Alexander Männel, Jonas Mücke, kc Claffy, Max Gao, Ricky Mok, Marcin Nawrocki, Thomas C. Schmidt, Matthias Wählisch

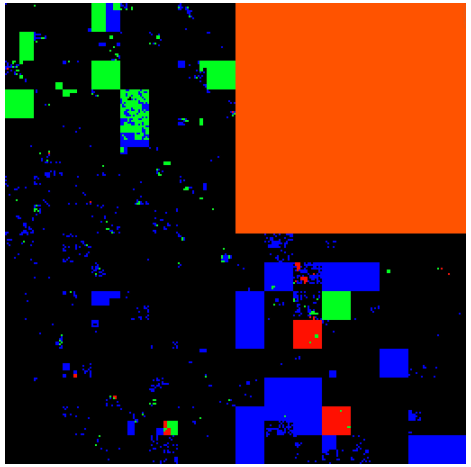
Understanding and Monitoring the Data Collected by the UCSD-NT

GMI-AIMS-5 Workshop, CAIDA/UCSD // February 10-14, 2025

Contact: alexander.maennel@tu-dresden.de

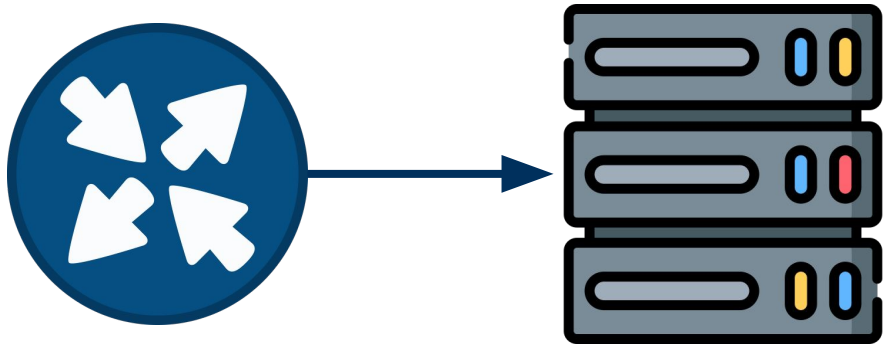
A Network Telescope consists of …

Address space



+

Infrastructure

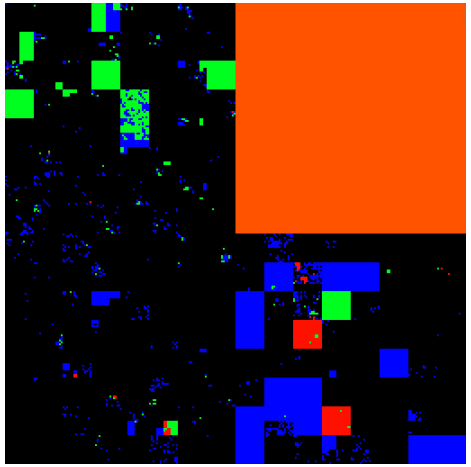


Capturing

Recording + Storage

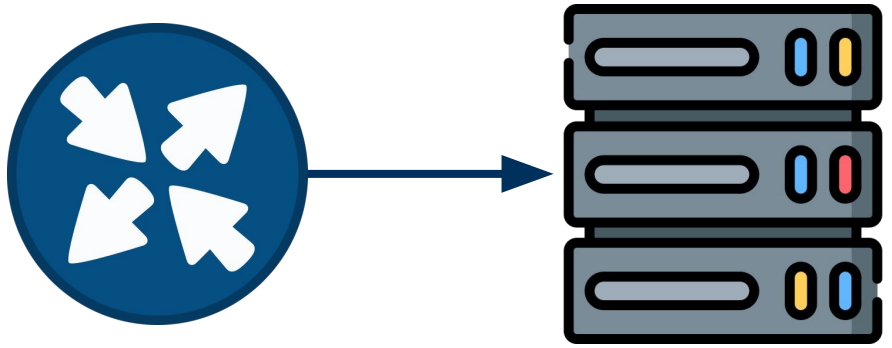
A Network Telescope consists of …

Address space



+

Infrastructure

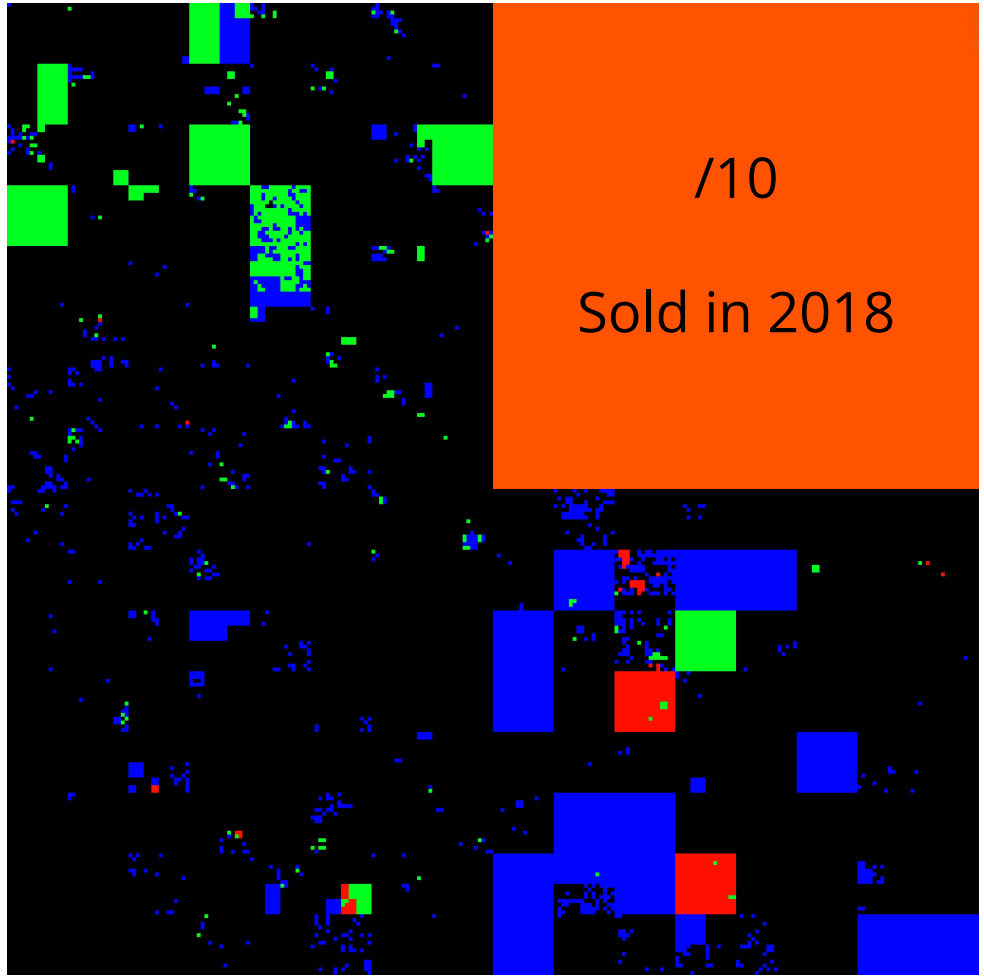


Capturing

Recording + Storage

Both building blocks introduce their own (operational) challenges, which we need to solve to ensure that the data set is complete.

The address space of the UCSD-NT is dynamic



Not all traffic received by the capturing infrastructure is intended for the UCSD-NT.

UCSD-NT deploys filter lists to exclude traffic.

Telescope address, Filtered address

… and some traffic is never delivered to the UCSD-NT capturing infrastructure:

Legitimate more-specific BGP announcement

Illegitimate more-specific BGP announcement

The address space of the UCSD-NT is dynamic

We now illustrate the impact of the filter list on telescope data.

Not all traffic received by the capturing infrastructure is intended for the UCSD-NT.

UCSD-NT deploys filter lists to exclude traffic.

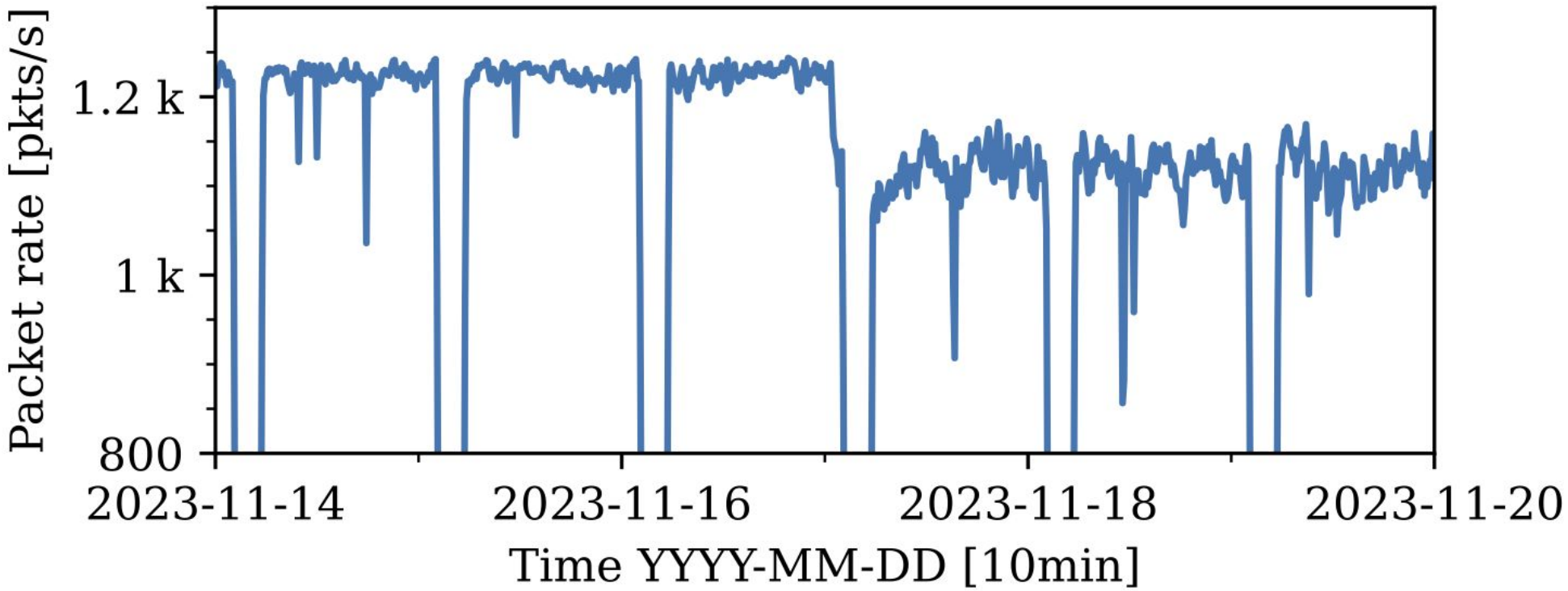
Telescope address, Filtered address

… and some traffic is never delivered to the UCSD-NT capturing infrastructure:

Legitimate more-specific BGP announcement

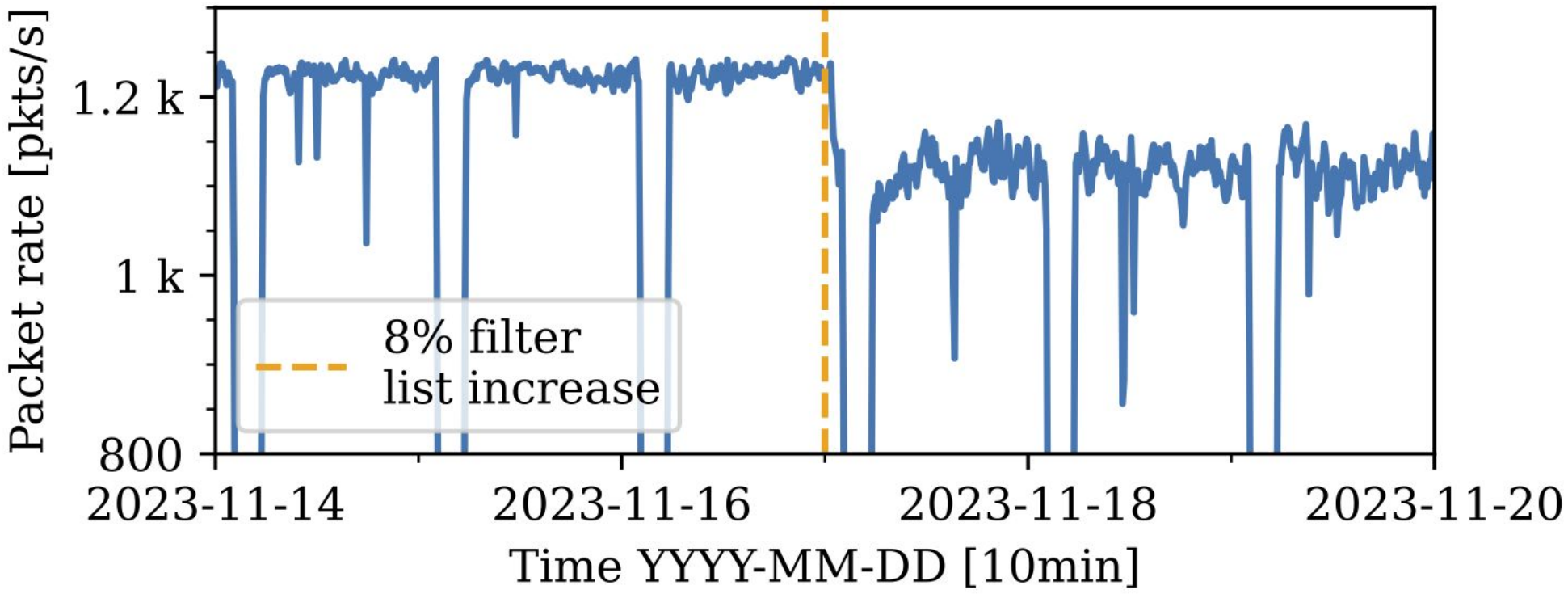
Illegitimate more-specific BGP announcement

IBR traffic at UCSD-NT is declining …



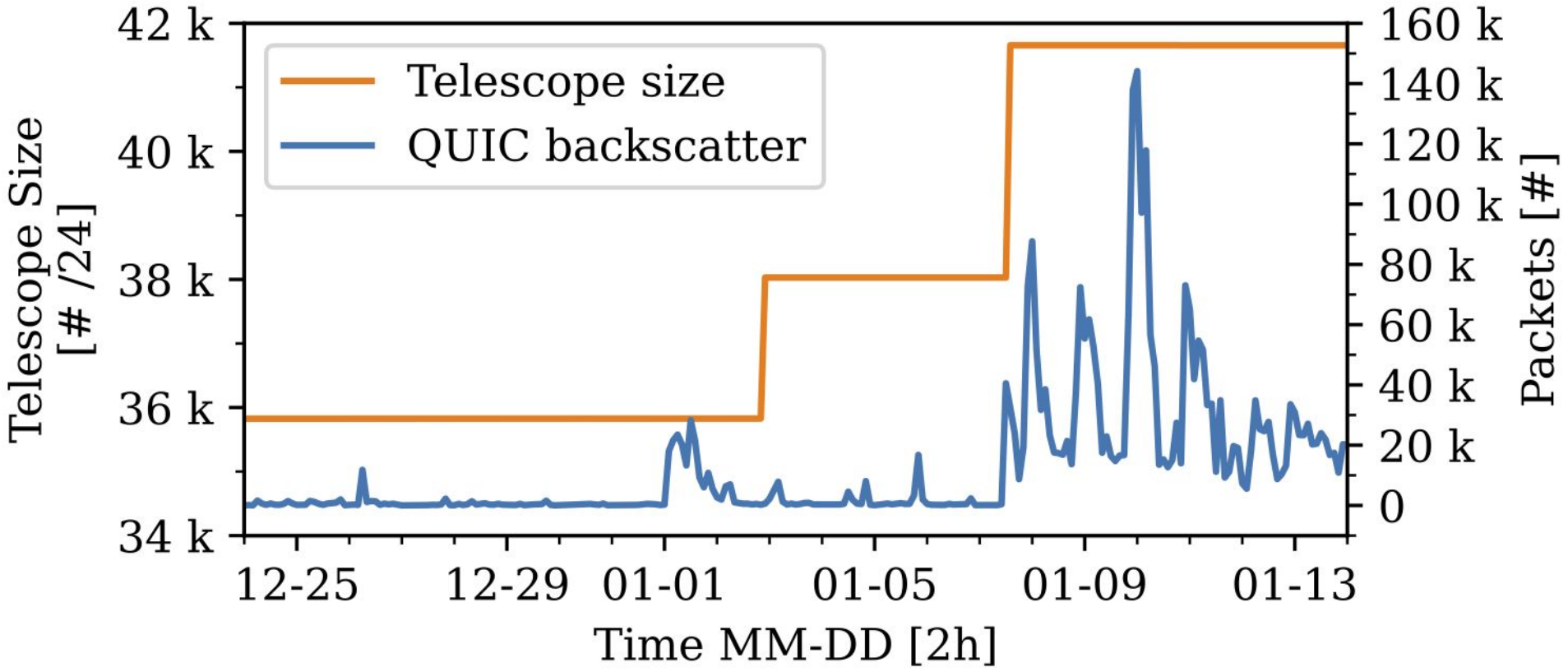
Packet rate of a measurement project targeting telescope address space.

IBR traffic at UCSD-NT is declining … because prefixes were added to the filter list, not because IBR traffic changed in the Internet



Packet rate of a measurement project targeting telescope address space.

QUIC backscatter traffic recorded by the telescope does not only depend on the telescope size but also on the subnets part of the filter list

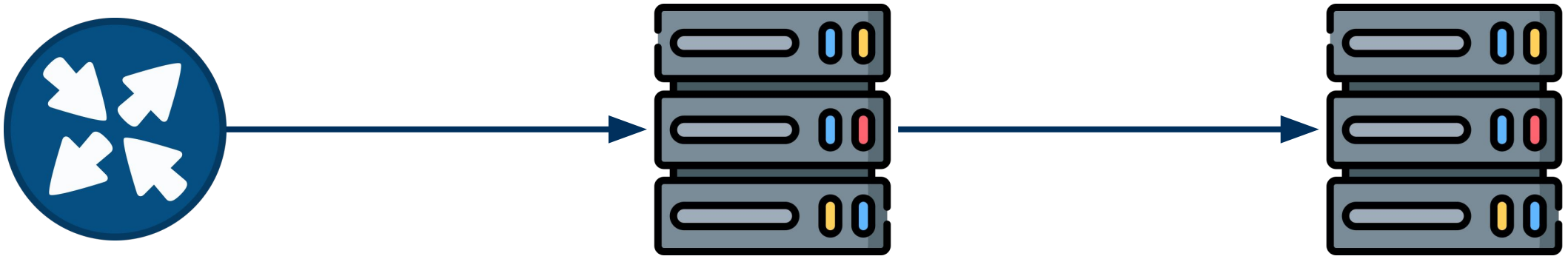


QUIC backscatter is localized, so when specific prefixes get added or removed, traffic patterns change drastically.

If you want to understand what you see in the UCSD-NT data set, **you should consider the filter list**, too.*

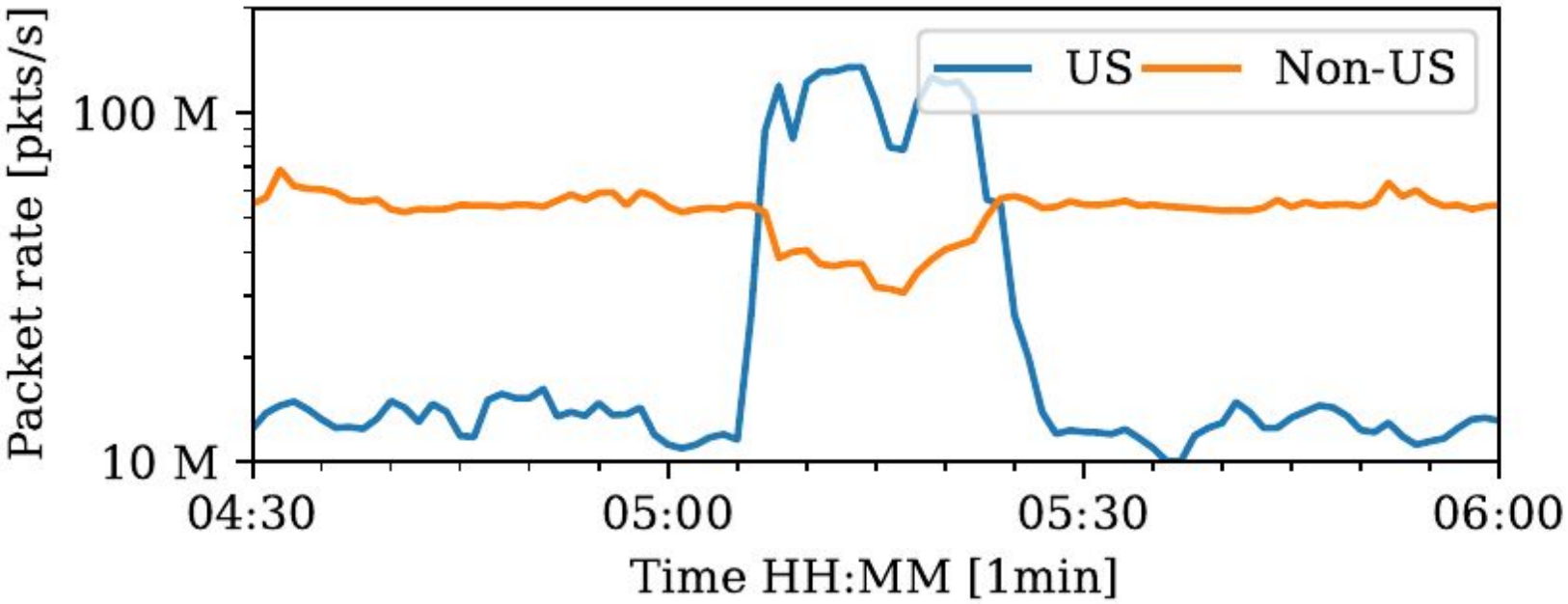
*specifically important in time-series analysis

The Infrastructure of the UCSD-NT

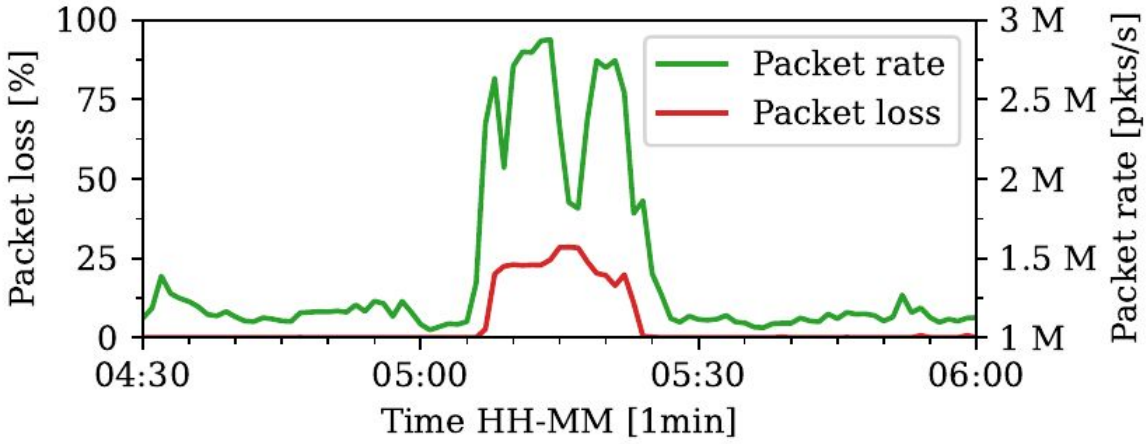


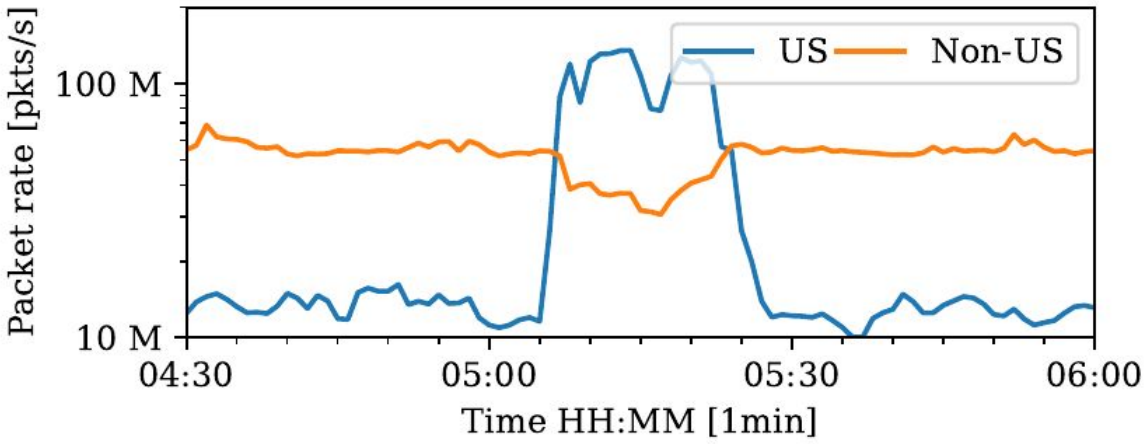
Issues can arise at different positions in the data processing pipeline. Depending on that position, **they manifest in different ways.**

Non-US sources show less activity during large scans from US …



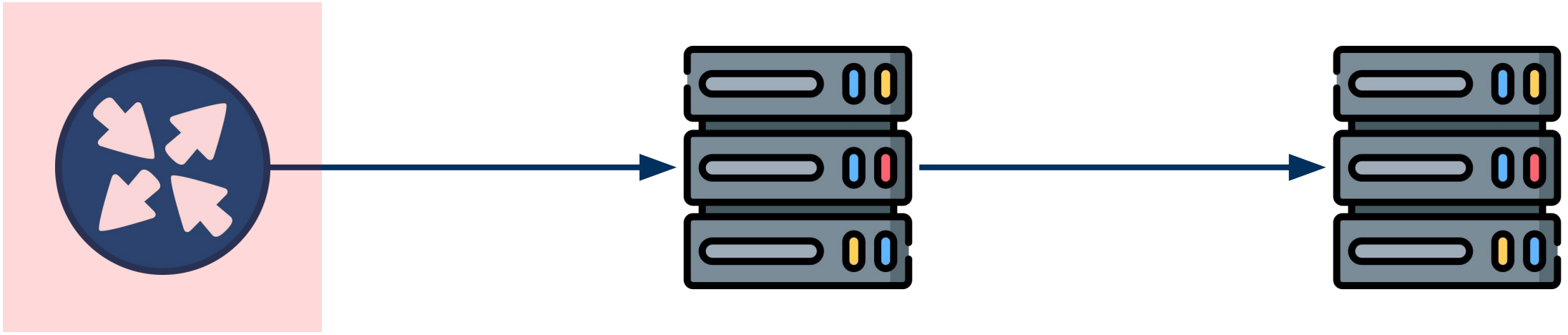
Non-US sources show less activity during large scans from US … because their packets get lost during peak traffic.





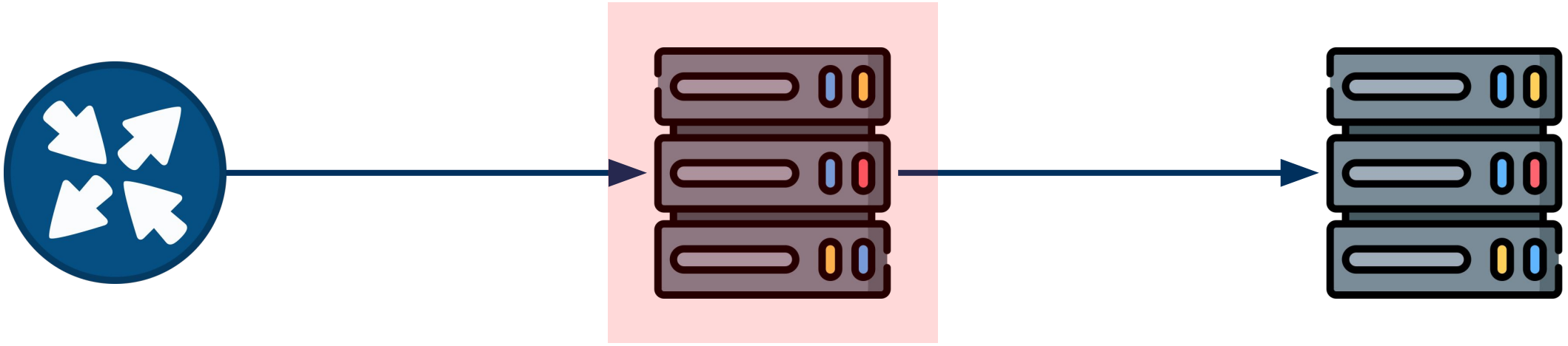
As the packet loss is distributed uniformly, **aggregates not directly connected to the peak traffic are impacted as well.**

The Infrastructure of the UCSD-NT



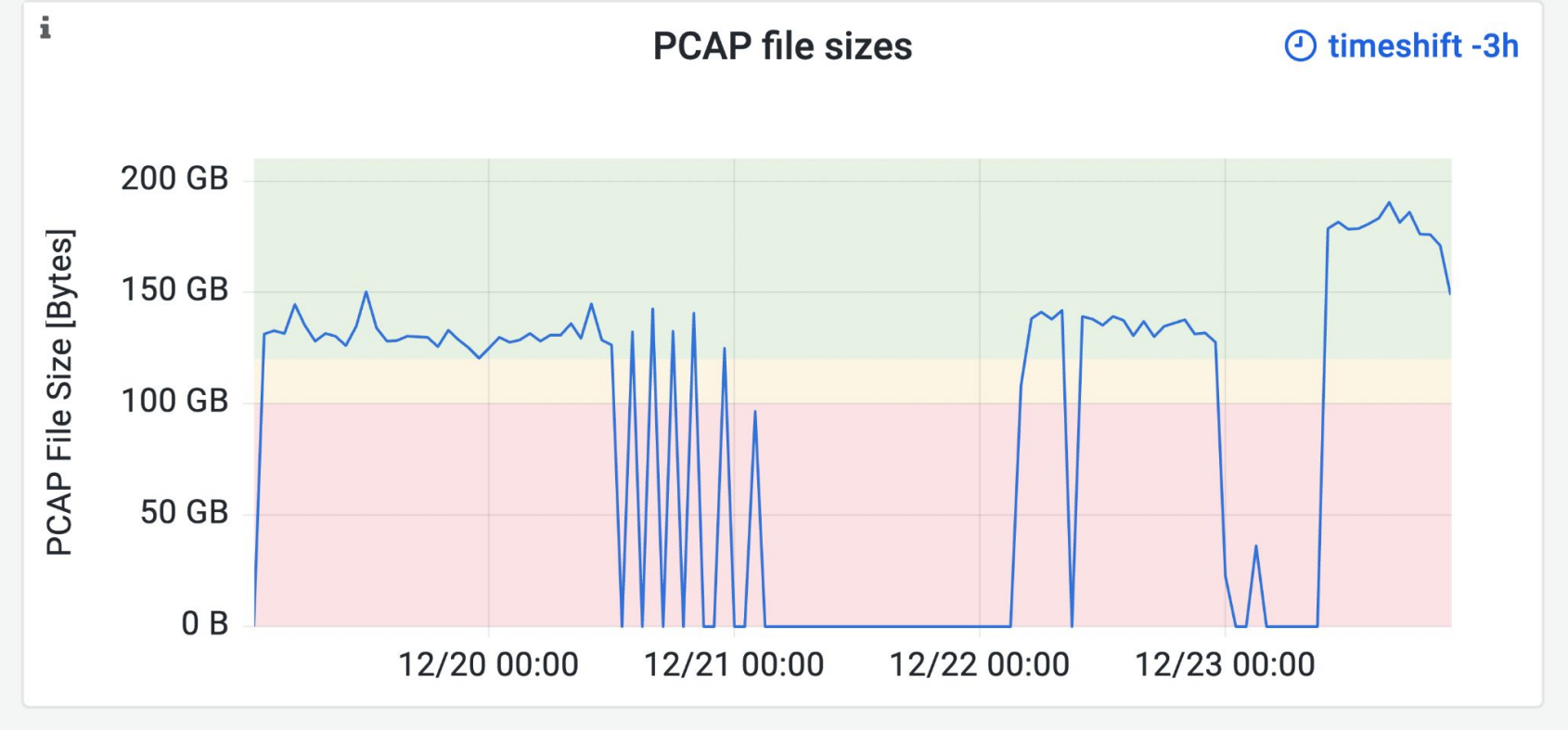
You can overload the capturing device because network card buffers are full.

The Infrastructure of the UCSD-NT



Issues can arise at different positions in the data processing pipeline. Depending on that position, **they manifest in different ways.**

Exhaustion of system resources



Recording software can run out of system resources, **causing complete loss of data dumps until the process recovers.**

Monitoring of the UCSD-NT: Data sources

We need to **measure reachability via data and control plane**, as well as **system resources.** The following measures are currently deployed at the UCSD-NT:

ARCHIPELAGO

alpha strike labs by Limes Security

leitwert

Establishing ground truth by controlled scanning of the network telescope (data plane)

RIPE NCC

Monitoring of the visibility of the telescope in BGP using RIPE RIS (control plane)

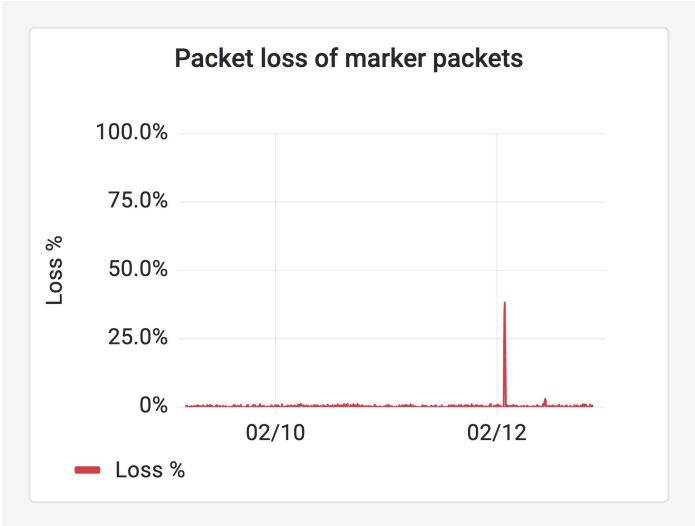
A R | D C

AMATEUR RADIO DIGITAL COMMUNICATIONS

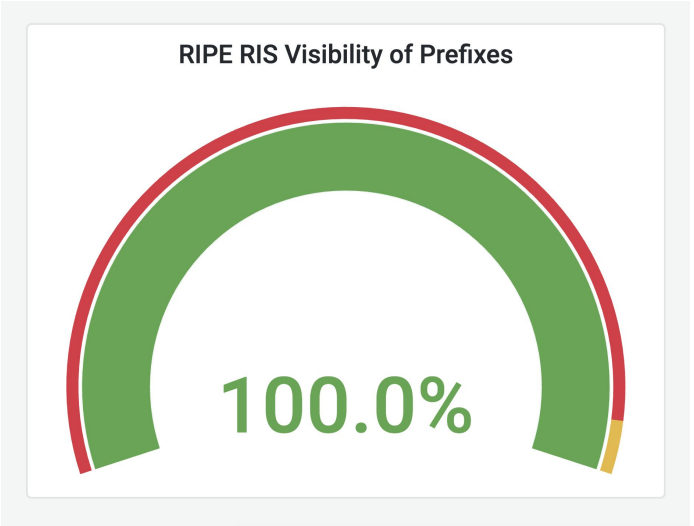
Monitoring and validation of the filtering setup

Monitoring of the UCSD-NT: Implementation

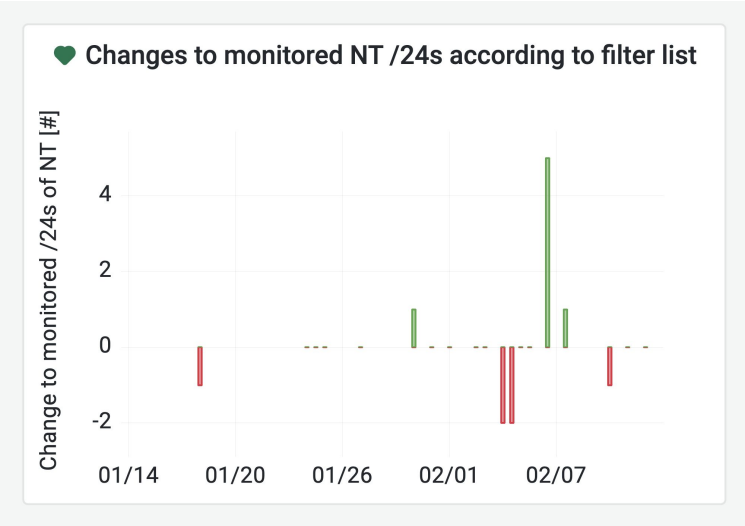
We need to **measure reachability via data and control plane**, as well as **system resources.** The following measures are currently deployed at the UCSD-NT:



Establishing ground truth by controlled scanning of the network telescope (data plane)



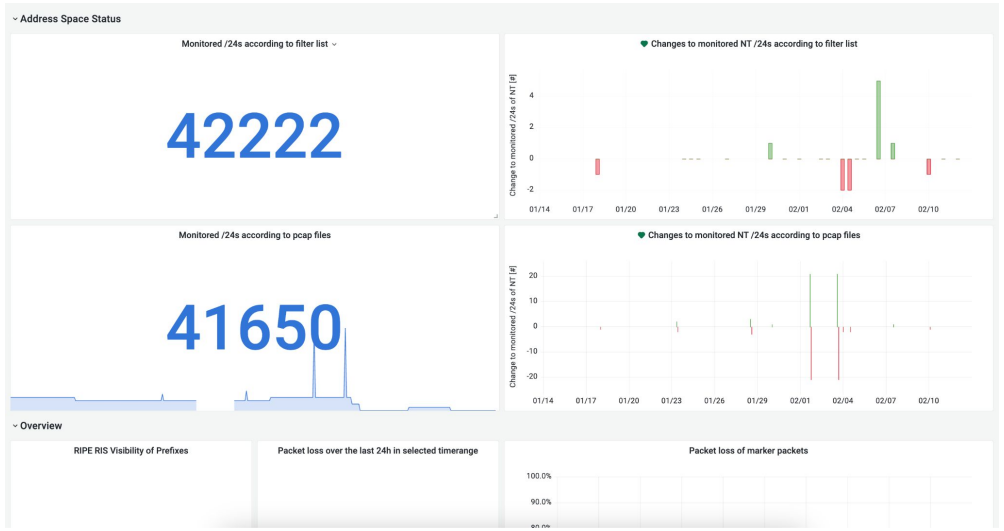
Monitoring of the visibility of the telescope in BGP using RIPE RIS (control plane)



Monitoring and validation of the filtering setup

Monitoring of the UCSD-NT: Dashboards and notification channels

Monitoring requires not only visualization but also alerting to be effective.



Grafana Dashboard showing current values and deltas

Notification to key ops persons via Mattermost

Monitoring of the UCSD-NT: Future work

Extend validation of reachability of the UCSD-NT by probing UCSD routers from Ark and RIPE Atlas.

Monitor the effect of changes in BGP on the telescope data set.