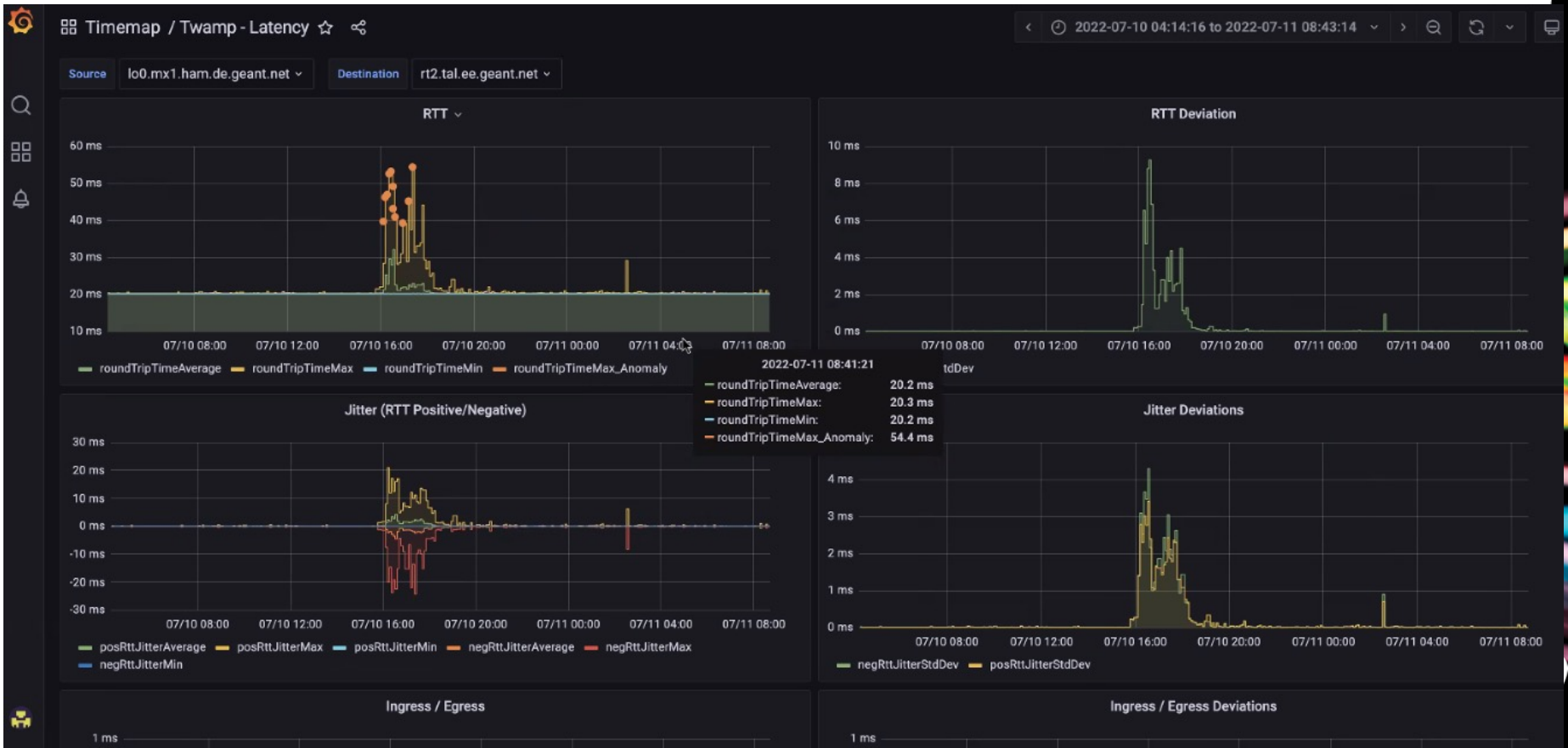
One more plot



Equal Cost Multipath Protocol (ECMP) effects

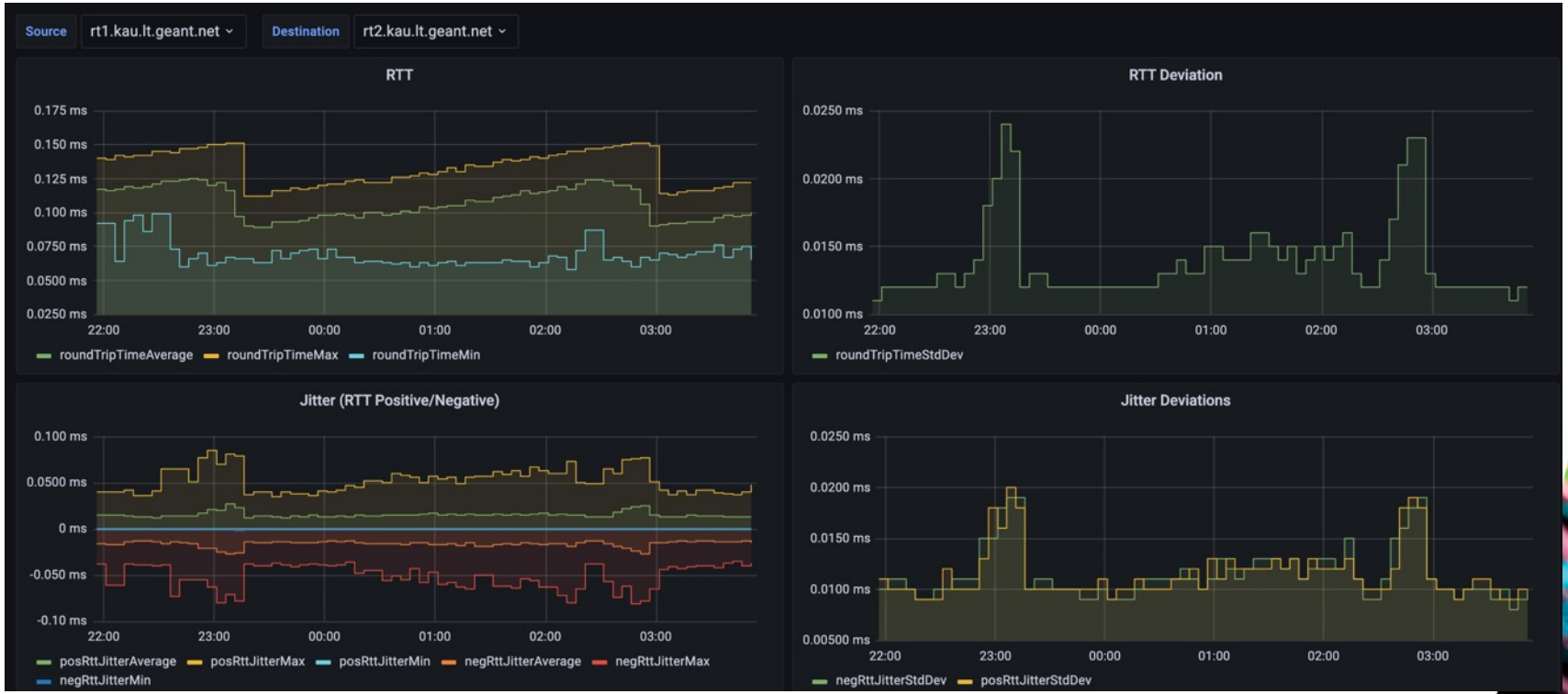


«non-identified event»



«non-identified event»

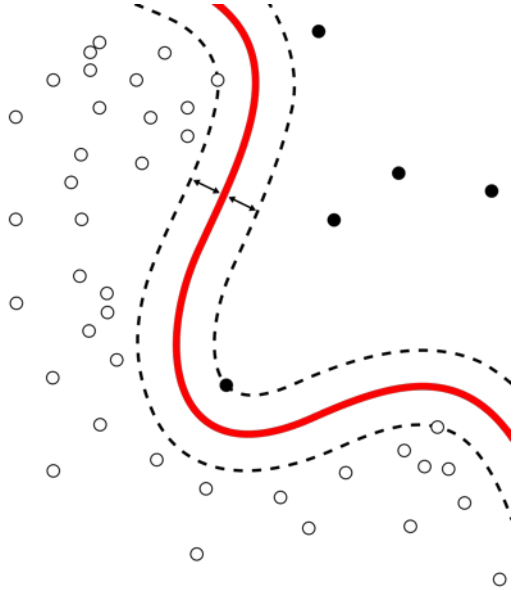
«non-identified event»



The research: Anomaly Detection (AD) in Timemap requirements

- Move beyond the simple observation
  - AD for Analytics and Alerting
  - Co-occurring events correlation

- Requirements on AD machine learning
  - Real-time or micro-batch learning/inference
  - Robust estimation
  - Light footprint

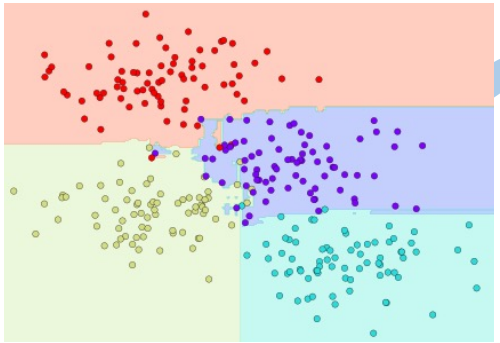


Anomaly Detection in Timemap – toolset

- Anomaly Detection, in short
  - Std.Dev classification
  - Unsupervised
  - Sensible to overfit

- Streaming ML in Python
  https://riverml.xyz

Half-space Random Trees

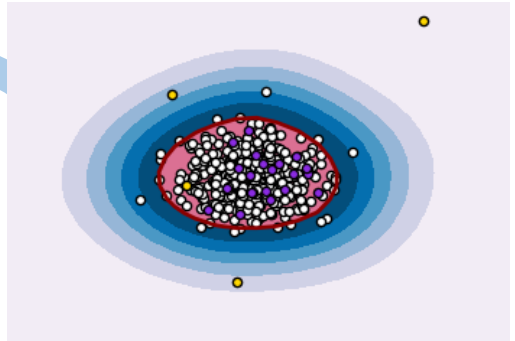


3σ

3σ

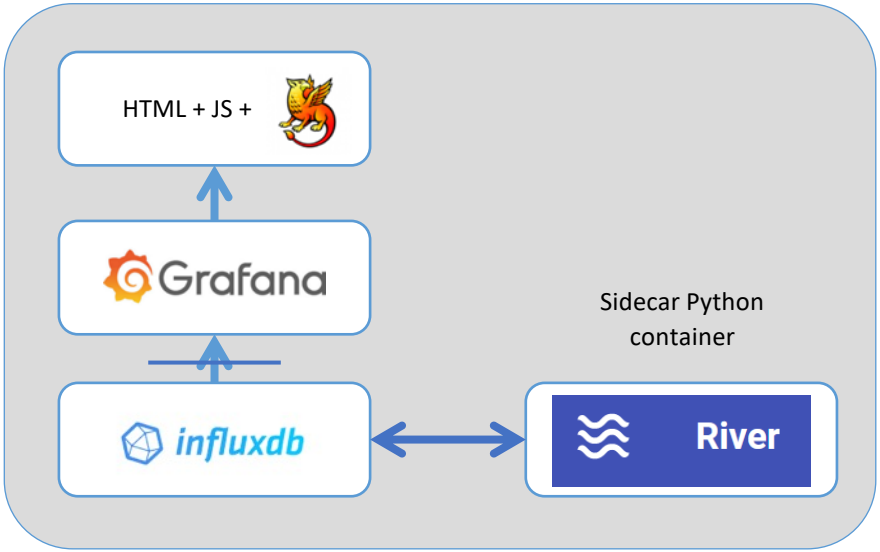
Model bagging

One-class Support Vector Machine

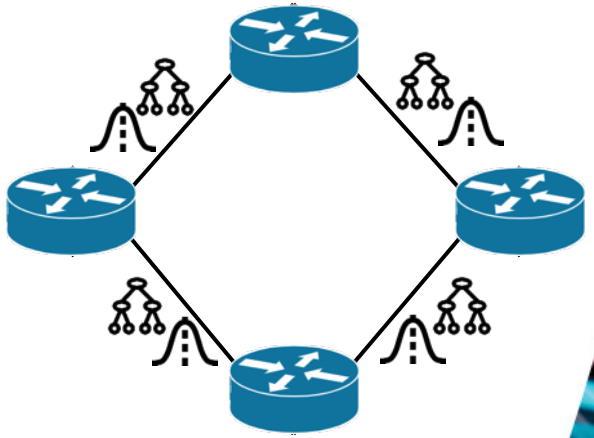


Anomaly Detection in Timemap – architecture

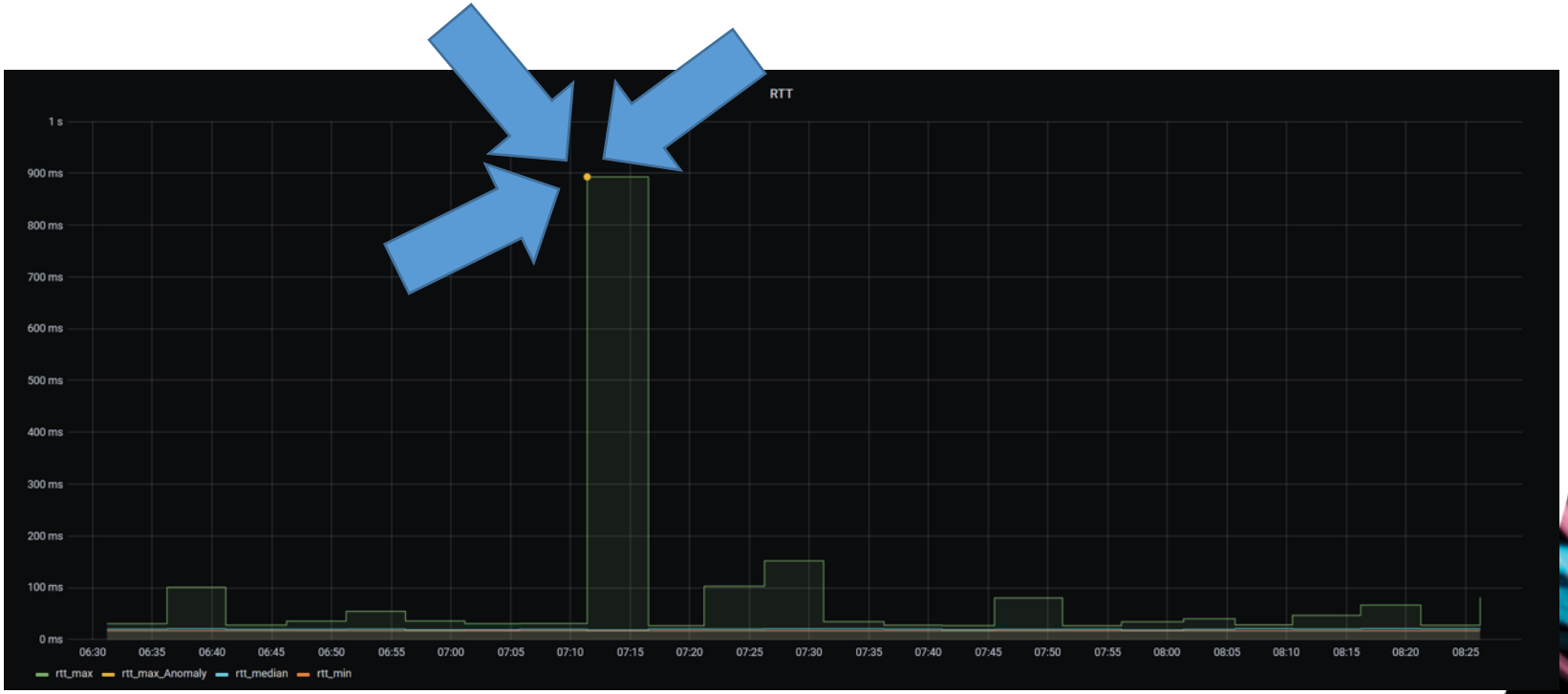
Software architecture extension



Network topology and ML models



Almost the same look and feel



More about TimeMap

- The service on GEANT backbone

https://timemap.geant.org/

- Documentation: source code, user and admin guides, customization

https://gitlab.geant.org/gn4-3-wp6-t1-lola/timemap_public

https://timemap.geant.org

Current Status

- TimeMap is a new service in production for GÉANT

- Next steps
  - More deployments @NRENs
    - Timemap @ GARR
    - DeIC is deploying TimeMap
    - Sikt is assessing TimeMap
  - Anomaly Detection
    - Up and running, Streaming ML, multi-model over network topology
    - About 200 lines of code in a Docker image
    - New feature-rich algorithms in development
  - New usage
    - Inter-Domain
    - Measure not only 1 segment (a path or a part of path)
    - Improve anomaly detection for BGP rerouting, clock drifting, …
    - Characterize the behavior model for a link thanks to AI (ambitious)

Just to repeat …

- The service on GEANT backbone

https://timemap.geant.org/

- Documentation: source code, user and admin guides, customization

https://gitlab.geant.org/gn4-3-wp6-t1-lola/timemap_public

GÉANT
Networks • Services • People

Thank you!

Do you have any questions?

Claudio.Allocchio@garr.it

TimeMap-dev@lists.geant.org

www.geant.org

© GÉANT Association

As part of the GÉANT 2020 Framework Partnership Agreement (FPA), the project receives funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).