https://tnc20.geant.org/submission-guidelines/

# Lightning Talk proposals

**Duration: 5 minutes | Deadline: Monday, March 9**

Lightning Talks focus on one key point. This can be an idea, a successful project, a cautionary story, a collaboration invitation, a quick tip or demonstration. It is an opportunity for ideas to get the attention they deserve, within a maximum of 5 minutes. The clock will be ticking, so get prepared!

All Lightning Talk submissions will be reviewed by the TNC20 Programme Committee and all submitters will be notified in April 2020.

Proposal abstracts should include:

- *Presentation title*
- *Presentation description*
- *Presenter's name and affiliation*
- *Authors names and affiliations (if different from the presenter)*

### Presentation Title:

**Making R&E OSS Network Data Available to Network Researchers**

### Presentation Description:

Considering R&E Networks as instruments that can be used for research purposes by the academic communities, this presentation will enumerate questions and issues to be answered, that are relevant to other members of the community interested in handling similar requests from third-party researchers within the academic community for collecting and making available production Operations Support Systems (OSS) and related data from their networks for research purposes.

Network operators in the GÉANT and NREN community will gather a wide range of data within their Operations Support Systems (OSS). This data may typically be used to monitor the status and availability of systems, to troubleshoot issues on the network, to support security investigations, or to evaluate network performance. But increasingly, operators, including NRENs and campus teams, are also being asked for access to such data by network researchers interested in evaluating their research work against real network data.

The main goal of this talk will be to ask how National Research and Education Networks (NRENs) and other network operators within the community can support requests from third-party researchers within the academic community for collecting and making available production OSS and related data from their networks for research purposes.

The talk will explore what can be done in technical operational aspects around how to collect, organise, anonymise and share data for research purposes. It will consider use open standards, best practices and the tools available, and in terms of design discuss what additional supporting infrastructure may be required.

The potential research interests are themselves broad. Some may lie with classic OSS data, e.g., applying machine learning to predict component failures based on observed data, some may wish to explore specific details of routing protocols or routing policies, and others perhaps data related to network flows and network performance.

Considering NRENs as instruments that can be used for research purposes by the academic communities, the talk will seek to bring together NREN operators and other members of the community interested in handling similar requests to discuss how to respond to questions like:

- What data do we already collect in our OSS? What additional data might researchers want access to?

- What can we as operators deduce from this data, for our own performance monitoring and troubleshooting? How might the outputs of network research help us in the future?

- What are the issues around sharing this data with third parties, especially network researchers, but also other NREN operators for cases of international multi-domain network (performance) troubleshooting.

- Considering advanced NRENs networks as instruments for CS scientific domain – how does your NREN support your researchers today?

- How can network traffic, topology datasets, etc. collected and made available for researchers in the computer networking field? Are there existing best practices to be followed?

- Should (N)RENs publish their data in open data repositories?

- What kind of network data can be open and, at the same time, still be valuable for networking researchers without compromising operations security or user privacy (e.g.: considering recent GDPR regulations)?

- How can network-related data be shared (and to what level of detail) with networking researchers without compromising operations security or user privacy, considering theGDPR regulations, even if NDAs are being used?

- Which kind of anonymisation can or should be applied to sensitive data without compromising research objectives? What can be learnt from experts in the privacy field?

**Presenter's name and affiliation:**

Alex Moura - RNP - www.rnp.br/en

## Abstract

RNP, the Brazilian NREN started a new project to design and deploy a new platform with automated operation features following DevOps practices with safe, reliable, robust, resilient components and systems to collect, anonymize, organize, store and share OSS network data from the academic network with third-party researchers and internal teams engineering, security and operations teams.

Every year RNP's Technical Committee for Network Measurements presents recommendations to improve RNP measurements and to support national research on networks using the network OSS data. The implementation of the recommendations is hampered by a lack of infrastructure and internal processes to support the operationalization for the deployment of new data collection methods, and data organization and sharing.

The new project intends to design, develop and deploy a new infrastructure platform to collect data using methods to reduce implementation costs through orchestration and automation of installation and configuration of components. Another objective of the project is  that the operation should be as automated as possible, looking for the lowest possible OPEX costs in the medium and long term, so the platform will have the lowest cost and the lowest possible impact for operations teams.

Simplified description
Design and implement a platform with a reliable, robust, resilient and secure architecture and automated operation to deploy an open service to share network OSS datasets to support scientific research and innovation by leveraging OSS network data.

**Some assumptions to be considered when designing the new project**
• Access to data should always be monitored and accounted for (i.e., logs of all accesses and download counts)

• Access to some types of data must have access control and be released only upon request and NDA authorization signed by the applicant.

• Some types of data must be anonymized before being made available for access by external users

• Open network measurement data to be made available in the federated repository should have automated deployment and operation, in order to minimize the operational impact and costs for curation and publication;

• Operations issues and alarms should automatically open trouble tickets and there must be automation for basic troubleshooting and data collection, and everything must be attached to the ticket to speed up the analysis and improve the resolution time of the problem.

**What has been done so far**
The project was approved in late December 2019 to select a workgroup from the academic community for a 12 month development period. By the time of this lightning talk proposal, it's being developed the call for proposals to select a workgroup from the academic community to select the team that will work on the development of the project's objectives.
By the time of the presentation of the lightning talk, the project will have a workgroup selected and working on the project's development, and define the deliverables, work packages, architecture, components, tools, and development methods.

**What's in the roadmap**

The team shall deliver a working prototype and a proof-of-concept in the first months of the project. In the final months of the project, the workgroup should deliver a working solution to deliver the first open OSS network datasets for research.