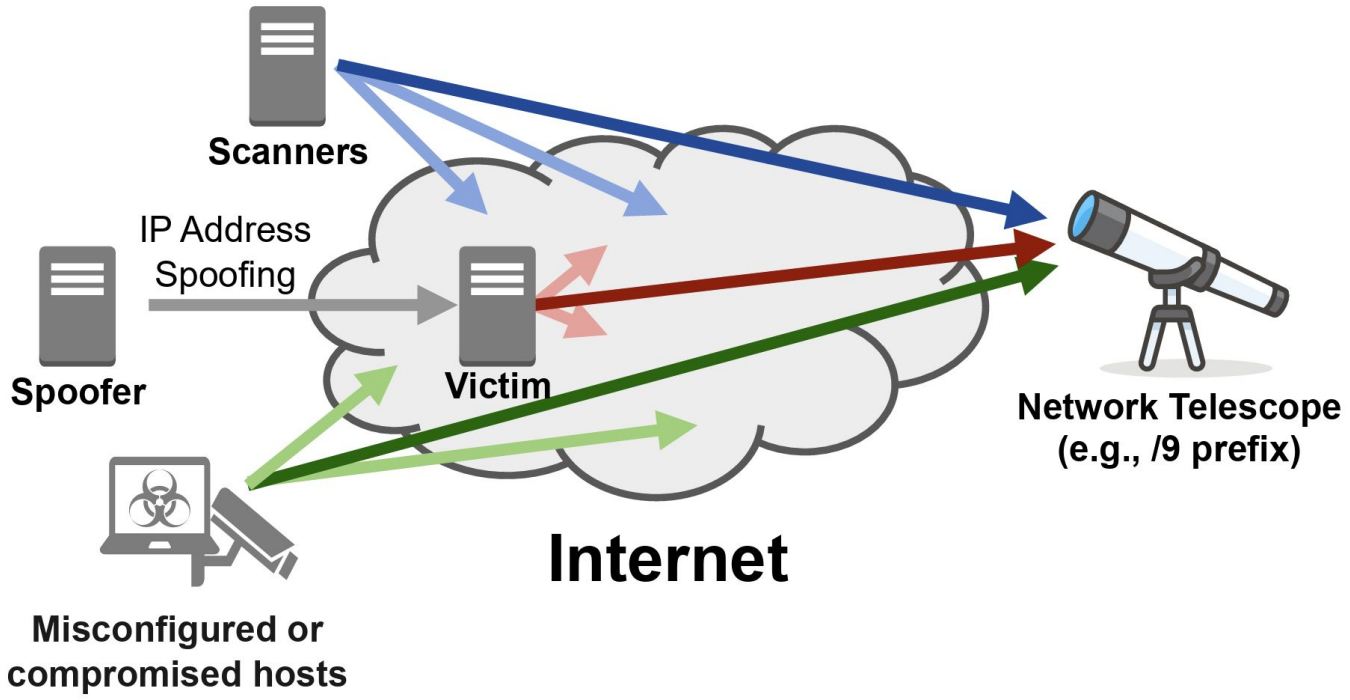
Alexander Männel, Jonas Mücke, kc Claffy, Max Gao, Ricky K. P. Mok, Marcin Nawrocki, Thomas C. Schmidt, Matthias Wählisch

Lessons Learned from Operating a Large Network Telescope

ACM SIGCOMM 2025, Coimbra, Portugal // September 10, 2025

What is a Network Telescope?

A measurement instrument to collect unsolicited Internet traffic.



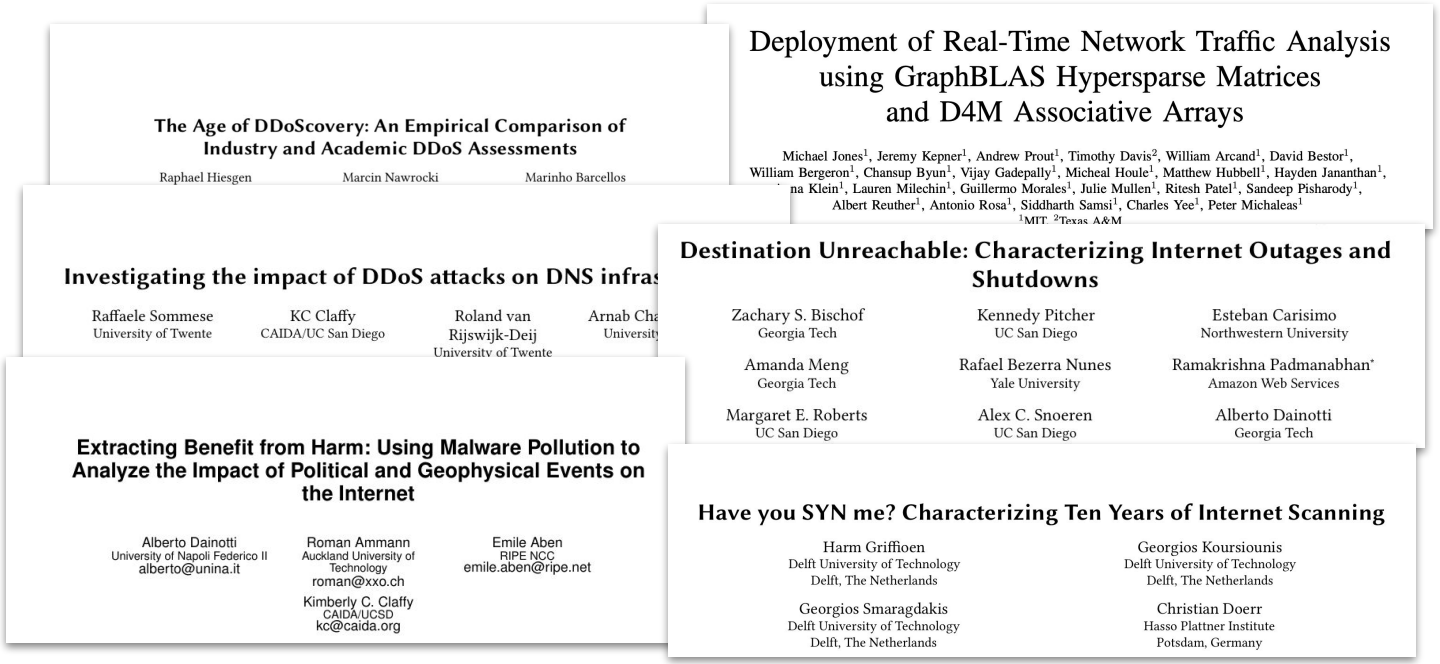
Unsolicited Internet Traffic (**I**nternet **B**ackground **R**adiation) contains:

- **Scanning**: malicious and benign
- **Backscatter**: Responses to spoofed packets
- **Misconfigured or compromised devices**

Network **T**elescopes collect IBR by storing all packets sent to unused IP address space.

We focus on IPv4 Telescopes in this work.

Network telescopes are relevant in research and practice.



[ACM SIGCOMM, ACM IMC, ACM CoNEXT, ...]

Network Telescopes have been highly relevant both in research and industry over the last 10 years.

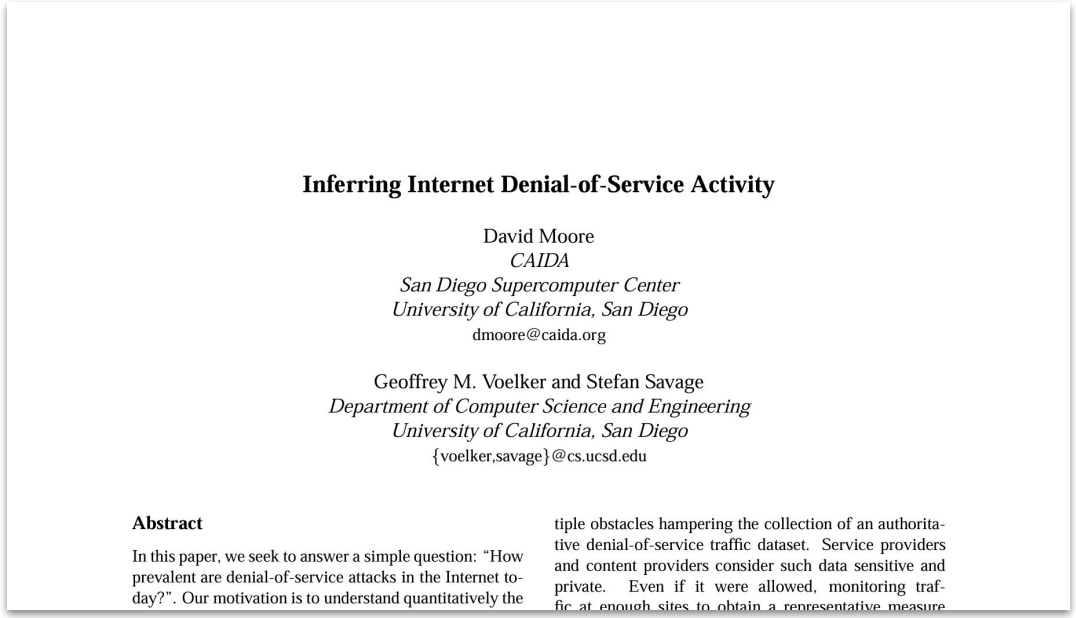
Telescope data is used to answer questions about cybersecurity, censorship, +++

Due to the challenges they face, only a handful of network telescopes exist.

Data integrity is highly important for accurate research.

In our work, we perform validation of the UCSD Network Telescope.

UCSD - Network Telescope



Inferring Internet Denial-of-Service Activity

David Moore
CAIDA
San Diego Supercomputer Center
University of California, San Diego
dmoore@caida.org

Geoffrey M. Voelker and Stefan Savage
Department of Computer Science and Engineering
University of California, San Diego
{voelker,savage}@cs.ucsd.edu

Abstract

In this paper, we seek to answer a simple question: "How prevalent are denial-of-service attacks in the Internet today?". Our motivation is to understand quantitatively the

tiple obstacles hampering the collection of an authoritative denial-of-service traffic dataset. Service providers and content providers consider such data sensitive and private. Even if it were allowed, monitoring traffic at enough sites to obtain a representative measure

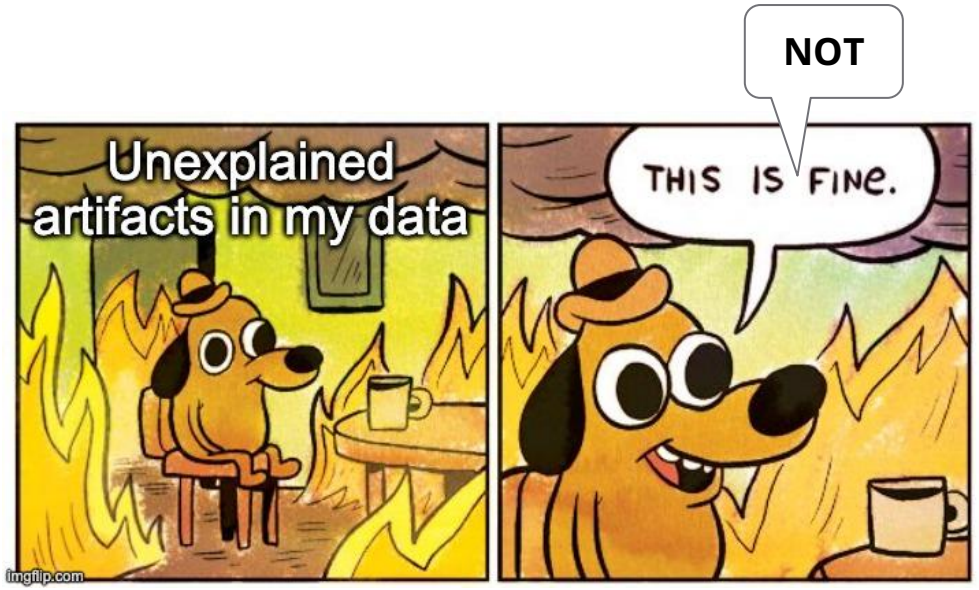
David Moore, Geoffrey M. Voelker, and Stefan Savage. 2001. Inferring Internet Denial-of-Service Activity. In Proc. of the 10th USENIX Security Symposium (USENIX Sec'01). USENIX, Berkeley, CA, USA, 9–22.

The UCSD-NT is the **largest publicly known Network Telescope** currently in operation.

It is operated by CAIDA at UCSD and has been in continuous operation since 2001.

The telescope utilizes the Class A block allocated as AMPRNet and UCSD provides upstream since the 1990s.

Goals of this work



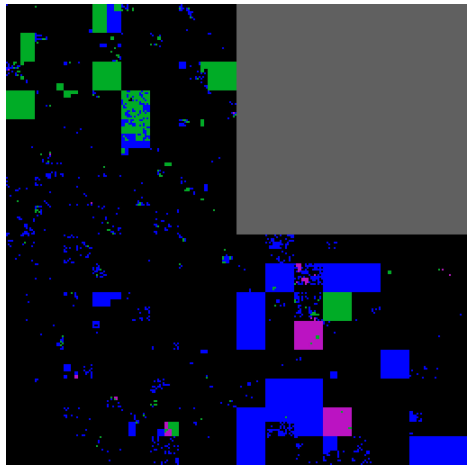
To ensure that conclusions and results drawn from traffic collected by Network Telescopes **are correct**, we need to understand:

1. **what traffic does (but should not) or does not (but should) reach the data set.**

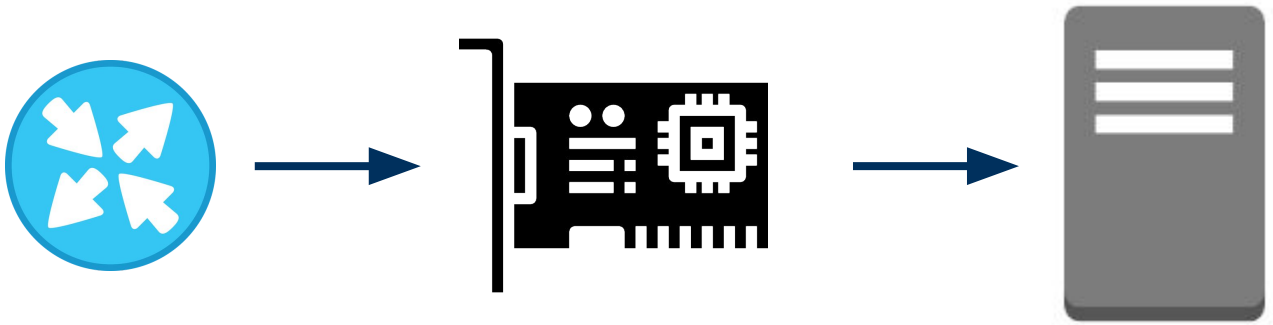
2. **how the operational state of a telescope impacts the telescope data set.**

Components of a Network Telescope

Address space



Infrastructure



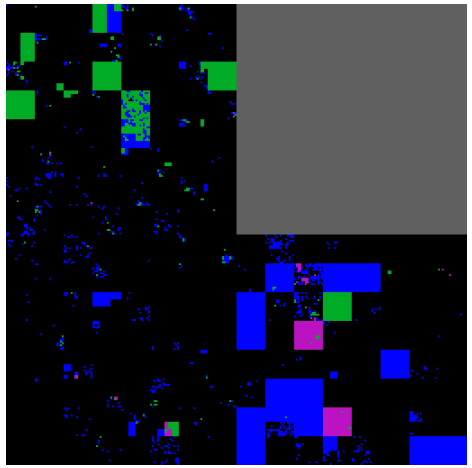
Receiving

Capturing

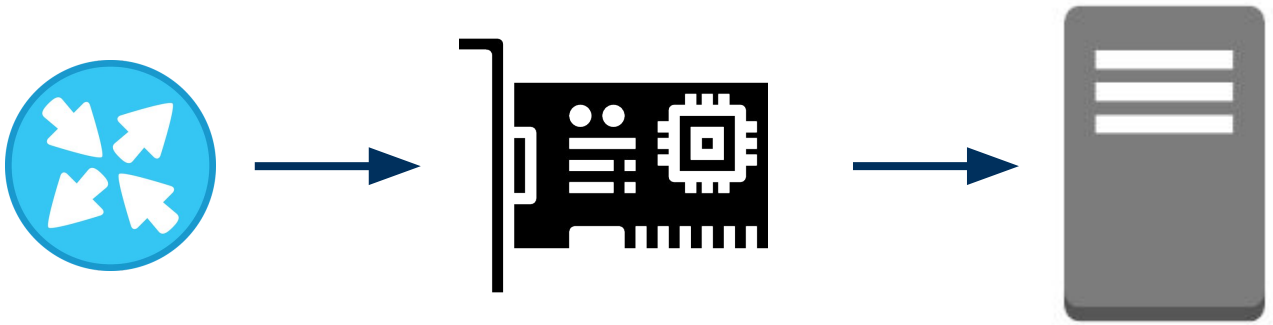
Recording + Storage

Components of a Network Telescope

Address space



Infrastructure

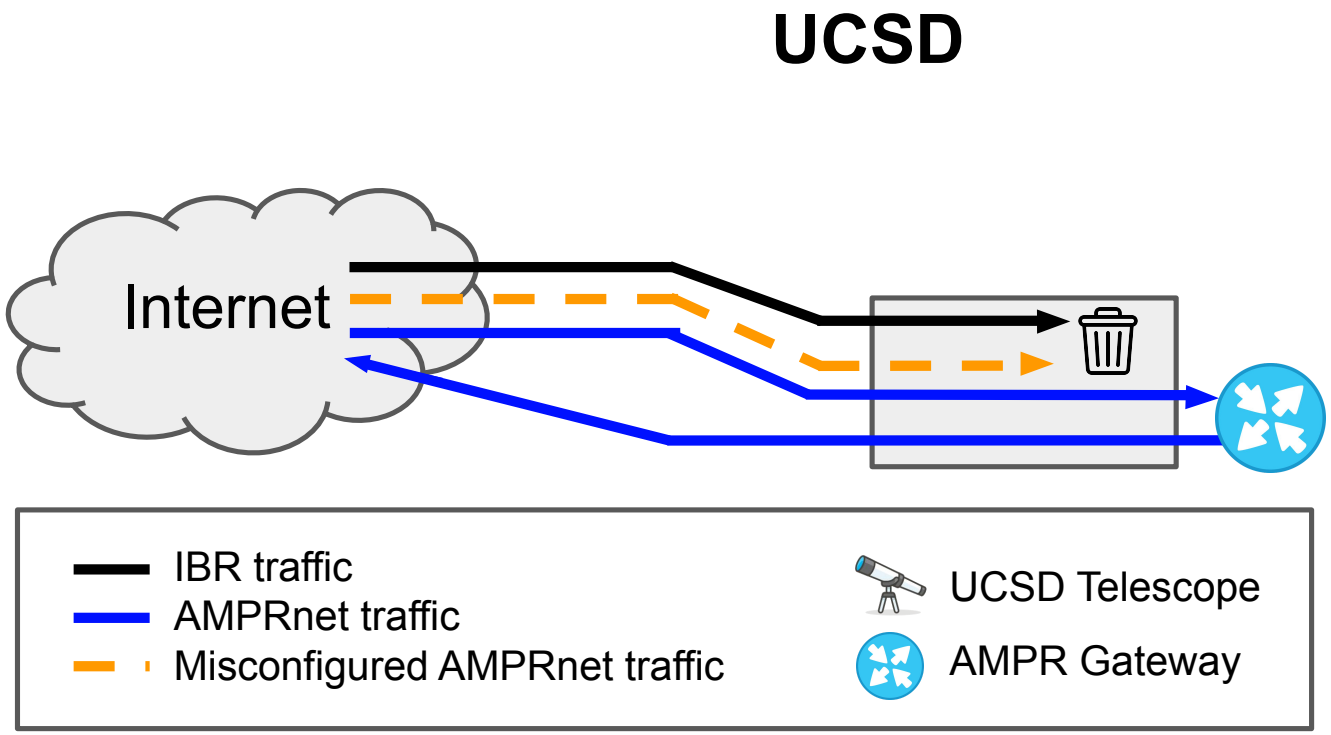


Receiving → Capturing → Recording + Storage

Challenge: IPv4 address scarcity

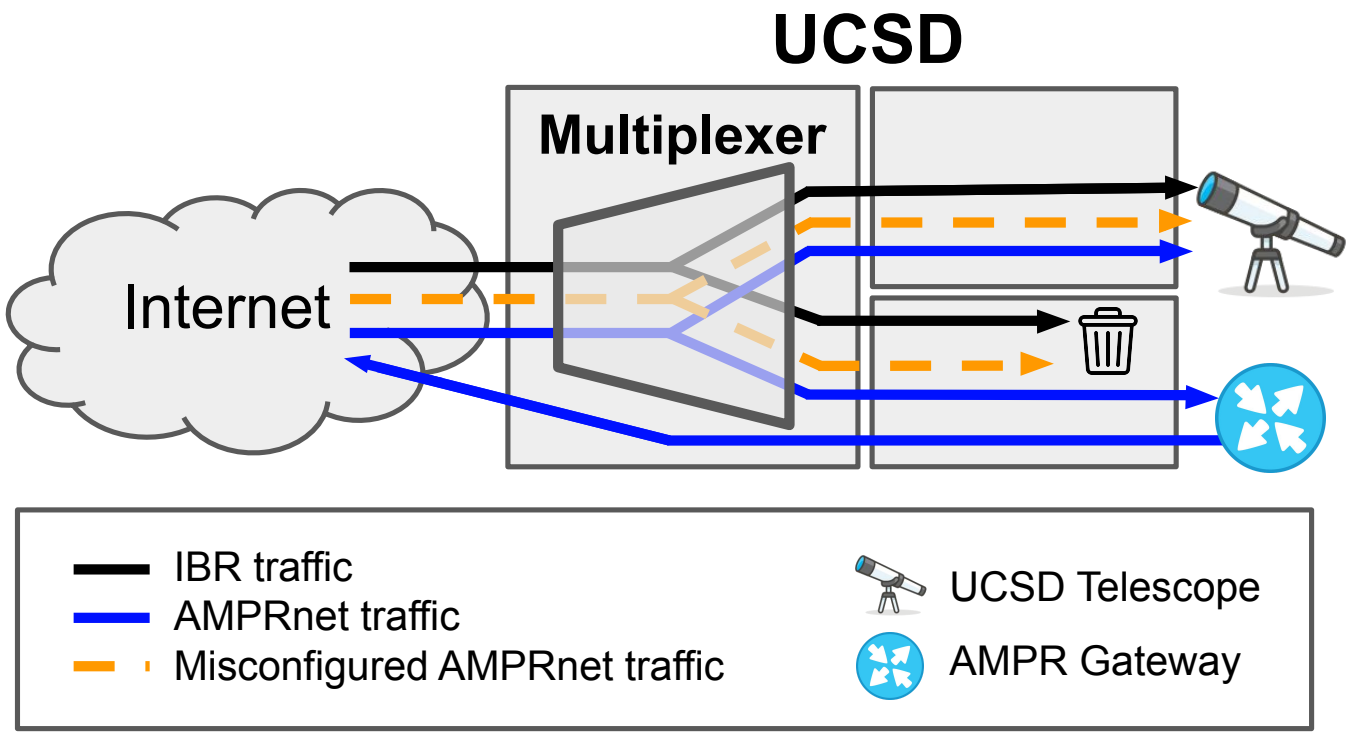
Challenges: Increasing volume
Storage requirements

Coexistence of UCSD-NT and AMPRNet



Traffic sent to the AMPRNet prefixes is routed to the AMPRNet gateway hosted at UCSD.

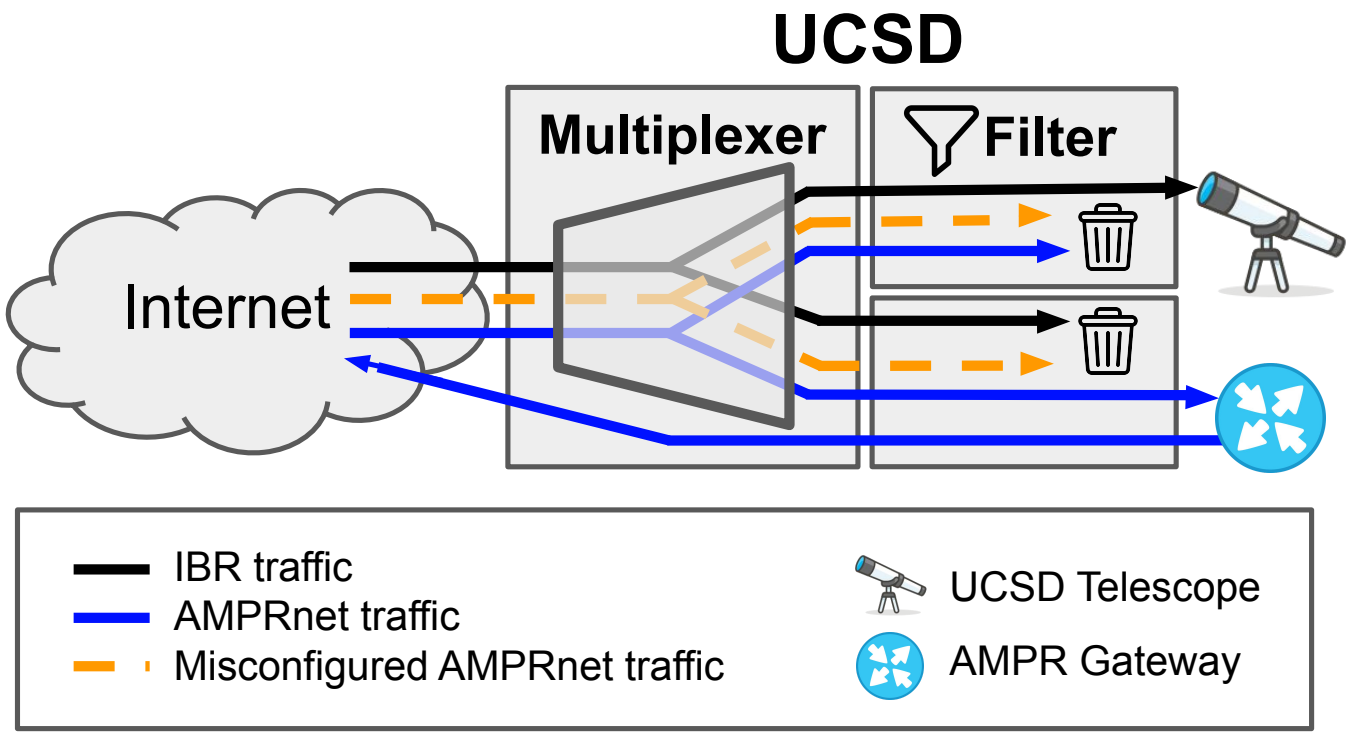
Coexistence of UCSD-NT and AMPRNet



Traffic sent to the AMPRNet prefixes is routed to the AMPRNet gateway hosted at UCSD.

The UCSD-NT also **receives all traffic** destined to AMPRNet and **filters out traffic destined to active networks**.

Coexistence of UCSD-NT and AMPRNet

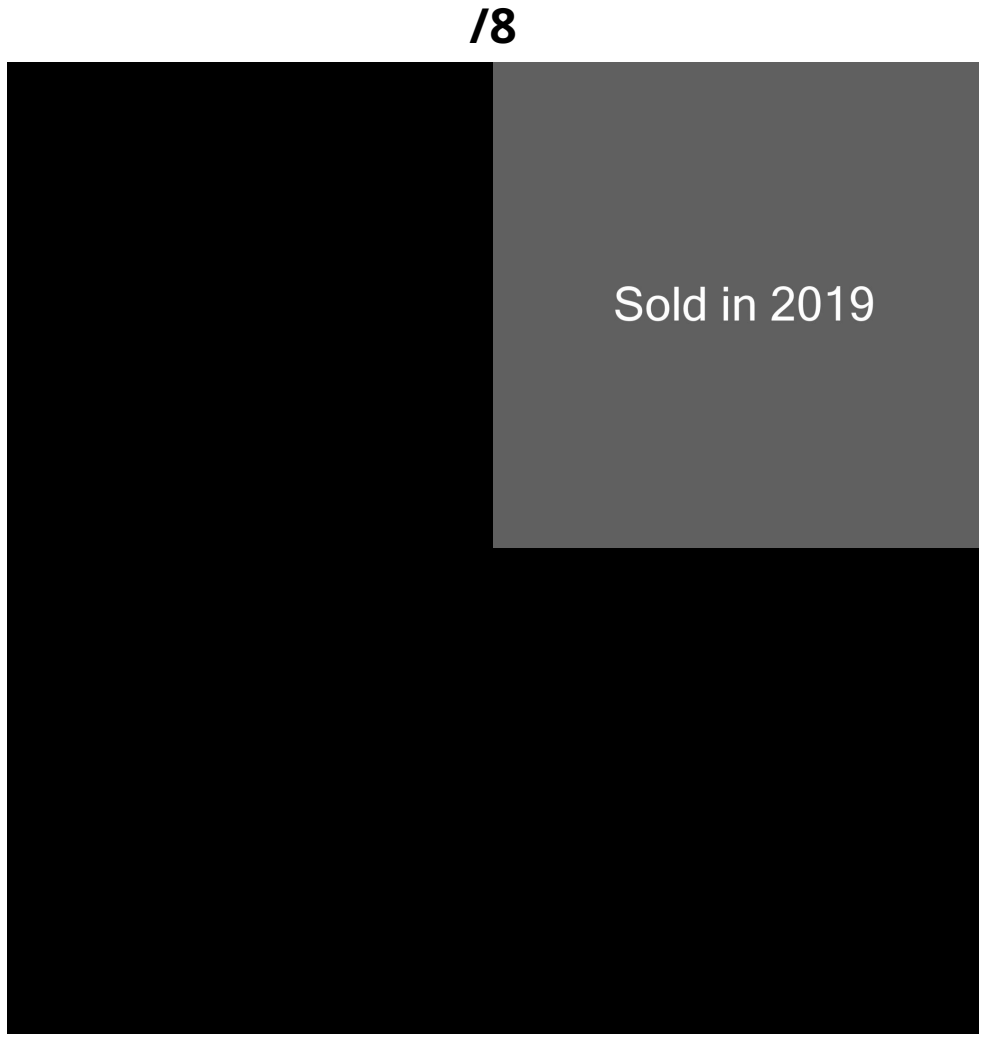


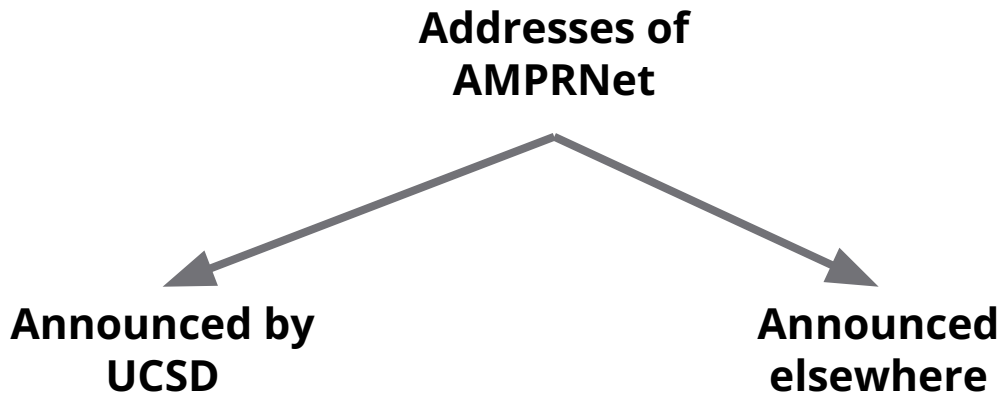
Traffic sent to the AMPRNet prefixes is routed to the AMPRNet gateway hosted at UCSD.

The UCSD-NT also **receives all traffic** destined to AMPRNet and **filters out traffic destined to active networks**.

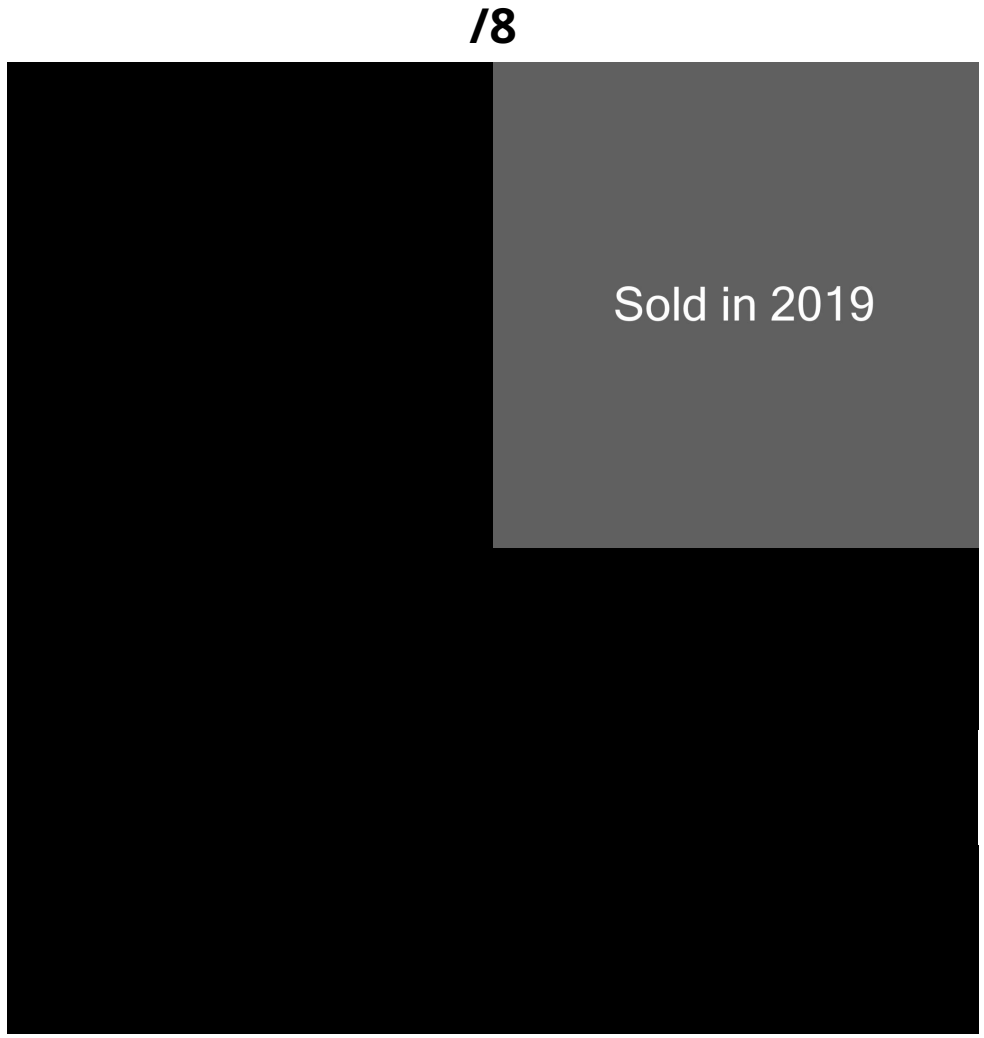
This is accomplished through a **filter list**, containing all addresses actively leased from ARDC, the organization managing address distribution in AMPRNet.

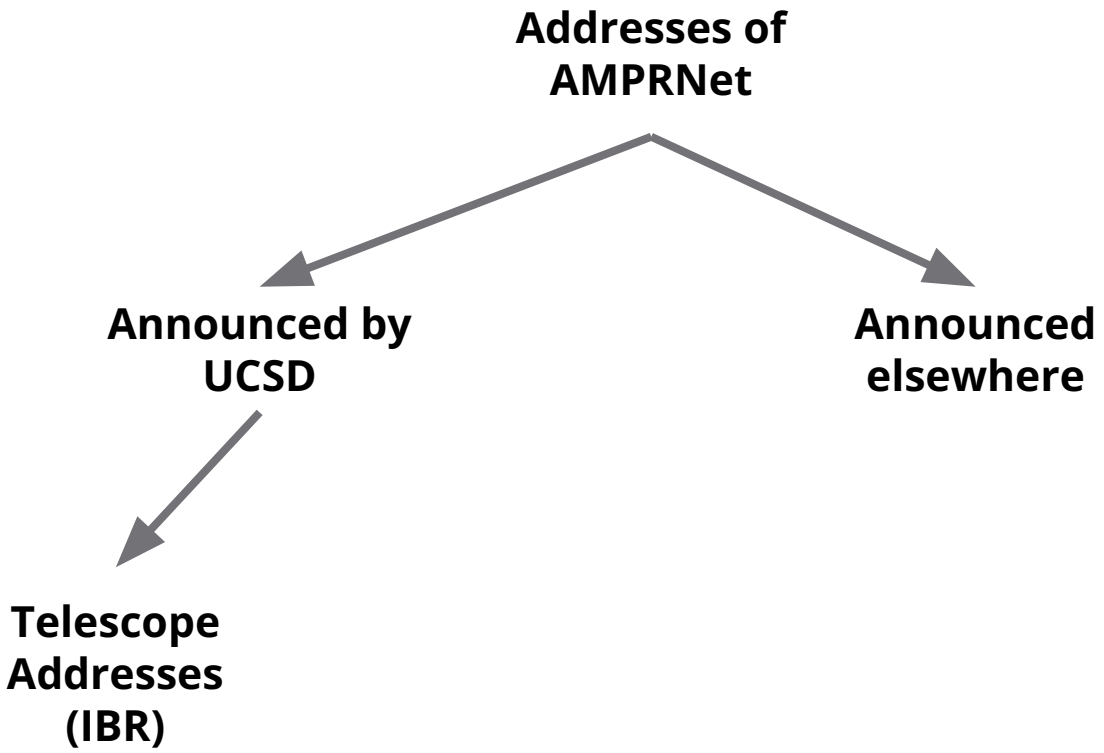
Telescope Coverage in Jan 2025. The UCSD-NT is not continuously dark.



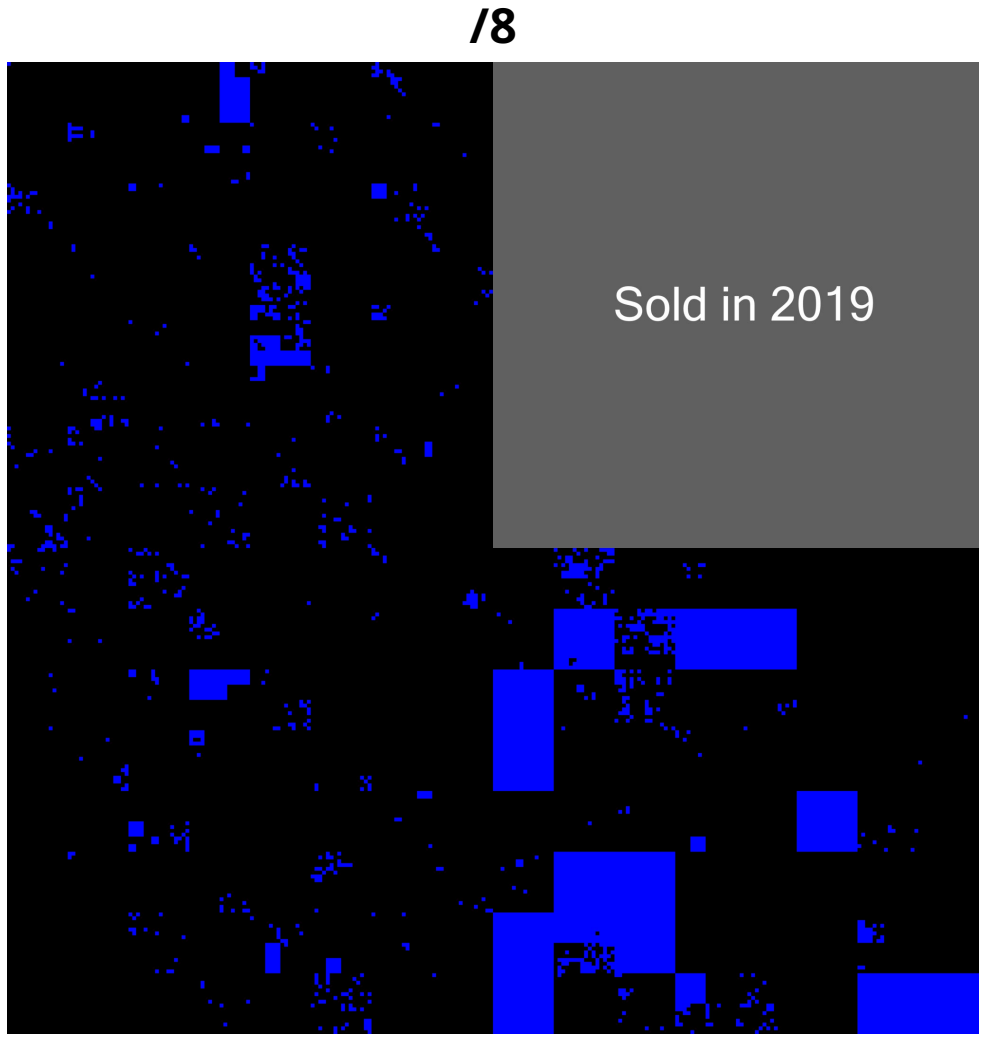


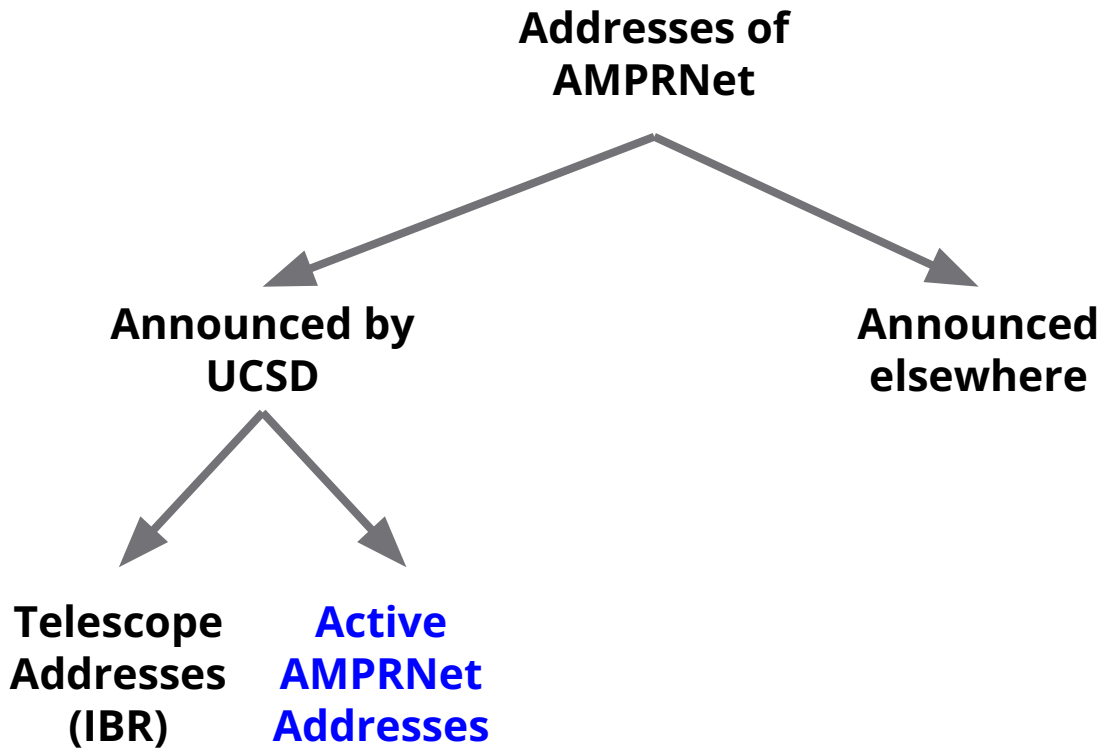
Telescope Coverage in Jan 2025. The UCSD-NT is not continuously dark.



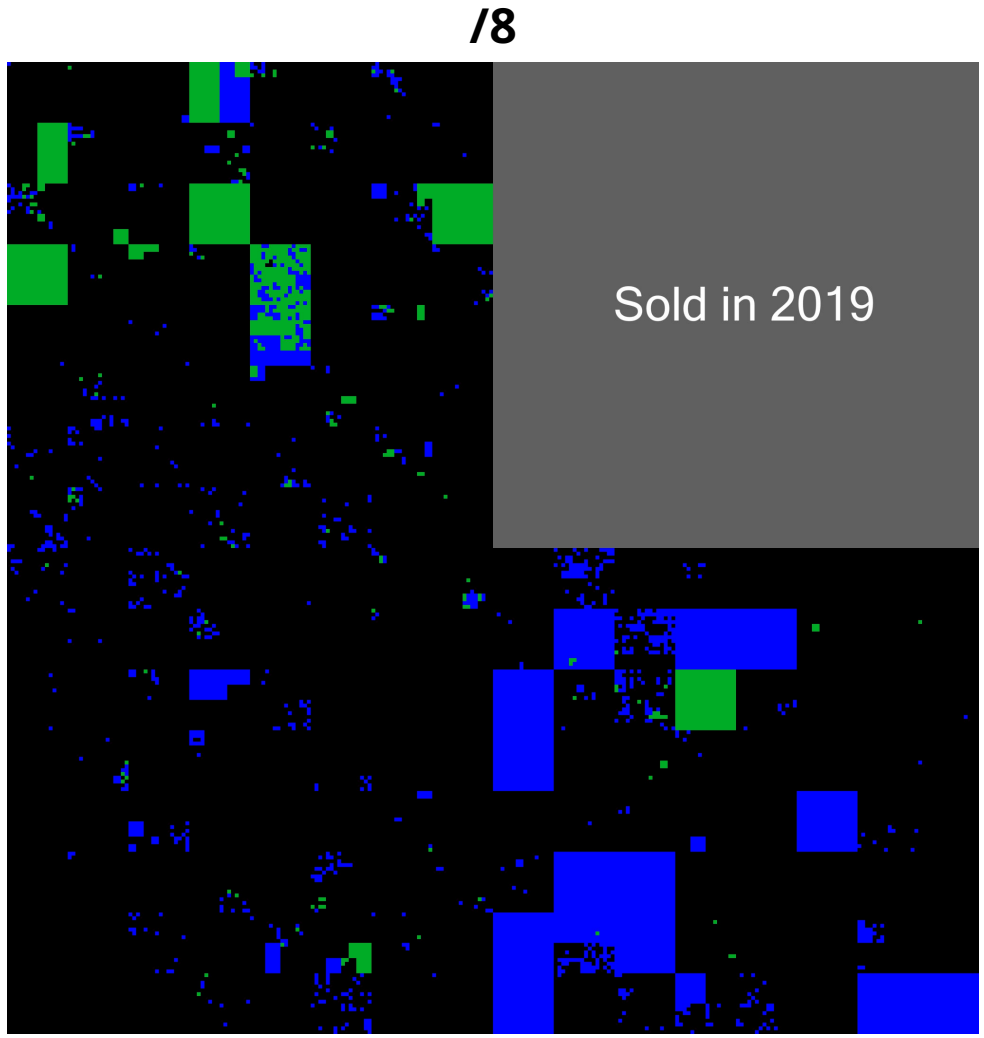


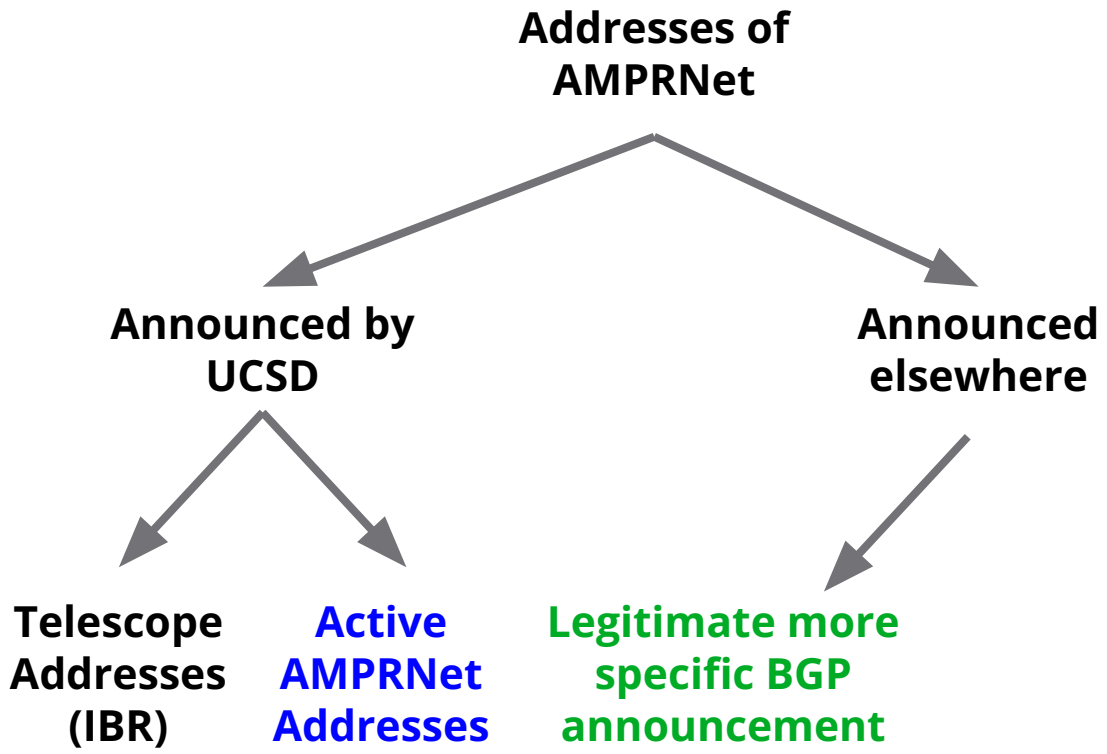
Telescope Coverage in Jan 2025. The UCSD-NT is not continuously dark.



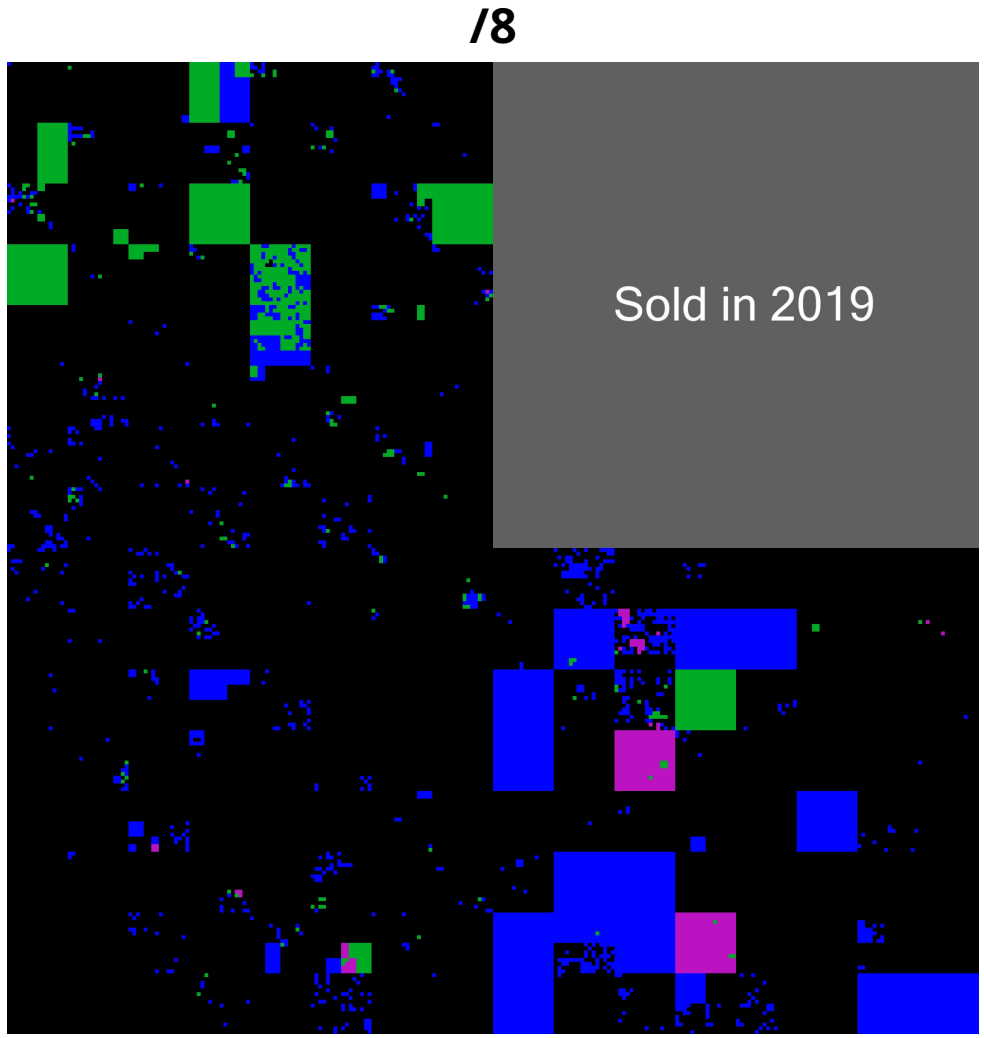


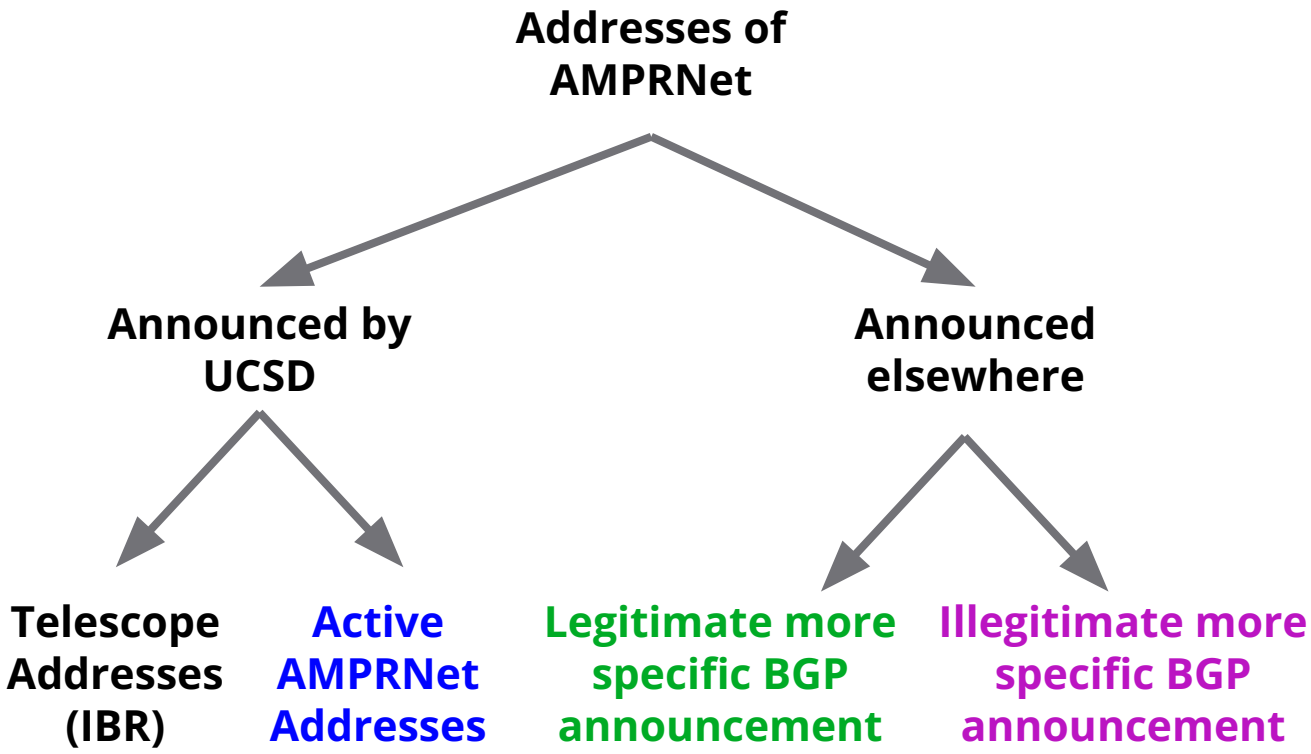
Telescope Coverage in Jan 2025. The UCSD-NT is not continuously dark.





Telescope Coverage in Jan 2025. The UCSD-NT is not continuously dark.





Method: Verifying Telescope Coverage & Packet Loss

To confirm that traffic sent towards the telescope is correctly received and stored, **ground truth is required**.

By **searching for known packets** in the telescope data set, we can **verify the data set correctness**.

We rely on third-party scanning projects to not alter the data collected by the telescope.

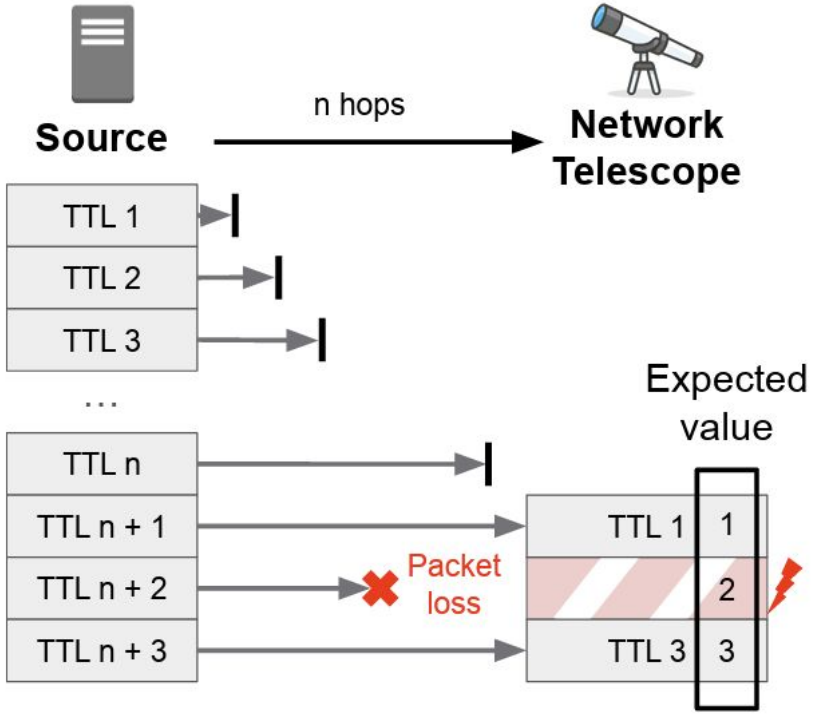
Method: Verifying Telescope Coverage & Packet Loss

Full IPv4 Scans every four hours

Traceroute to every /22 every day

Full IPv4 address scans enable tracking IP addresses that are part of the telescope.

If no packet is stored for an IP address over the interval, it is likely not part of the telescope.



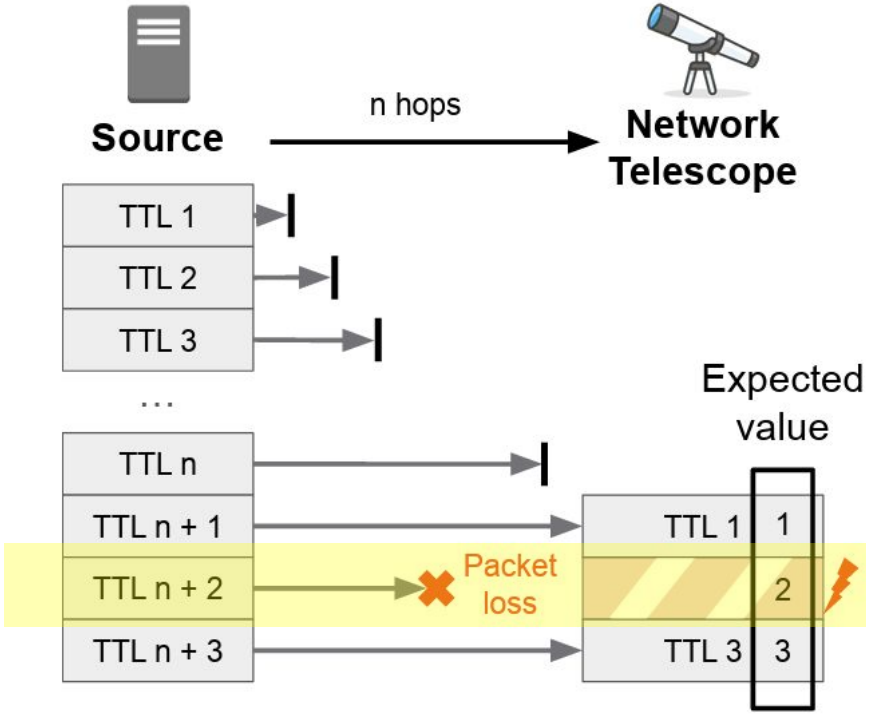
Method: Verifying Telescope Coverage & Packet Loss

Full IPv4 Scans every four hours

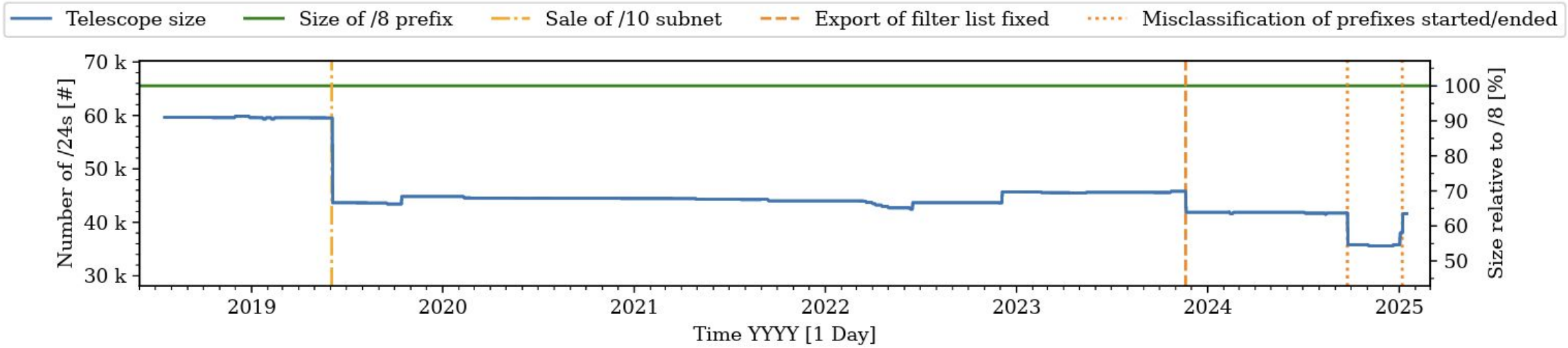
Traceroute to every /22 every day

Full IPv4 address scans enable tracking IP addresses that are part of the telescope.

If no packet is stored for an IP address over the interval, it is likely not part of the telescope.



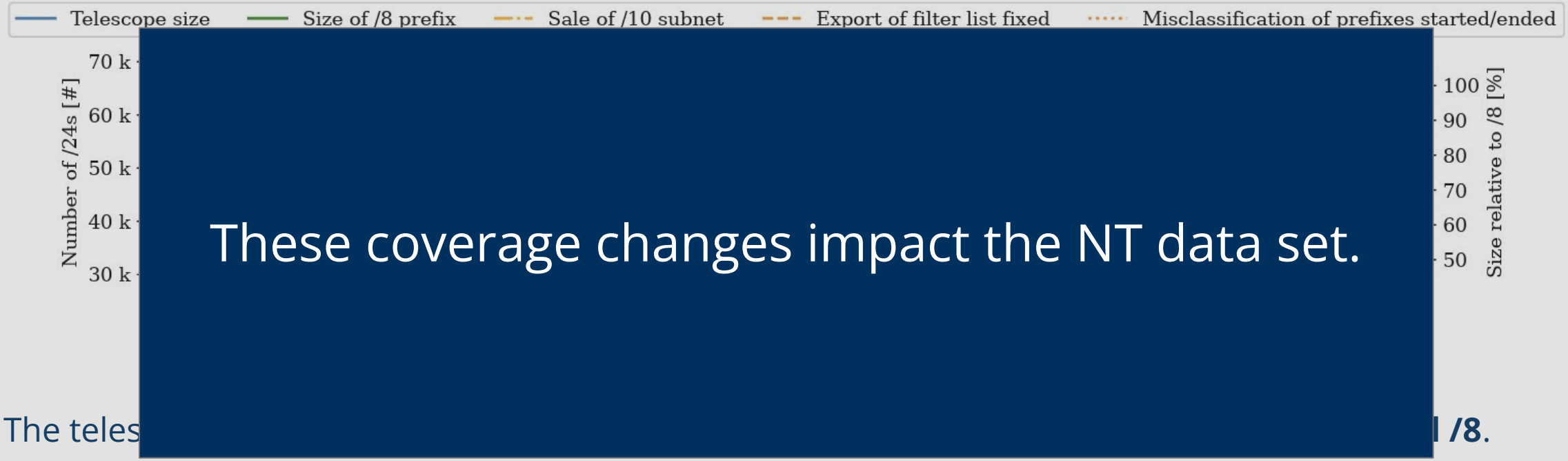
Telescope Coverage
Since July 2018



The telescope size **decreased in the last 6 years.** The **current size is 63.56% of the original /8**.

Both the sale of a /10 by ARDC and new lease granting reduced the telescope size.
Due to an incorrect update procedure detected with our method, the filter list included many newer leases only after November 2023.

Telescope Coverage
Since July 2018

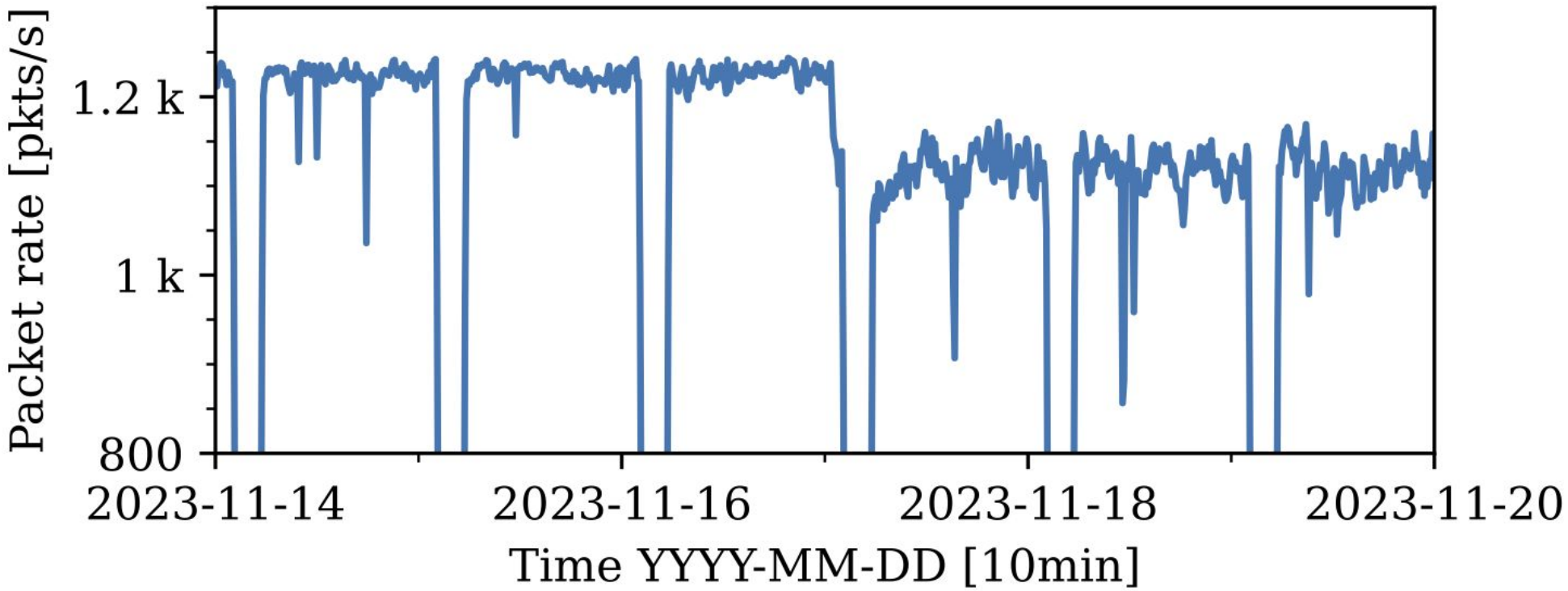


These coverage changes impact the NT data set.

The teles **/8**.

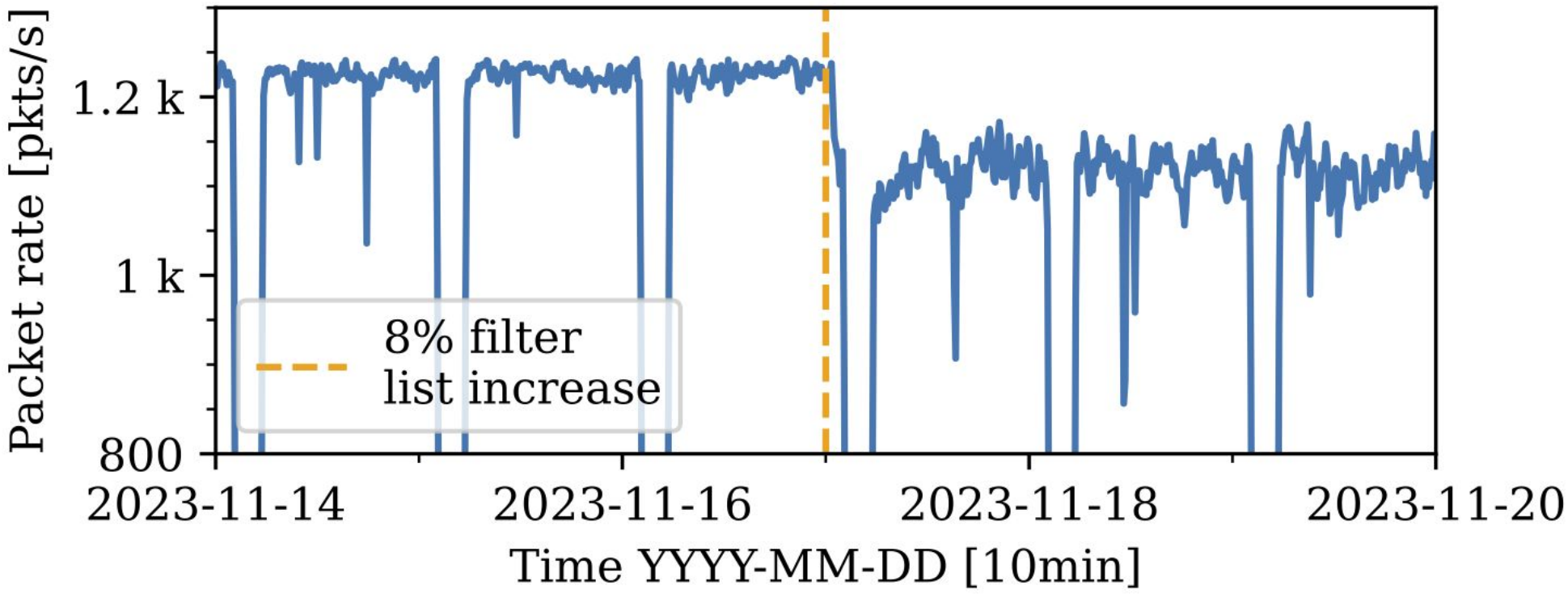
Both the sale of a /10 by ARDC and new lease granting reduced the telescope size.
Due to an incorrect update procedure detected with our method, the filter list included many newer leases only after November 2023.

IBR traffic at UCSD-NT is declining …



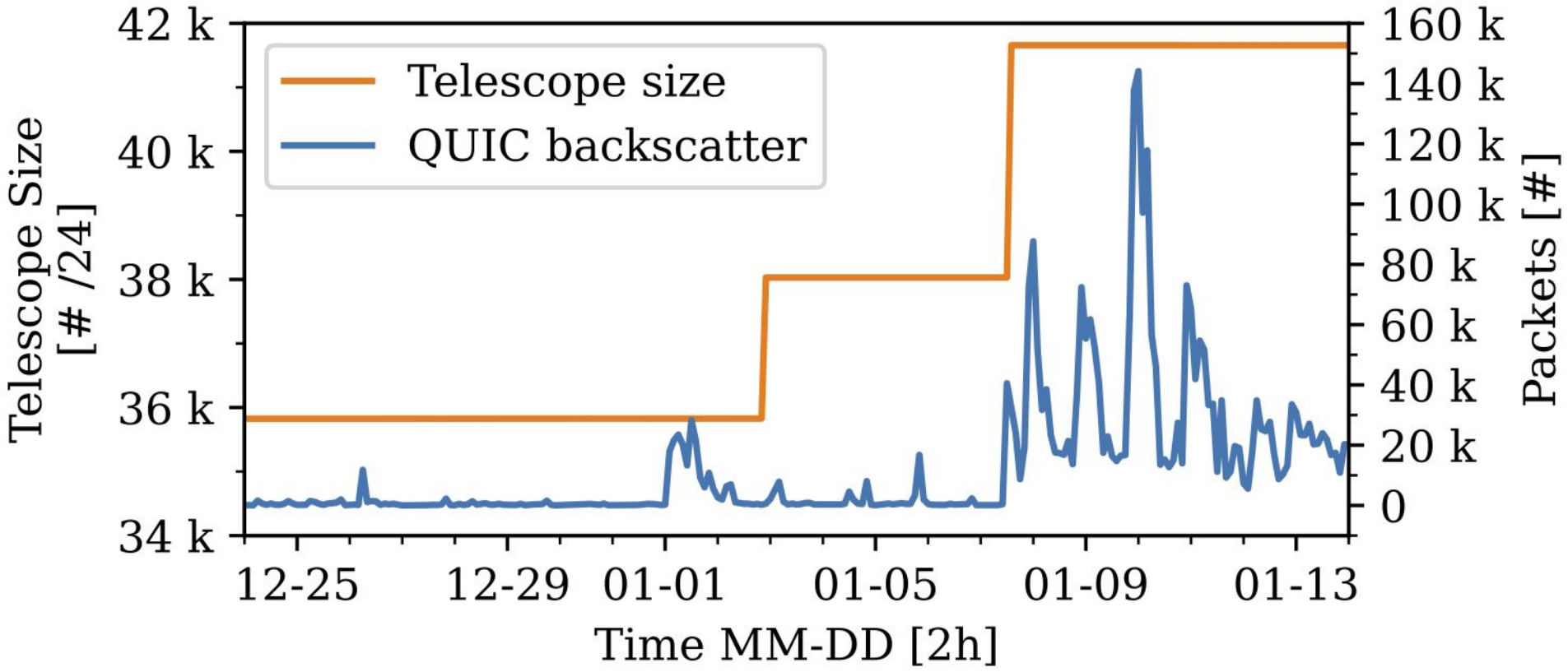
Packet rate of the traceroute measurement project targeting telescope address space.

IBR traffic at UCSD-NT is declining … because of a larger filter list, not because IBR traffic changed in the Internet



Packet rate of the traceroute measurement project targeting telescope address space.

Traffic recorded by the telescope does not only depend on the telescope size but also on the specific available subnets



Example: QUIC backscatter is localized, so when specific prefixes were added in January 2025, traffic patterns changed drastically.

Guidelines

Telescope Operators

Monitor address space in BGP and harden it with RPKI

Accessible documentation of changes telescope size

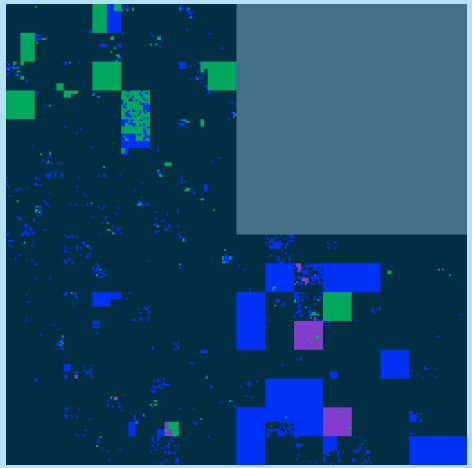
Telescope Data Consumers

Consider Telescope size changes during your observations

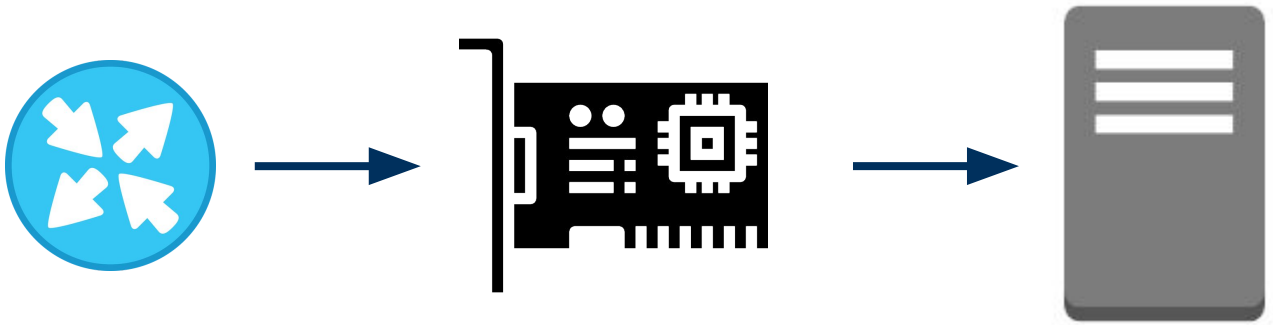
Consider individual subnet importance and availability

Components of a Network Telescope

Address space



Infrastructure



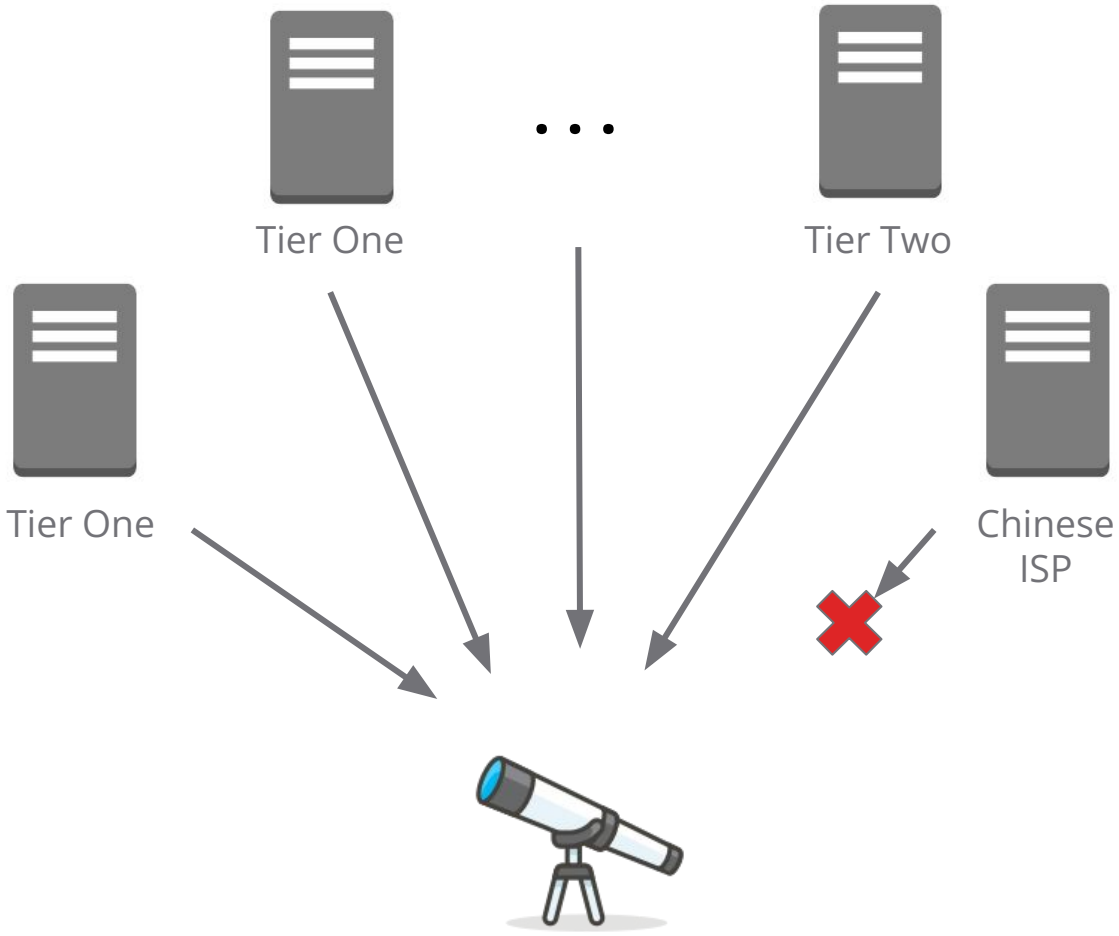
Receiving

Capturing

Recording + Storage

Besides changes in the **address space**, issues can arise **on path** or through the **infrastructure of a Network Telescope**.

Misconfigurations cause packets to not reach UCSD-NT



One vantage point of the Leitwert project **receives upstream from a Chinese ISP**.

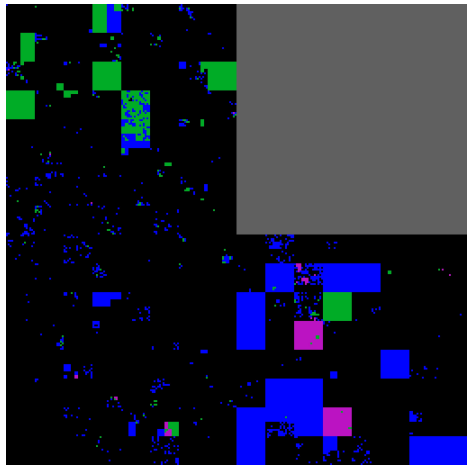
Even though the telescope prefix was visible, **packets from this vantage point did not reach the UCSD-NT** until November 2023.

The cause was an incomplete propagation of the scanner prefix by the ISP.

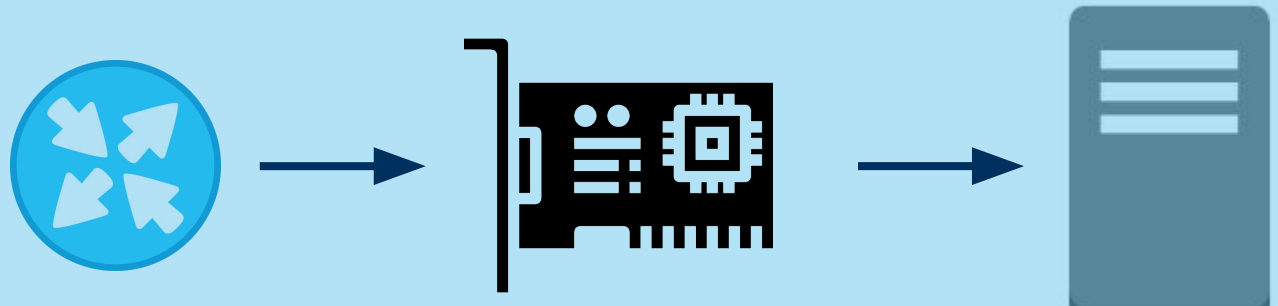
This creates **potential blind spots in the data set**.

Components of a Network Telescope

Address space

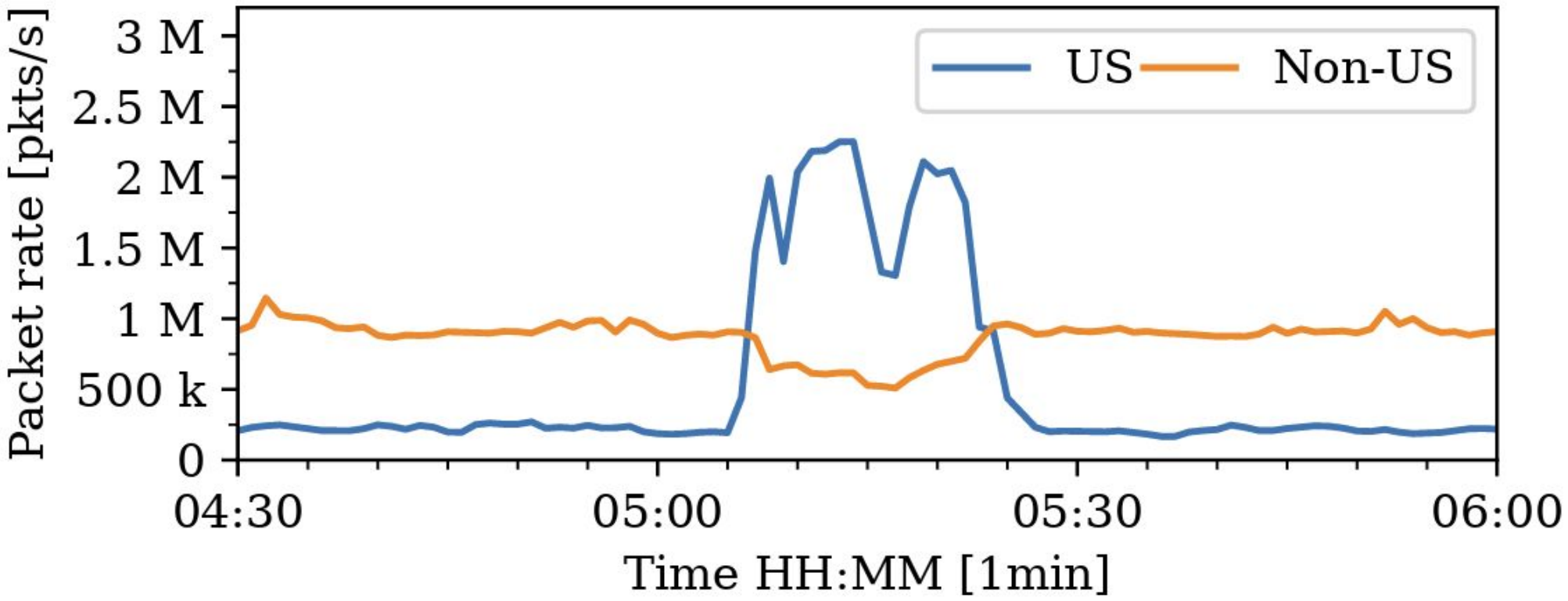


Infrastructure

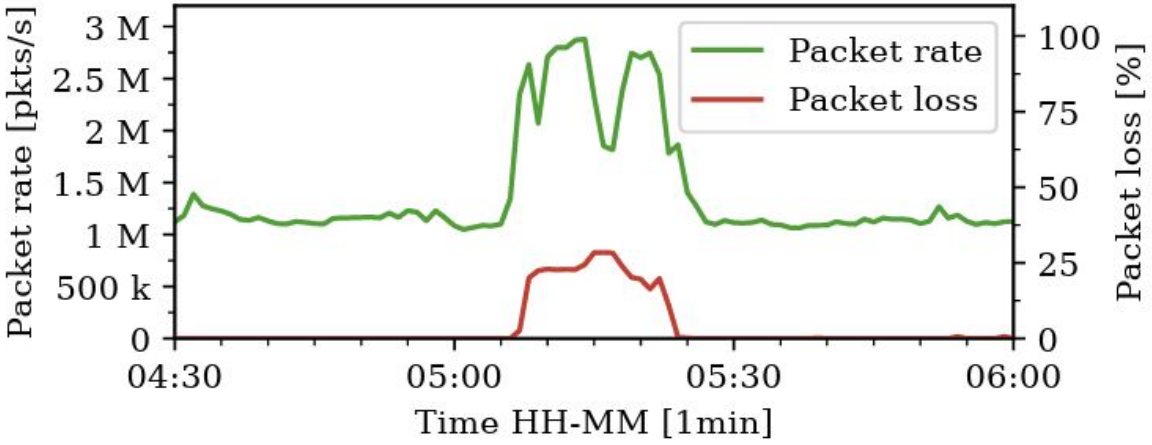


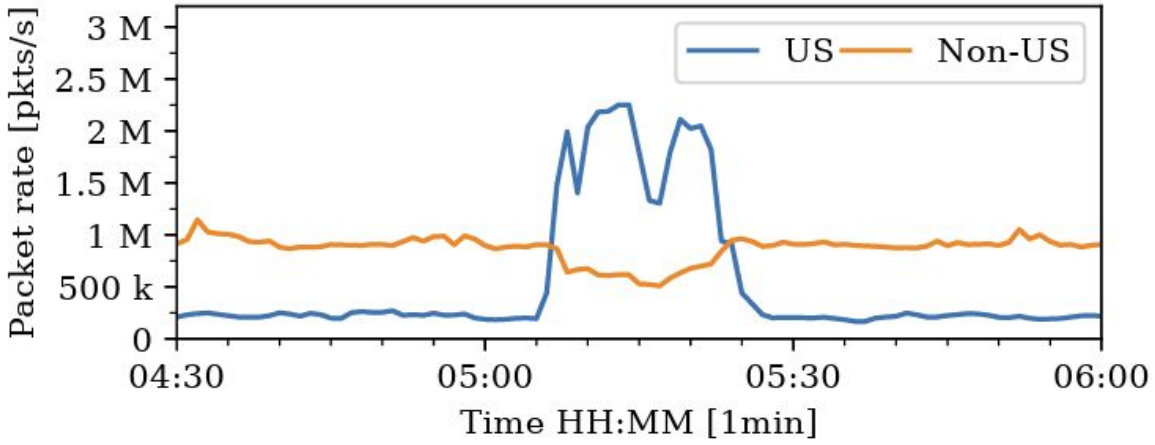
Besides changes in the **address space**, issues can arise **on path** or through the **infrastructure of a Network Telescope**.

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.**

Guidelines

Telescope Operators

Monitor address space in BGP and harden it with RPKI

Accessible documentation of changes telescope size

Perform data plane monitoring to validate the reachability of NT

Monitor system and networking metrics of capturing infrastructure

Validate the final data set to catch problems during processing

Telescope Data Consumers

Consider Telescope size changes during your observations

Consider individual subnet importance and availability

Validate the collected data with ground truth in regards to your research question if possible

Conclusion

Network telescopes are an important measurement instrument. Monitoring and validating data collected by a Network Telescope is a complex endeavour, though.

More automated solutions are required to continuously perform these tasks in real time.

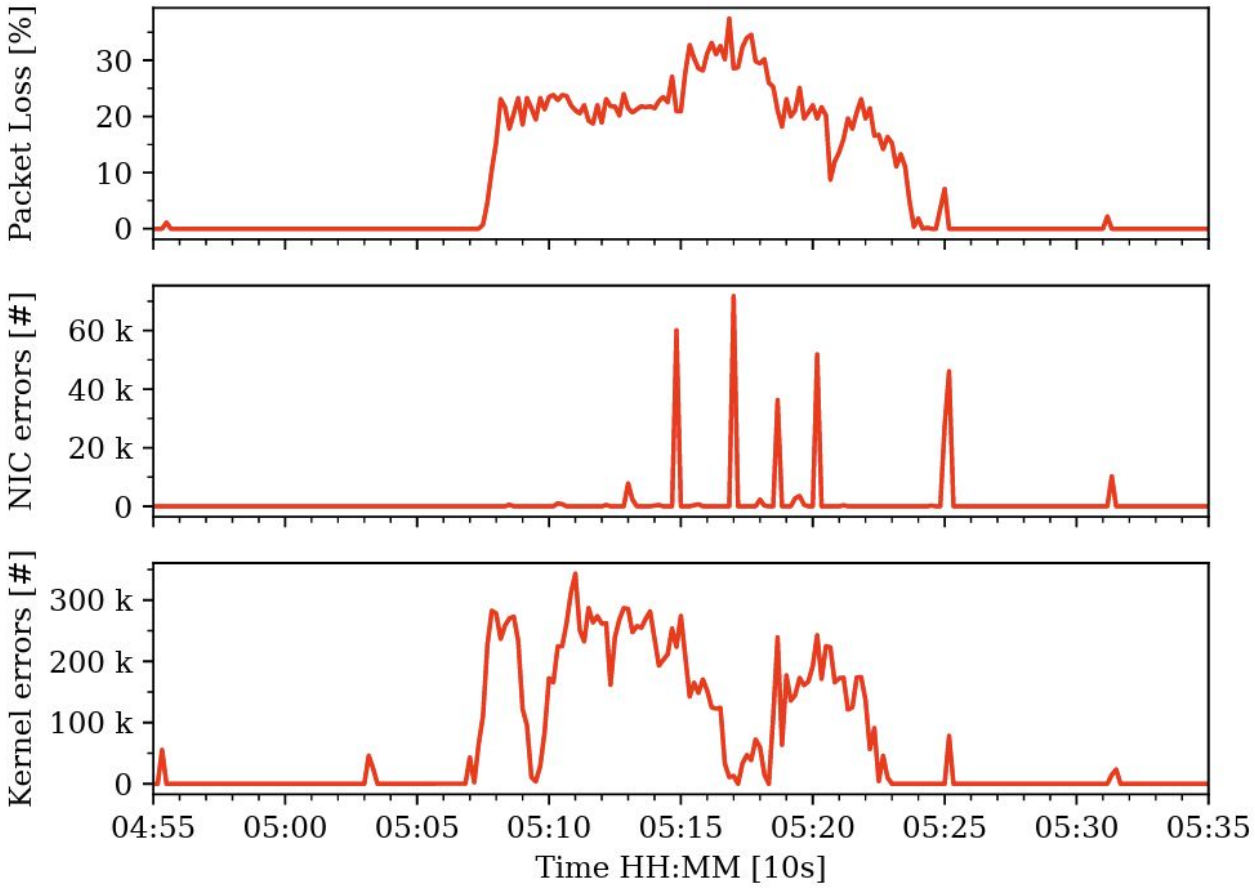
We need to monitor and detect changes in:

1. Address space dynamics
2. Control and data plane reachability
3. Data reception, parsing, and storage

Most Internet measurement infrastructures lack long-term funding to support them and allow for this extra effort but research and practice rely on such infrastructures.

Backup

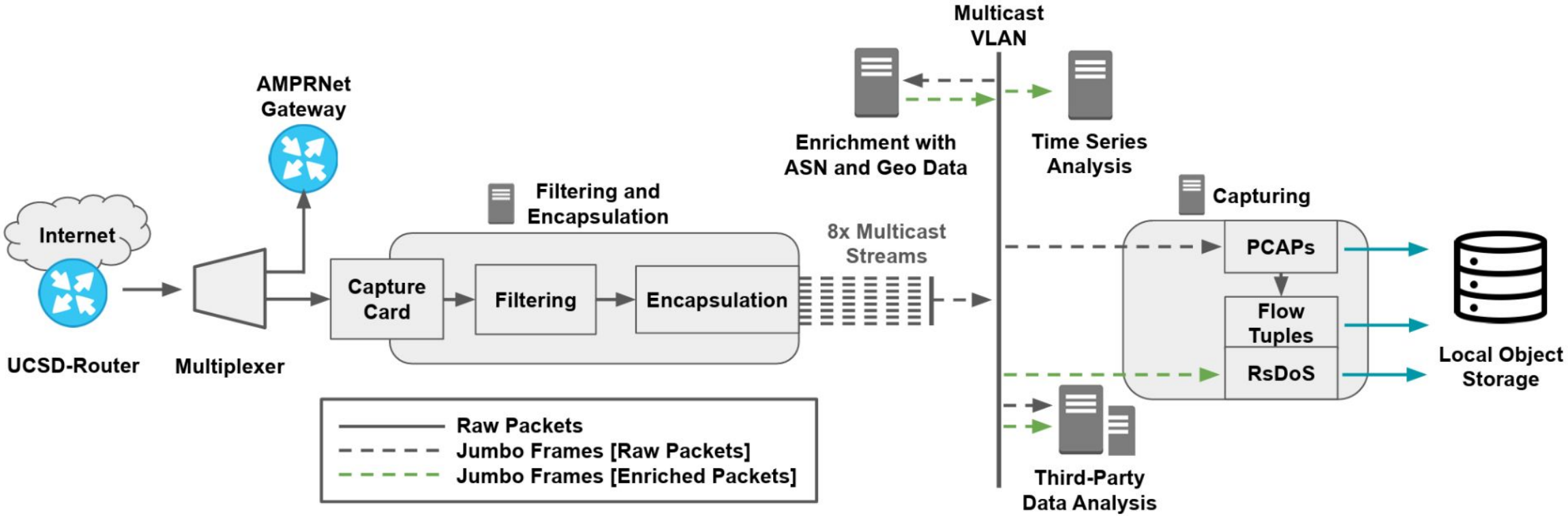
Packet loss at the UCSD-NT under high load



Several error counters on the capture machine align with the packet loss detected in the telescope data set.

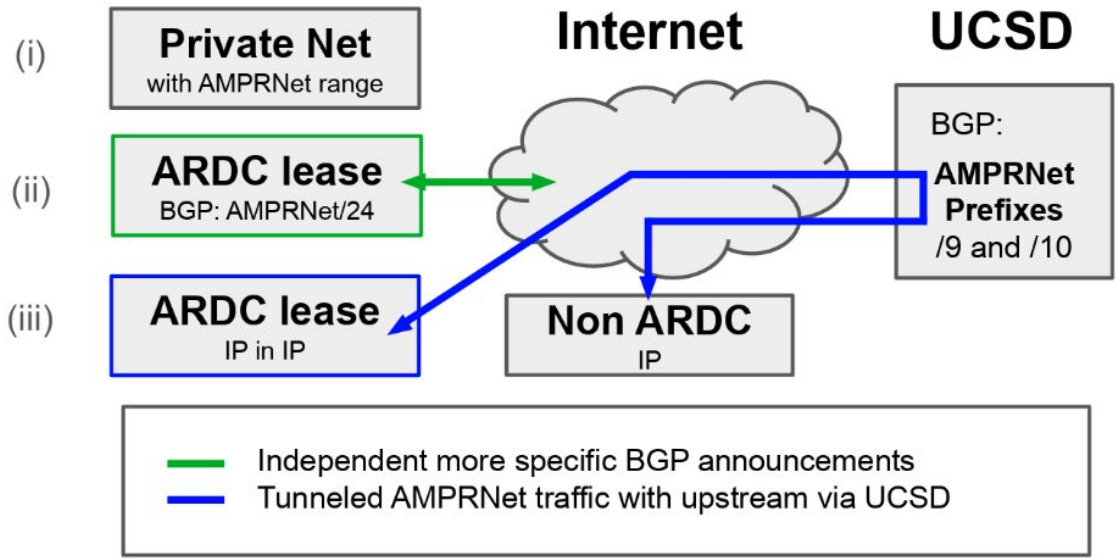
For a more detailed explanation, see Section 5.4 in the paper.

Architecture of the UCSD-NT

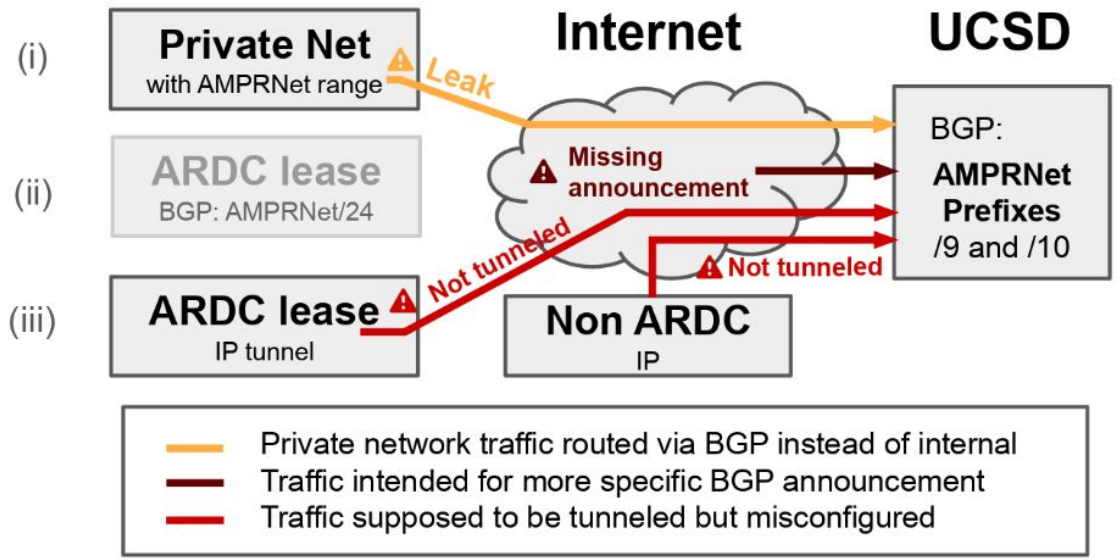


For a more detailed explanation, see Section 3.3 in the paper.

Active Use Cases for AMPRNet



(a) Intended use cases.



(b) Issues that can cause traffic to incorrectly reach UCSD.

AMPRNet addresses are leased to amateur radio operators as experimental resources. These operators either use them in **private networks**, for **separate BGP announcements** or **with upstream provided through UCSD**. Misconfigurations and issues can cause traffic to incorrectly reach the telescope.

How did this investigation come about?

External Researchers:

Dresden University of Technology

HAW HAMBURG

Telescope Operators:

While investigating other research questions with the IBR collected by the UCSD-NT we noticed inconsistencies:

1. **Expected traffic was missing.**
2. **Packet rates contained unexpected drops.**

We devised methods to investigate these issues with the access we have as data consumers.

Once the suspicions were confirmed, we worked with CAIDA to resolve them.

Guidelines

Telescope Operators

Monitor address space in BGP and harden it with RPKI

Accessible documentation of changes telescope size

Perform data plane monitoring to validate the reachability of NT

Monitor system and networking metrics of capturing infrastructure

Validate the final data set to catch problems during processing

Telescope Data Consumers

Consider Telescope size changes during your observations

Consider individual subnet importance and availability

Validate the collected data with ground truth in regards to your research question if possible