

Monitoring the hidden: TimeMap

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



TimeMap

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

...

www.geant.org

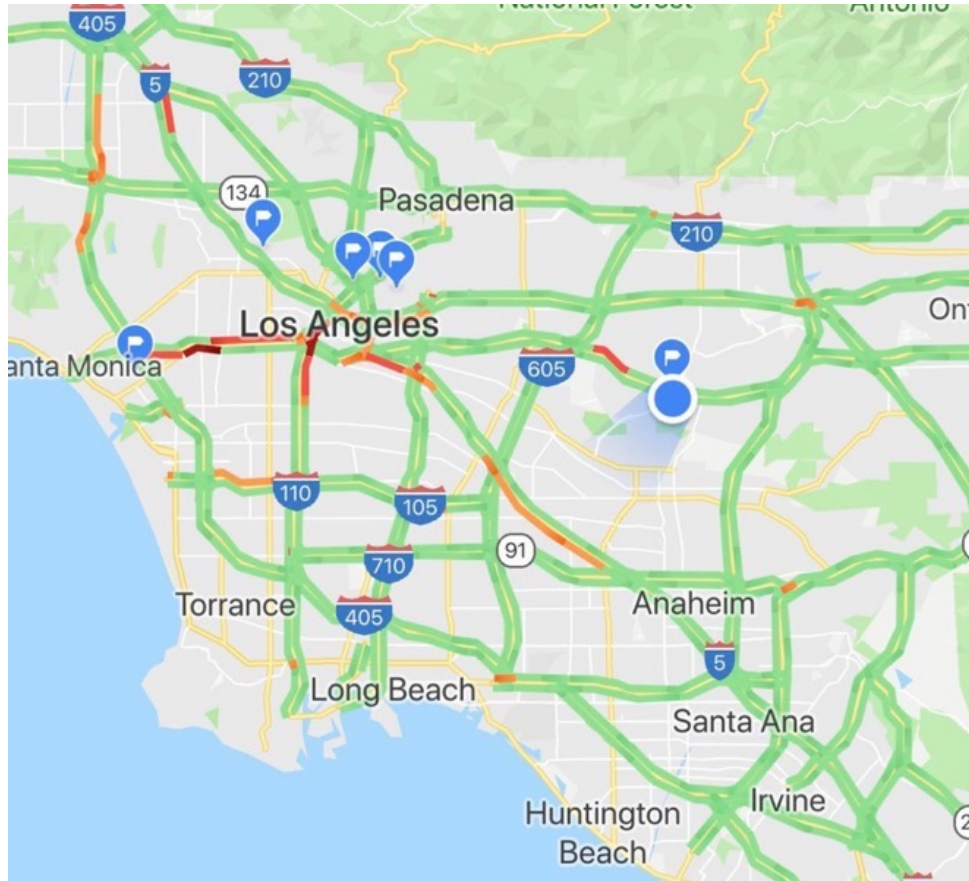
GÉANT

“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**

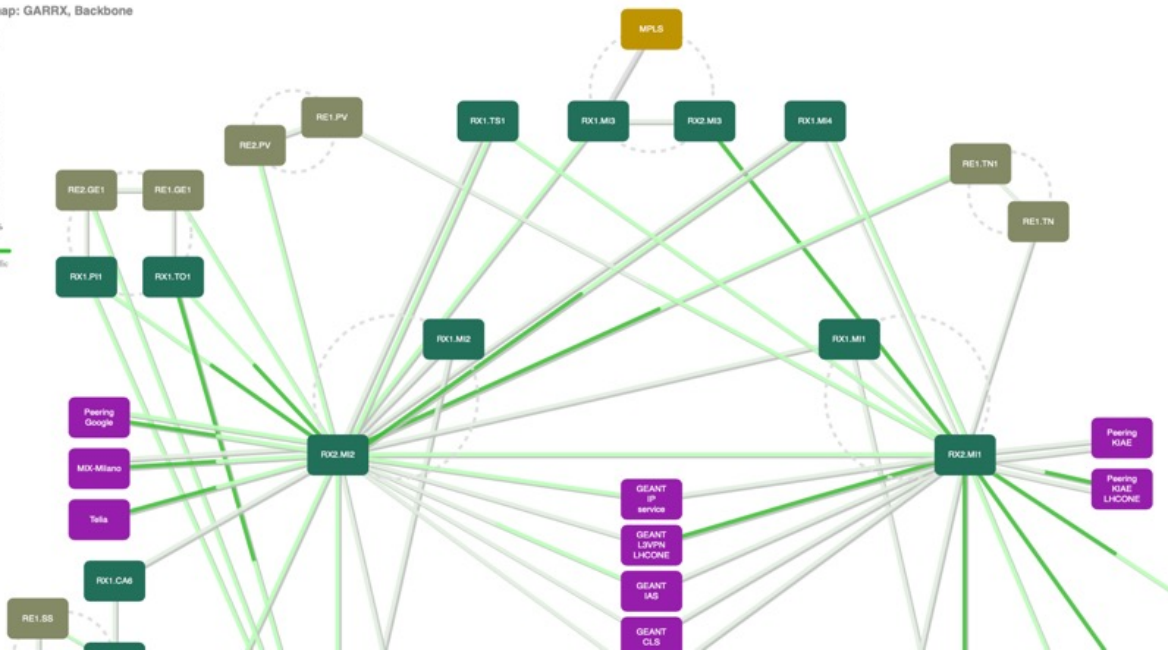
Network Traffic: what do we usually have?

GARR Weathermap: GARRX, Backbone

Load percentage

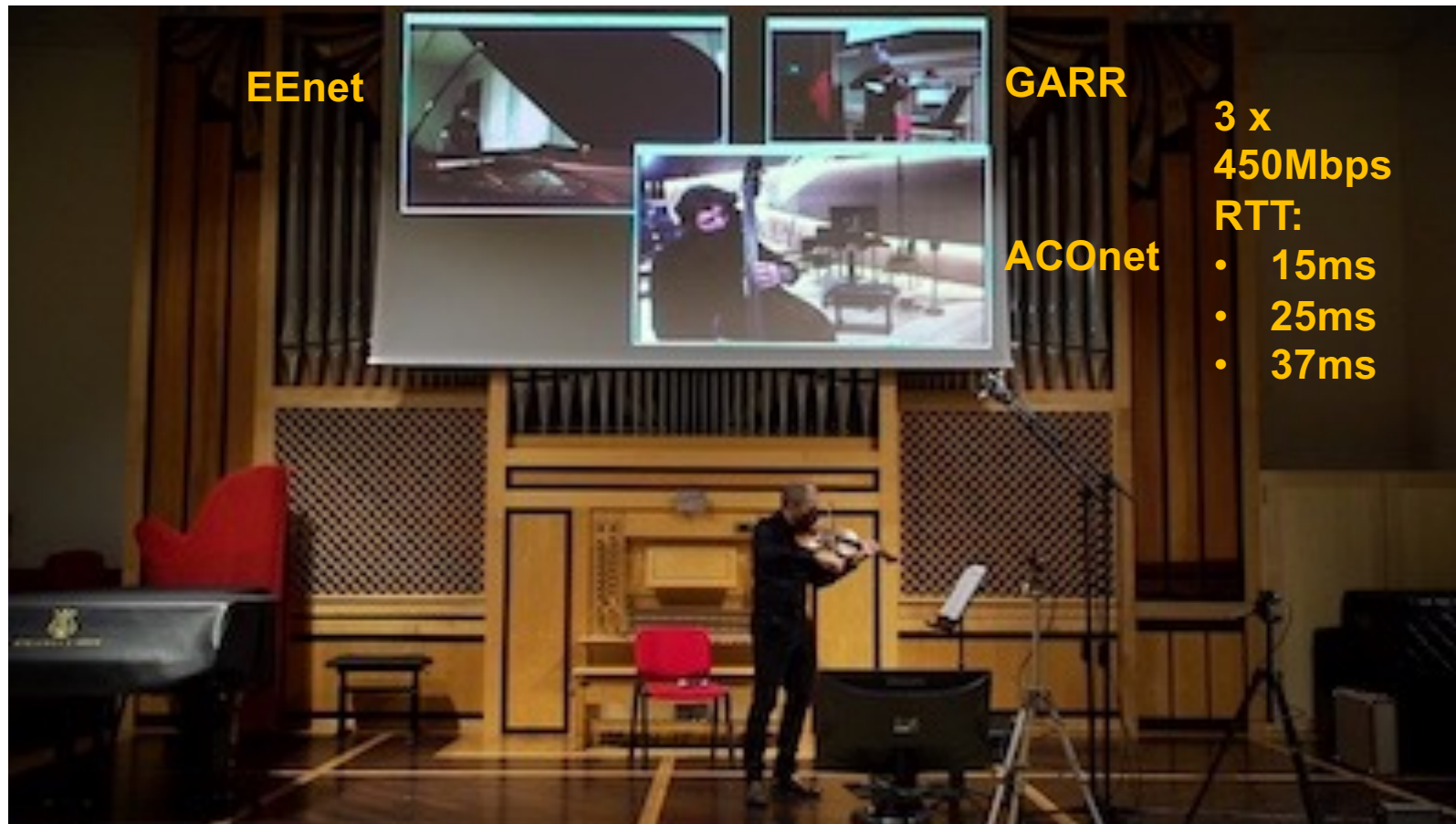


- Node
- User access
- User VPN
- Router Core/Pop
- Router Edge
- Switch PoP L2
- Peering
- GARR Service
- Aggregator



**But this is OK
for bulk data
transfers**

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



**3 x
450Mbps
RTT:**

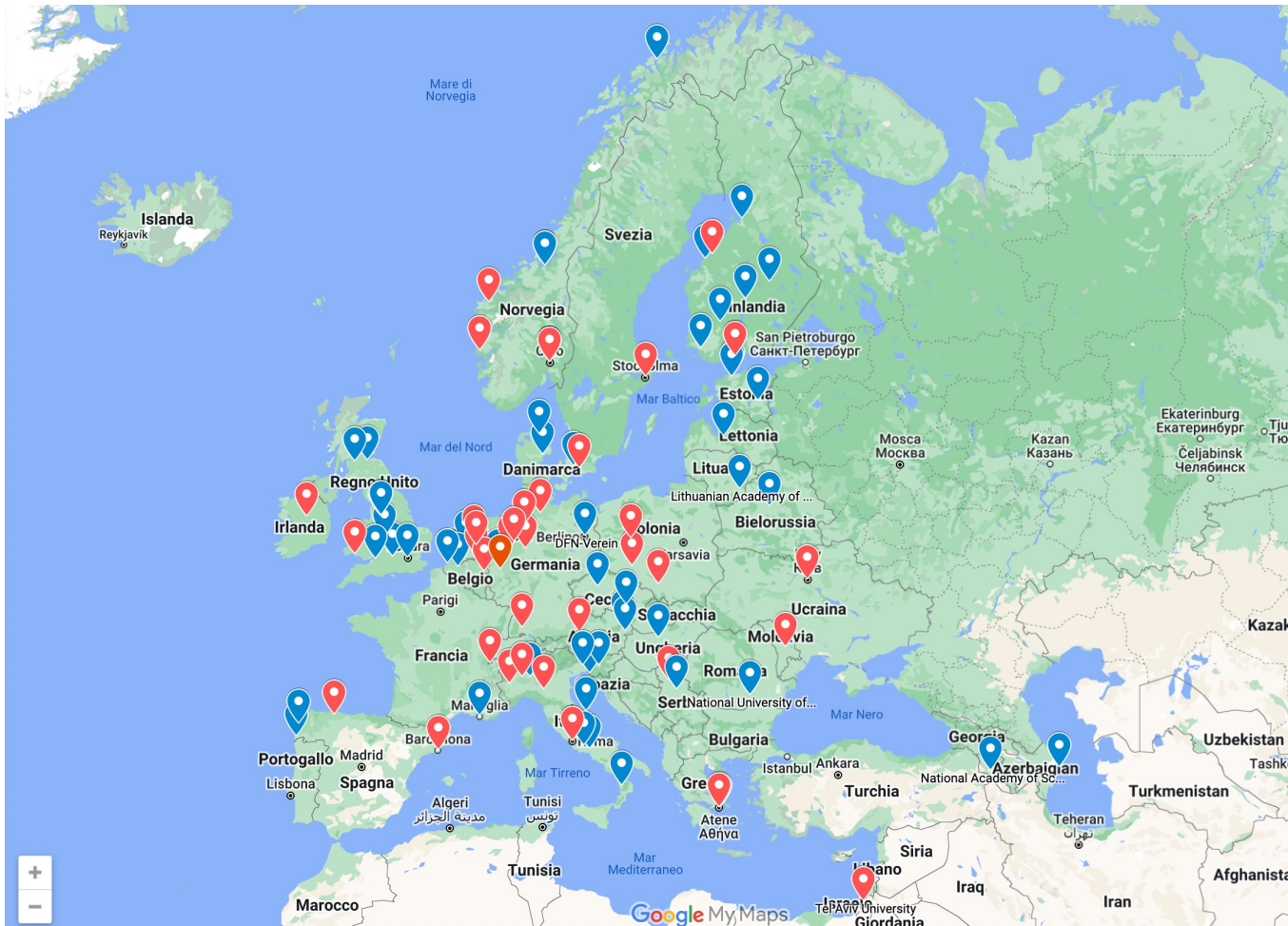
- 15ms
- 25ms
- 37ms

www.geant.org

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



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



• **LoLa**

+ 32%

www.geant.org



We need to monitor “the hidden”:

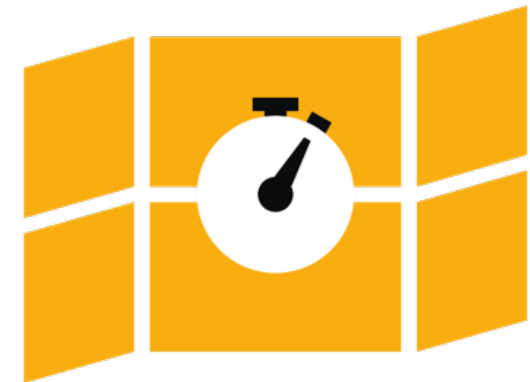
- latency
- jitter

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!



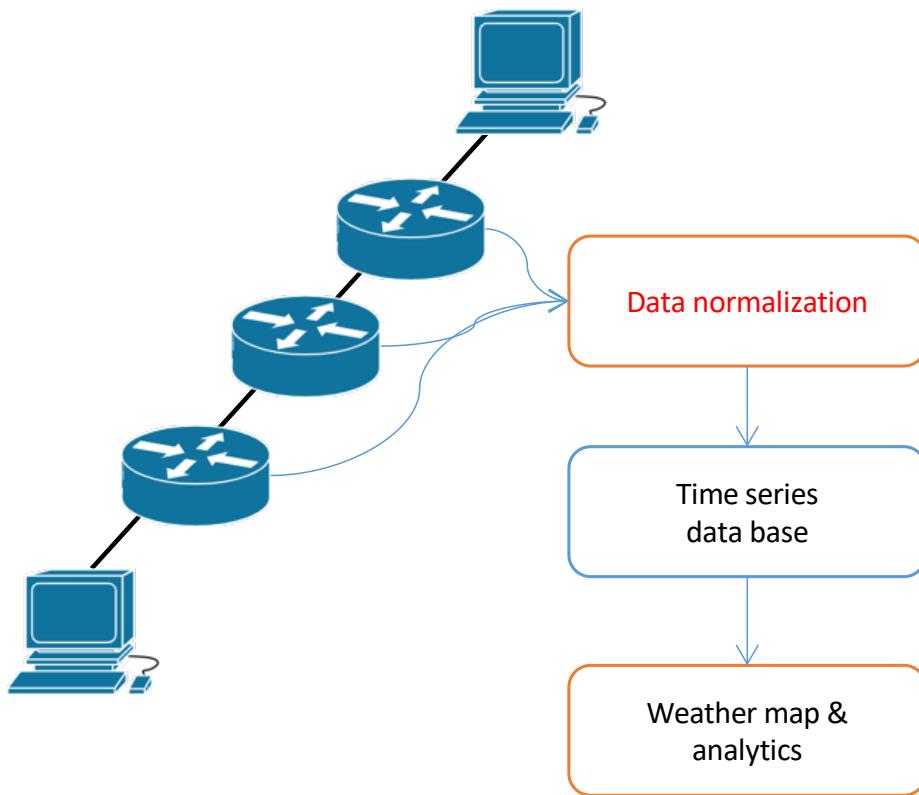
TimeMap

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

Architecture requirements

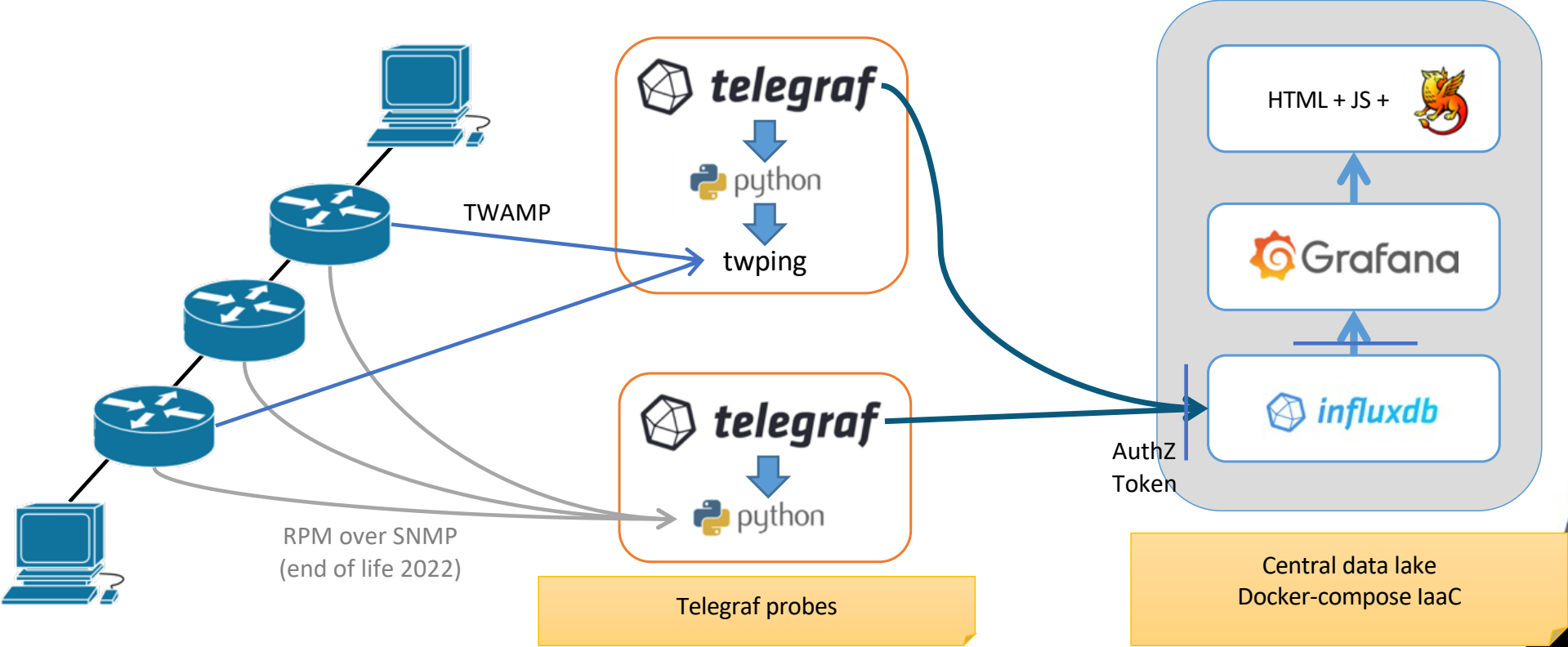
- Scalable and portable system
- Network architecture neutral
- Based on monitoring standard specifications
- Based on Open Source components
- Modular containerized system
- Easy to deploy
- With federated access control

TIMEMAP architecture and features

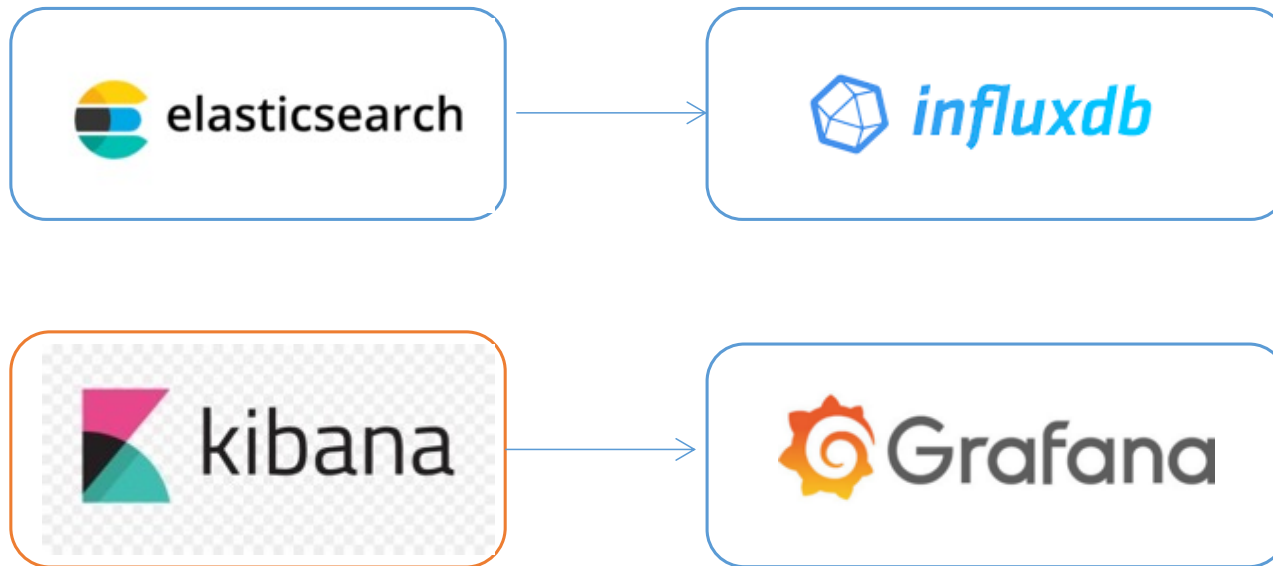


- Latency & Jitter data collection
 - TWAMP from all backbone routers
 - TWAMP from selected PerfSonar installations
 - RPM from all backbone routers (EoL 2022)
- Simplicity: almost zero footprint
 - Docker + Linux packages
 - Minimal custom code
 - Dynamic weather map GUI
- Security
 - eduGAIN authentication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

TIMEMAP v1 architecture – 1+ year of data taking



Flexibility: from prototype to production modules:

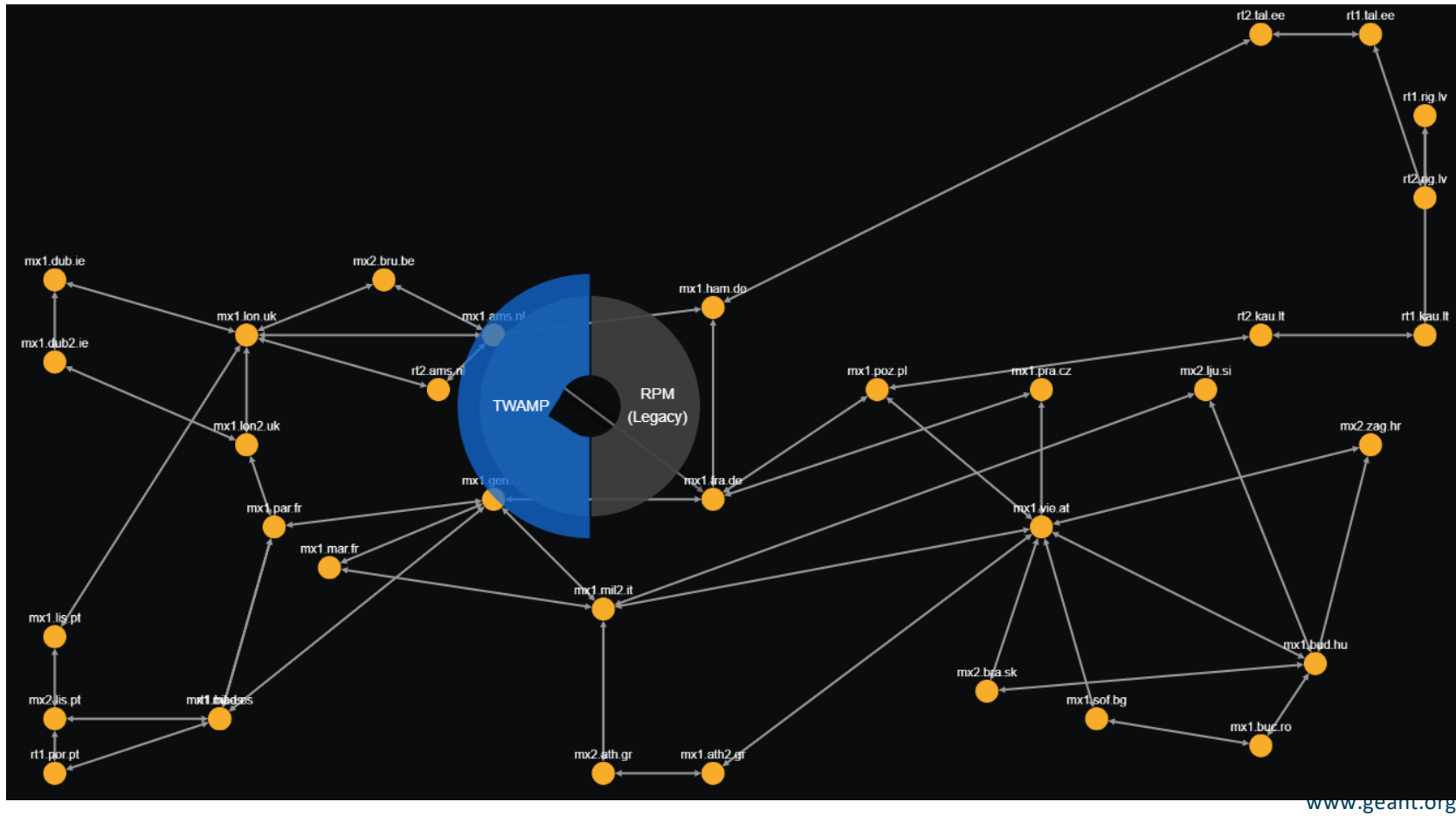


An “offline” view of the service
(before we **try** go live!)

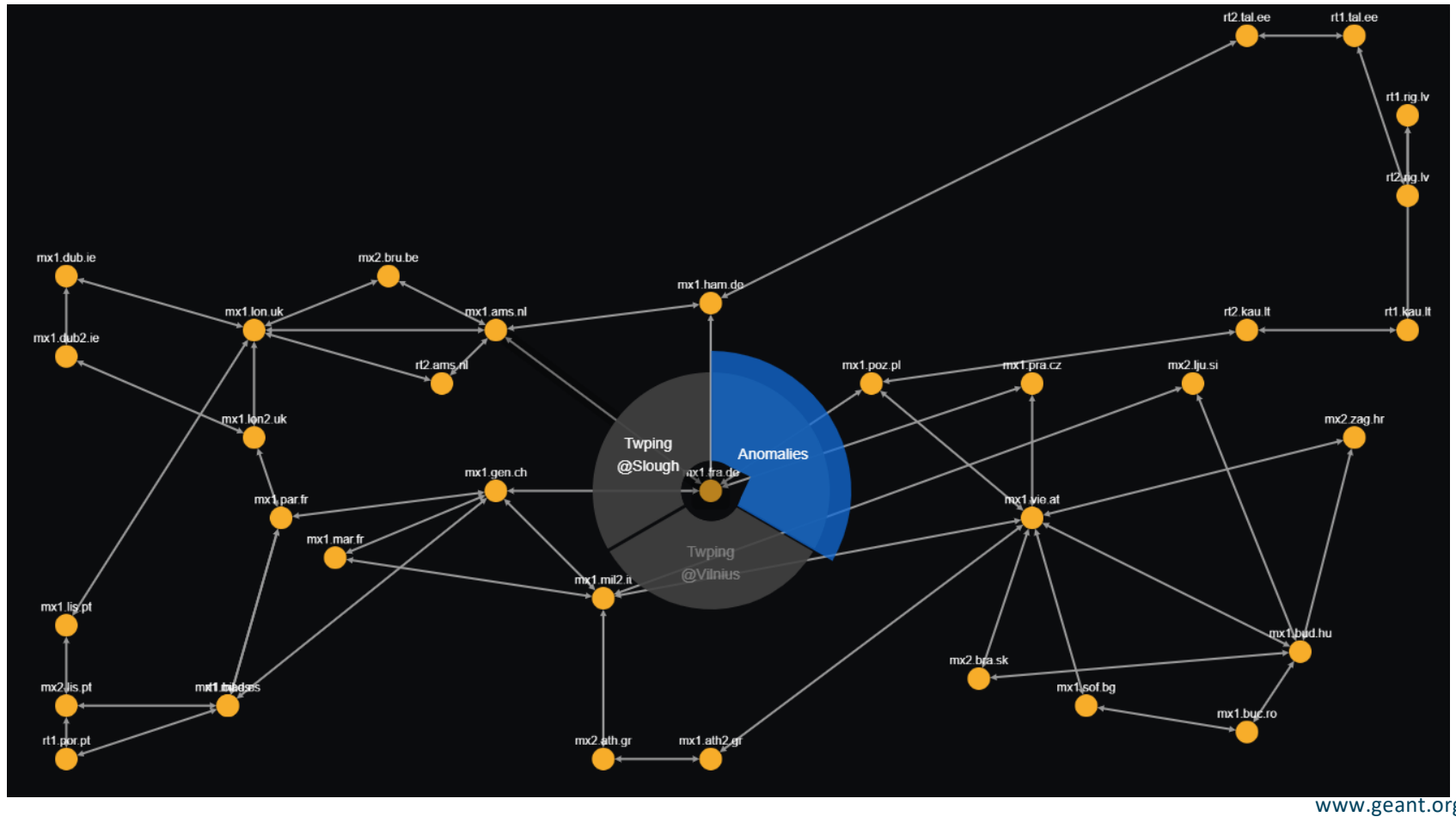
www.geant.org



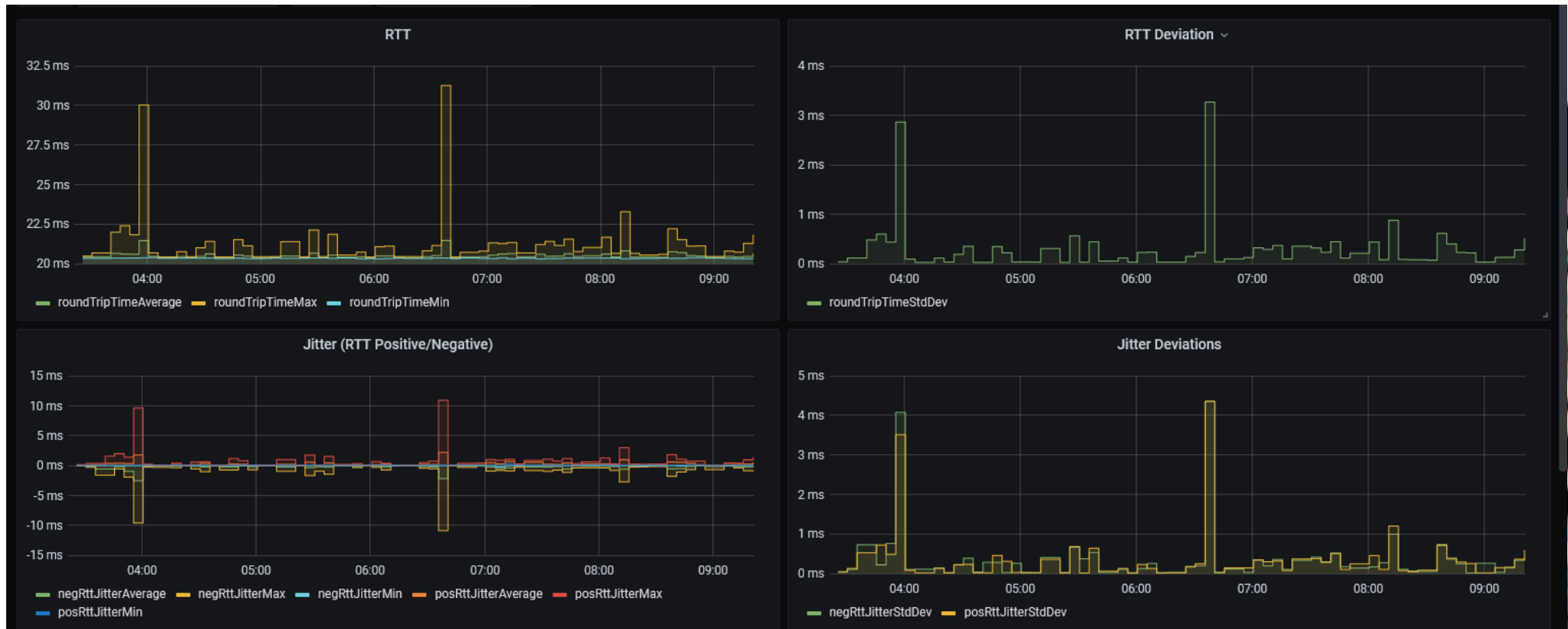
The entry map page: click on link



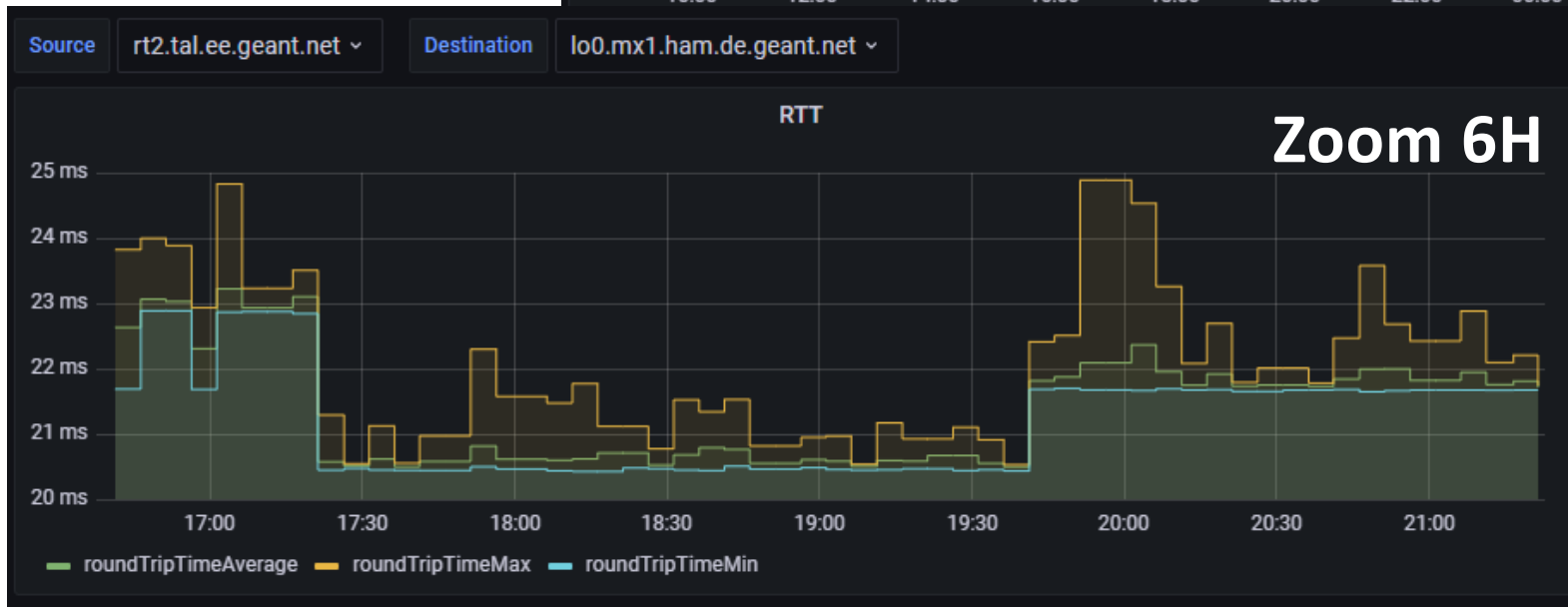
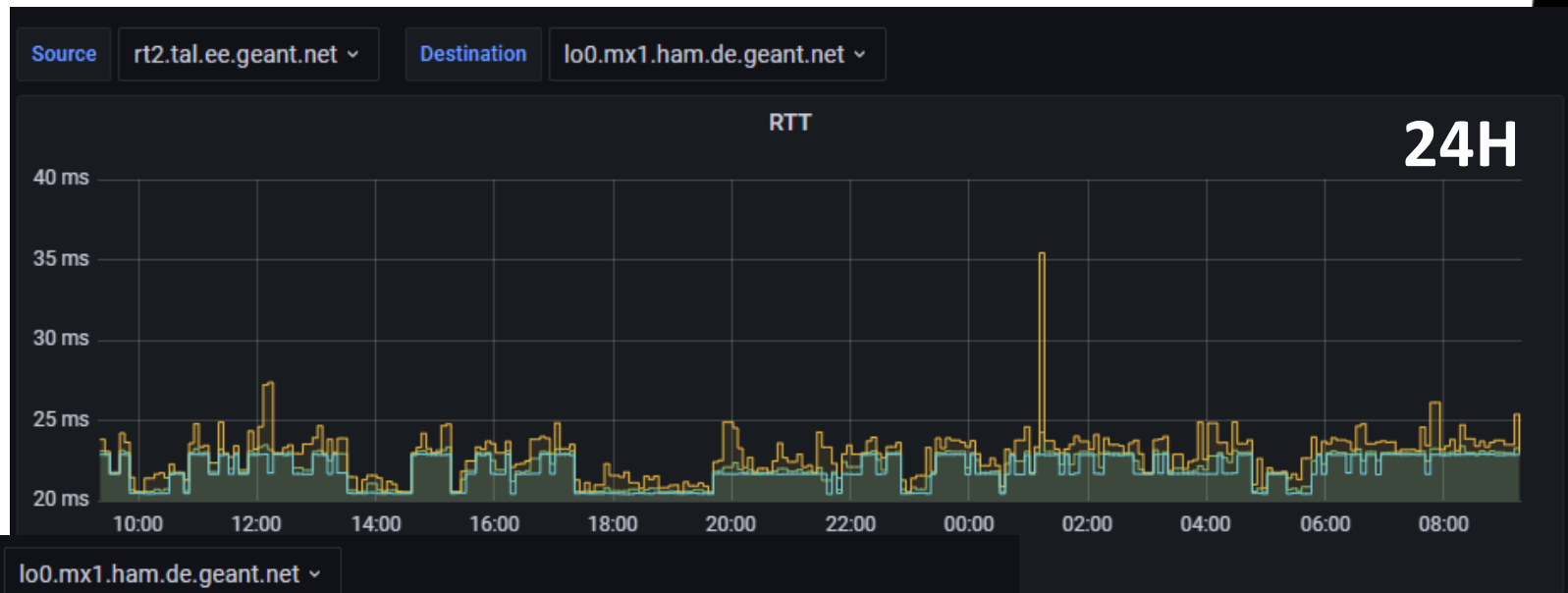
The entry map page: click on router



Periodic events



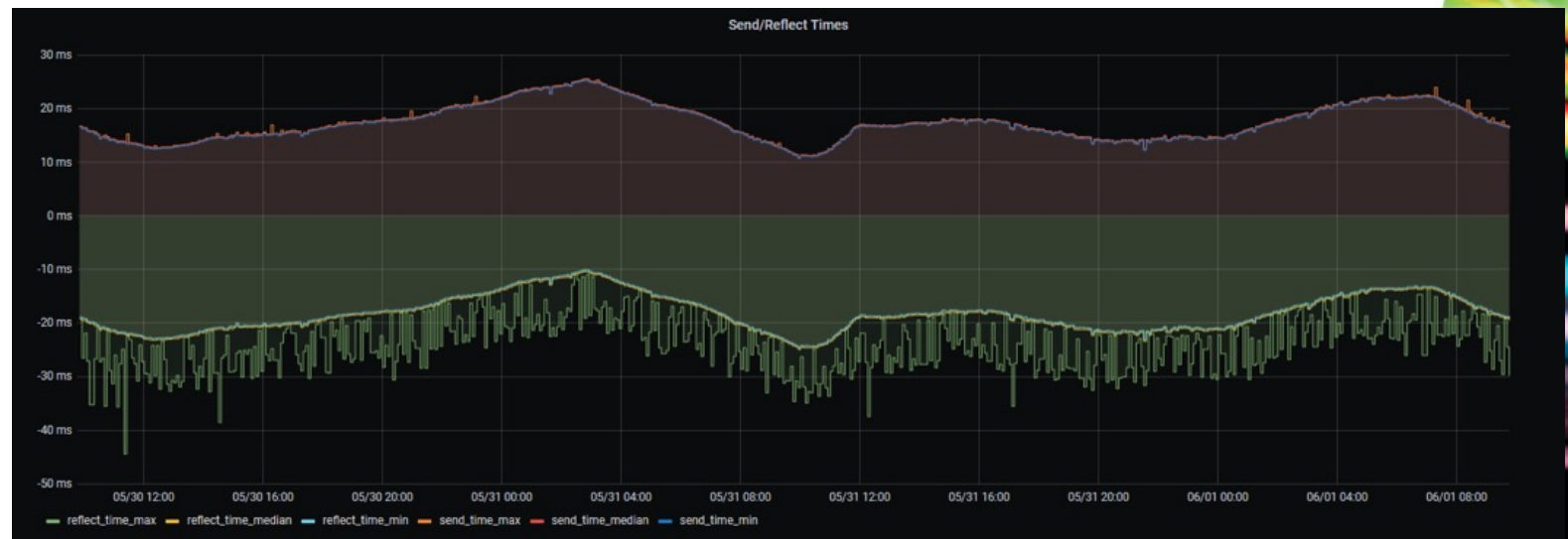
Re-routing



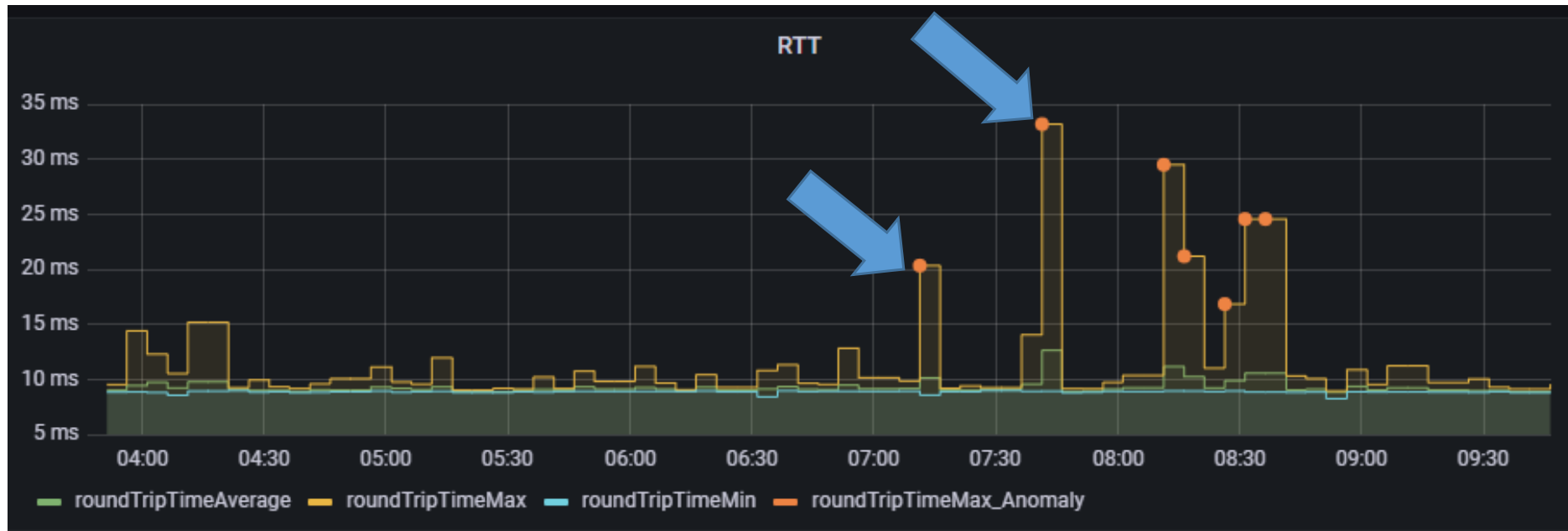
www.geant.org



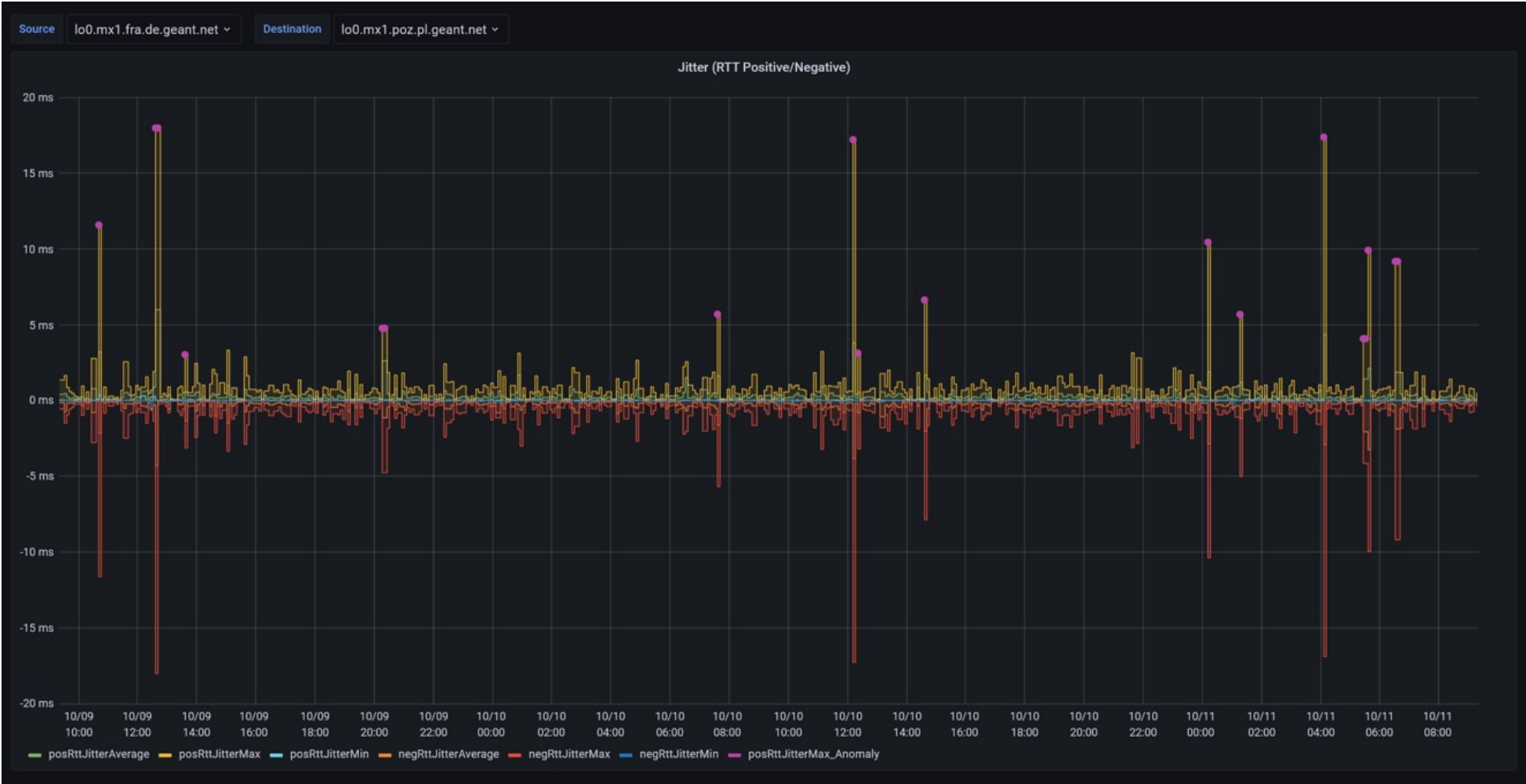
Trends (clocks shifting?)



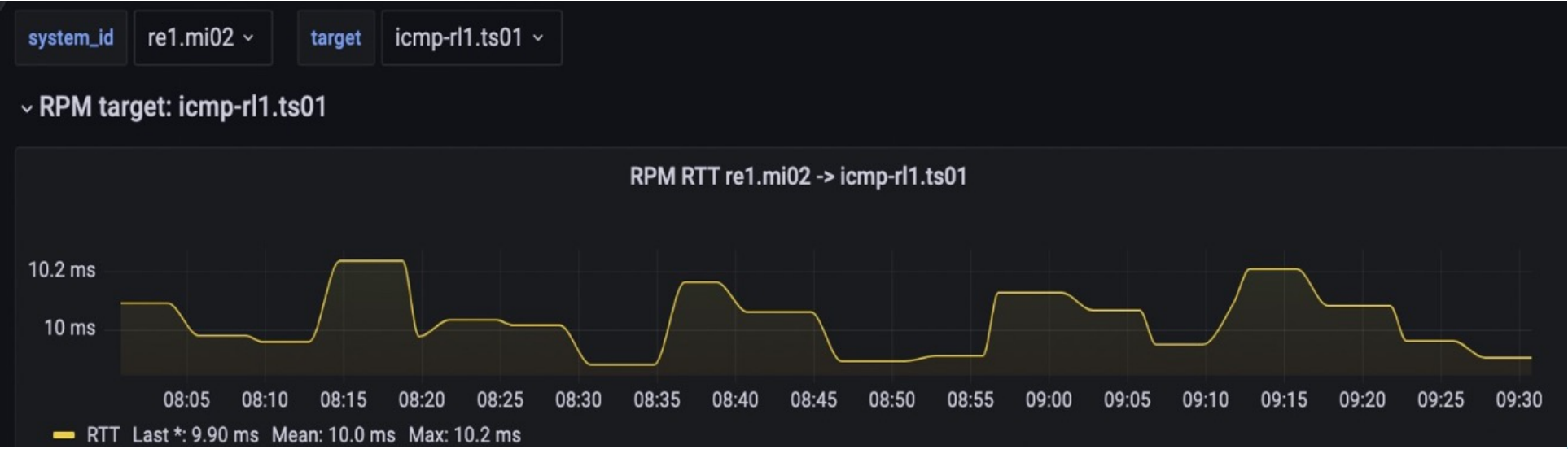
Anomaly Detection (AD) in Timemap



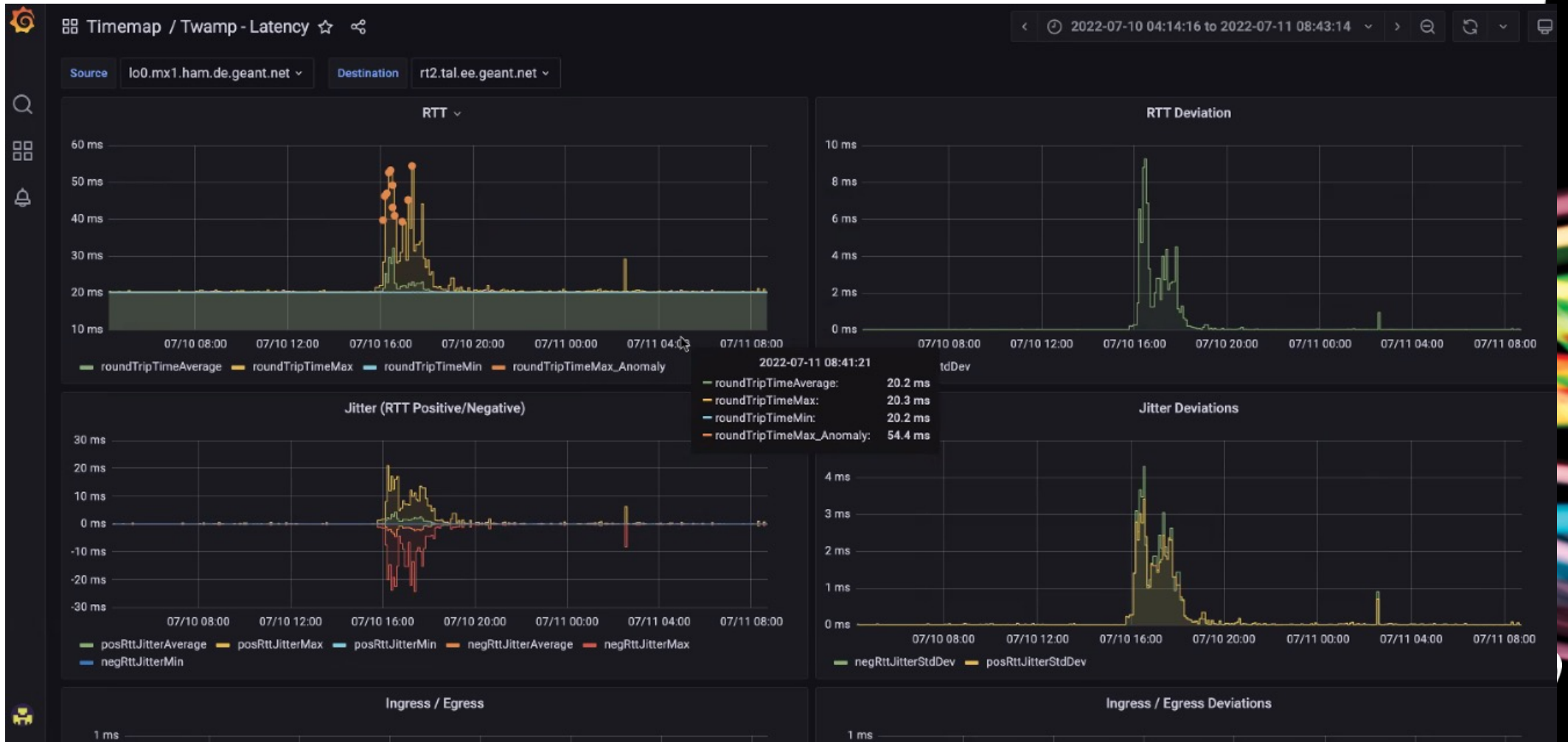
One more plot



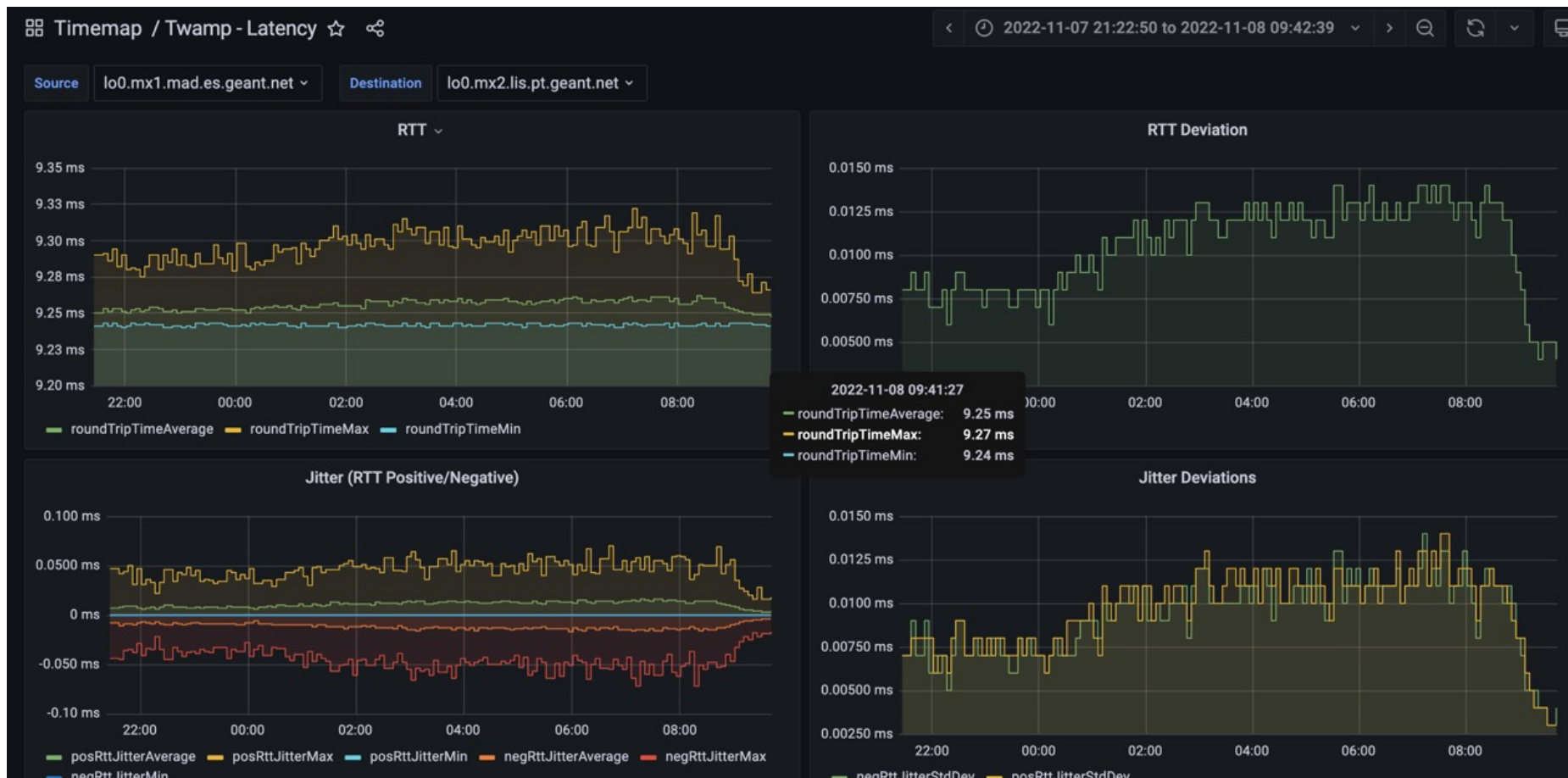
Equal Cost Multipath Protocol (ECMP) effects



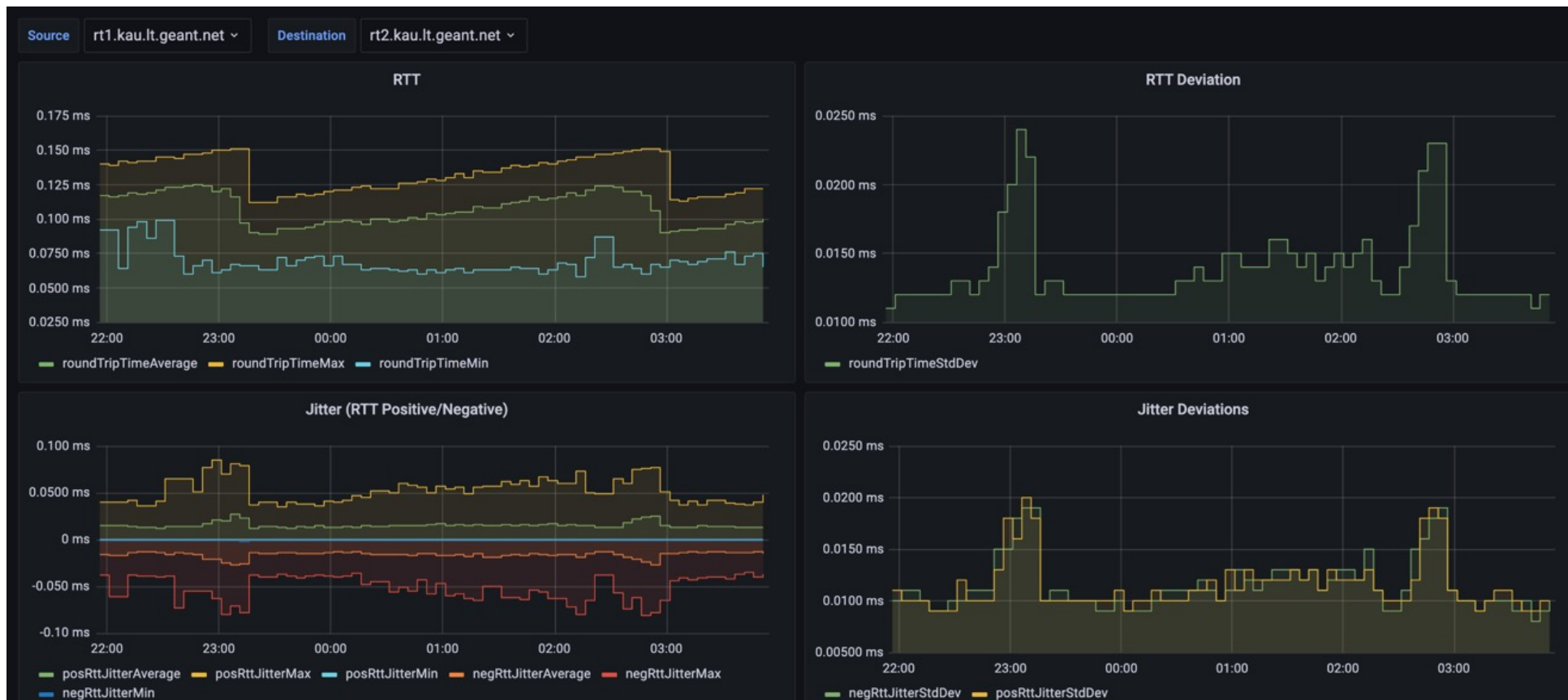
«non-identified event»



«non-identified event»

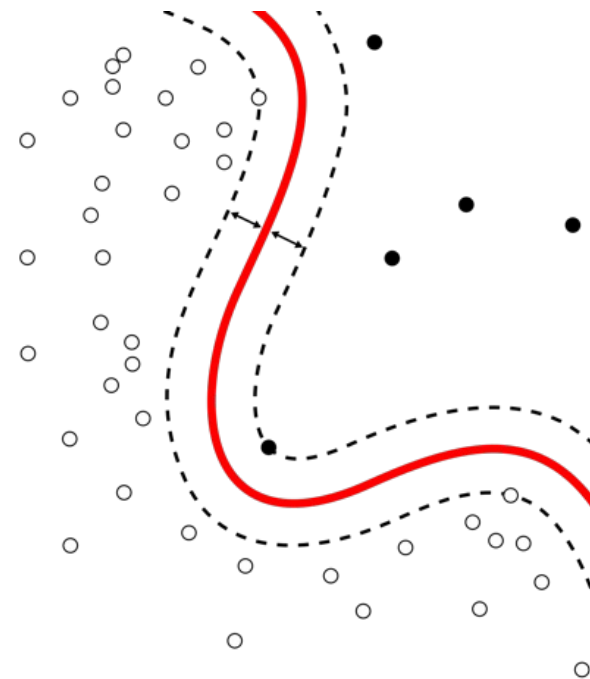


«non-identified event»



The research: Anomaly Detection (AD) in Timemap requirements

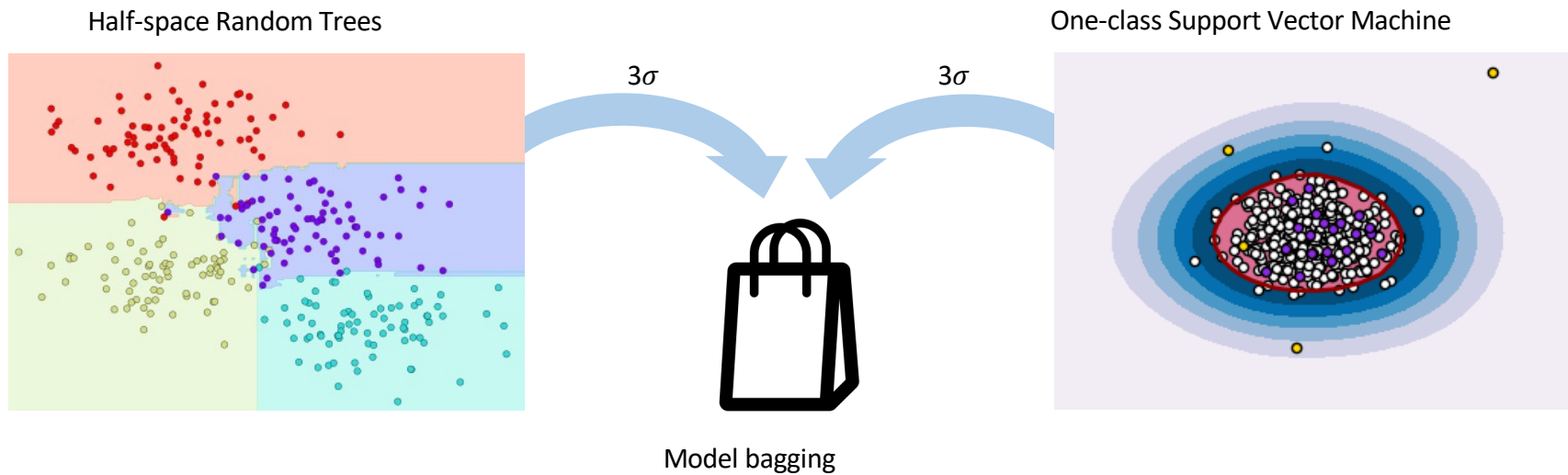
- Move beyond the simple observation
 - AD for Analytics and Alerting
 - Co-occurring events correlation
- Requirements on AD machine learning
 - Real-time or micro-batch learning/inference
 - Robust estimation
 - Light footprint



Anomaly Detection in Timemap – toolset

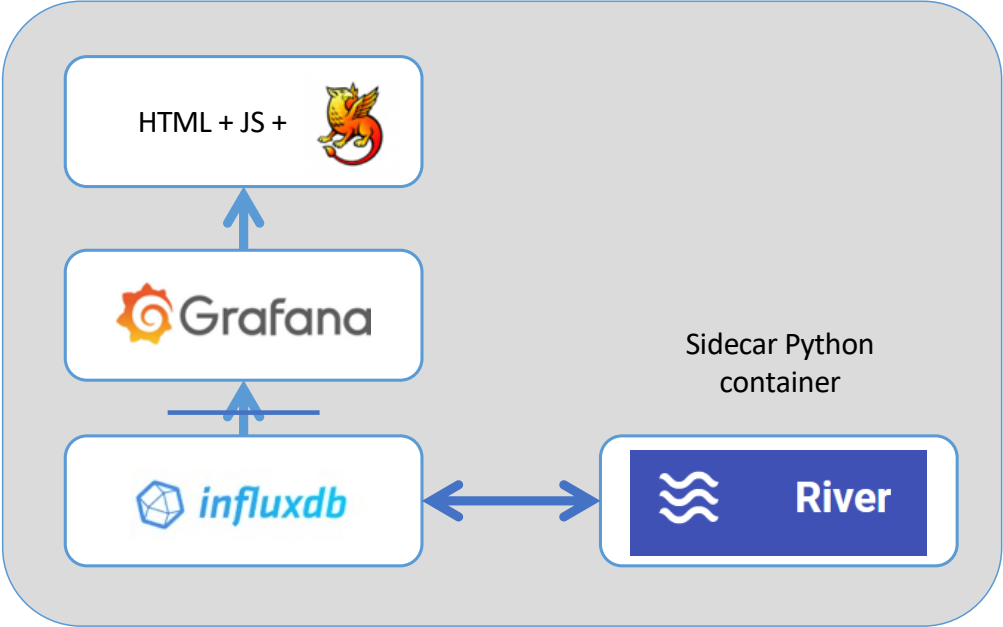
- Anomaly Detection, in short
 - Std.Dev classification
 - Unsupervised
 - Sensible to overfit

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

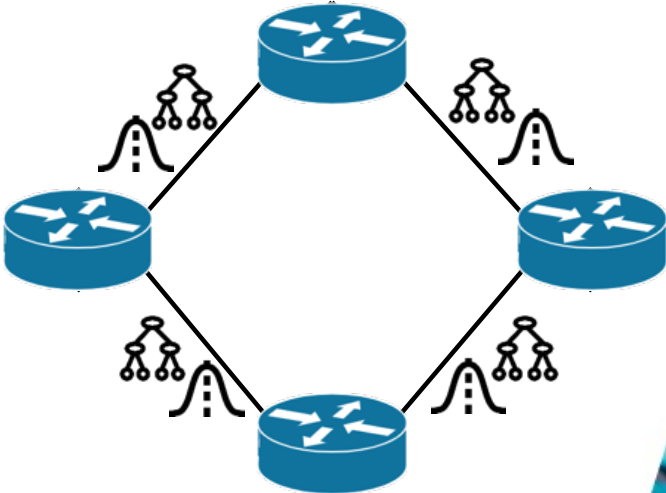


Anomaly Detection in Timemap – architecture

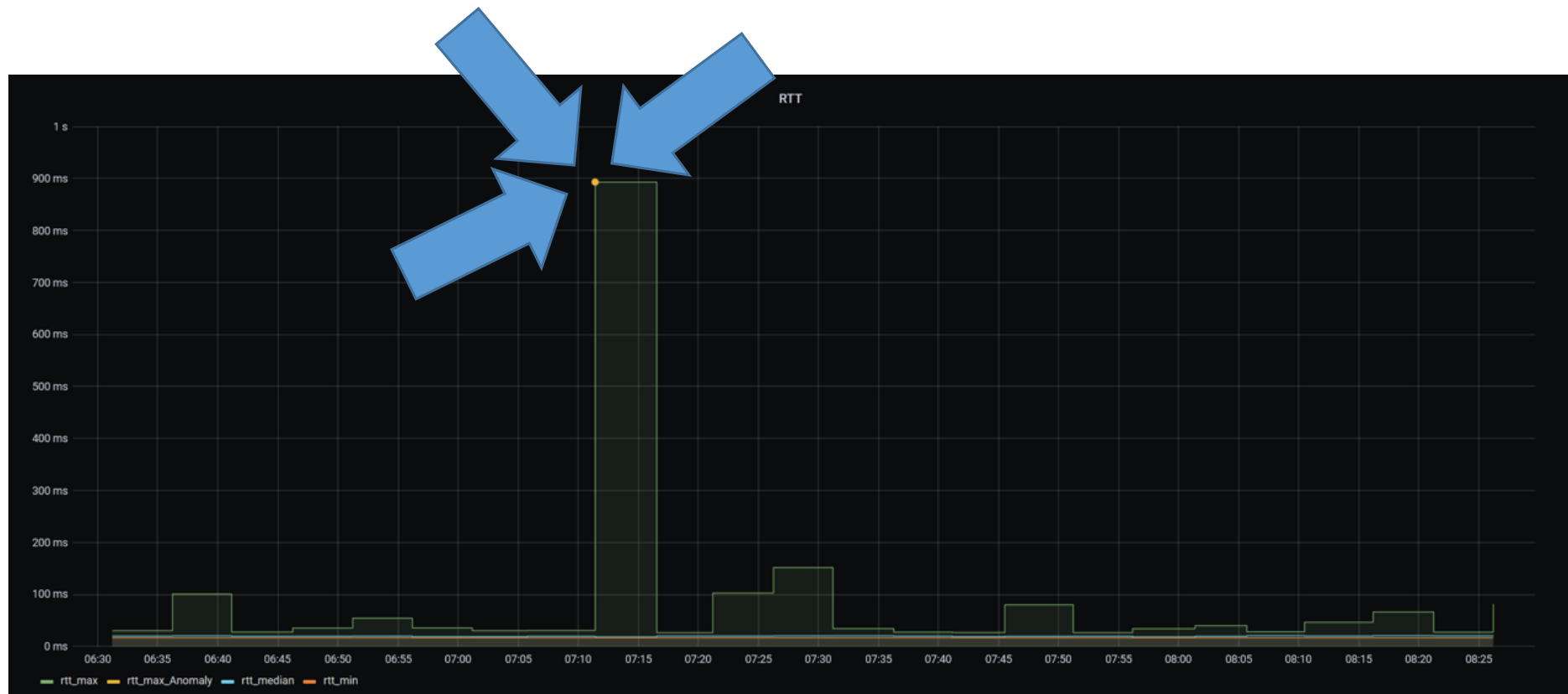
Software architecture extension



Network topology and ML models



Almost the same look and feel



Next steps on Anomaly Detection

- Issues with current models
 - Overfitting and concept drifting
 - Identify when anomalies end
- Explore richer models
 - Signal processing – train filters, anomalies as high frequencies
 - Nowcasting – training models, anomalies as deviations
 - Models selection & hyperparameters optimization
 - And more ...

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>

www.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





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).