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

**Submit new proposal**

**BoF (Birds of a Feather meeting - 2 hours)**

For TNC20 we will only offer a limited number of slots for small 2-hour meetings (BoFs). The bigger \*\*side\*\* \*meetings\* that usually take place during TNC will be selected beforehand and the organisers of these meetings will be notified by us.\* Good to know: The BoFs will take place on Tuesday June 9 from 8:30 - 10:30 and Thursday June 11 from 18:00 – 20:00. This is in the evening of the last conference day. All requests for a BoF will be handled as a 2-hour meeting. Only TNC participants may enter the venue to attend the BoF meeting. The following criteria for evaluation will also be applied: Submission for an interactive meeting and not a presentation for the main programme. Submission with a clearly identified audience that will be attending TNC20. Submission complete and including all the requested information.

**Title\***

**Please fill out the official name of the BoF.**

Making your OSS Network Data Available to Network Researchers

**Proposer names and affiliations\***

* Alex Soares de Moura - RNP
* Tim Chown - Jisc
* Ivana Golub - PSNC
* Pavle Vuletić - AMRES

**Meeting description\***

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 BoF will be to discuss how National Research and Education Networks (NRENs) and other network operators within the community can support requests from 3rd party researchers within the academic community for collecting and making available production OSS and related data from their networks for research purposes.

The BoF 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 BoF 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?

**Intended audience\***

NREN and campus network operators (NOCs), network managers and engineers, (academic) network researchers, GDPR and privacy researchers and specialists,  Science Engagement specialists.

**Estimated number of attendees\***

Around 20 people

**Open or Closed meeting?\***

Open meeting

**Is the meeting open to all participants or on invitation only?**

Meeting open to all participants

**Technical requests**

Notebook, TV screen or projector to display slides to the audience. If possible (not a strong requirement), a second TV screen or projector to display interactive polls and interact with the audience.

**Video Conferencing**

If possible, to have remote participants interested in the BoF topics

**Whiteboard / flipchart**

None

**Projector and screen**

Yes, please

**Organisers are being asked to bring their own laptops**

Yes

**Meeting format\***

Auditorium Style, U-Shape Style, School

**Any other comments**

**References**

**Workshop on Network Management and Monitoring - public - GÉANT federated confluence**

https://wiki.geant.org/display/PUB/Workshop+on+Network+Management+and+Monitoring

**18th STF - Copenhagen, October 2019 - GEANT APM - GÉANT federated confluence**

https://wiki.geant.org/display/APM/18th+STF+-+Copenhagen%2C+October+2019#id-18thSTF-Copenhagen,October2019-agenda

**Systems Anonymization of Network Traces Using Differential Privacy** - Ahmed Aleroud - RIPE74

<https://ripe74.ripe.net/archives/video/73/>

**SNAS - Linux Foundation**

<https://www.snas.io/>

**Why you need 'Network Error Logging' (NEL)**

https://www.uriports.com/blog/network-error-logging/