



Private relay services

Localization of traffic -
Does it really work?

2023



Background on Private Relay

Acknowledgement

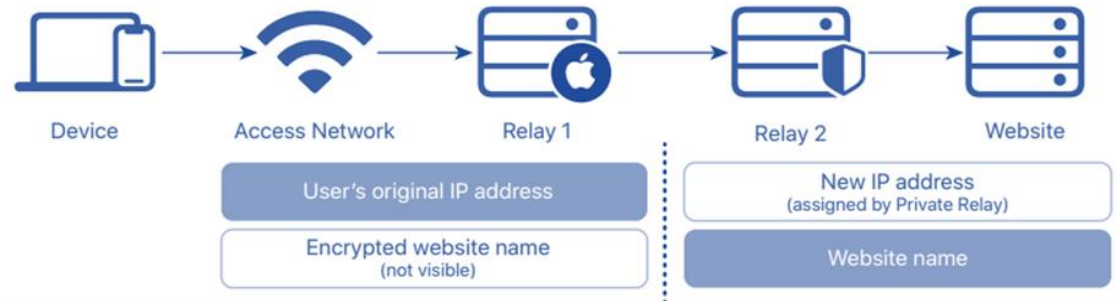
- Private Relay traffic has, by design, its limitations with regards to traffic analysis even though the architecture is well documented.
- Based on our research and findings, only Safari and port-80 traffic is currently handled over Private Relay. This is not necessarily a representative traffic profile.
- Special thanks to Patrick Sattler from Technical University of Munich for his advice and research data.

Architecture

The prominent design feature in this private relay service is the ingress/egress-proxy structure:

- It secures that no party in the chain can connect source & destination, not even the proxy providers.
- Ingress proxies are operated by Apple (some hosted by Akamai).
- Egress proxies are operated by Akamai, Cloudflare or Fastly.

Private Relay Dual-hop Architecture



Source: apple.com/privacy/docs/iCloud_Private_Relay_Overview_Dec2021.PDF

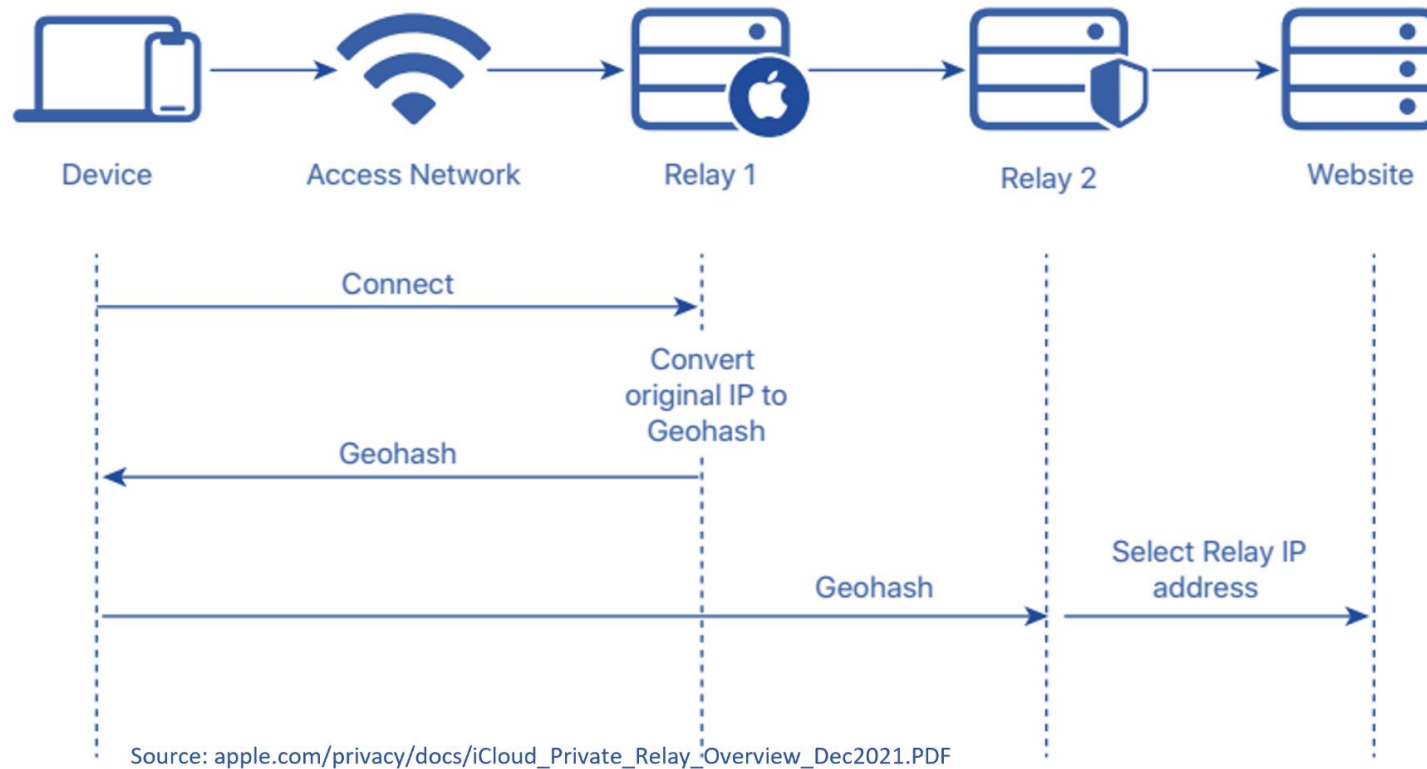
Localization challenge

CDNs try to localize traffic as close to the end-user as possible. This becomes challenging for two reasons:

- In Private Relay, CDNs have limited visibility on end-users' location.
- Relay 1 (aka Ingress-Proxy) is handing over the content to the access-network. Geographical spread of these proxies might not resemble a major CDN's server- and interconnect footprint.



Solution 1 for localization challenge: geo-hashing



Relay 1 provides a geo-hash which translates into a geo-representative IP for Relay 2.

Solution 2: Edge locations for Relay 1

bgp.tools Start here...

View Edit

Akamai Technologies, Inc.

AS Number 36183
Website <https://support.apple.com/en-us/HT212614>

About iCloud Private Relay
How Private Relay works

Overview Prefixes Connectivity Whois

Prefixes Originated
549 IPv4, 1393 IPv6
[Show Low Visibility Prefixes](#)

Addresses Originated
549 /24's of IPv4
1393 /48's of IPv6

Prefix	Description
172.224.0.0/24	Akamai Technologies, Inc.
172.224.1.0/24	Akamai Technologies, Inc.
172.224.2.0/24	Akamai Technologies, Inc.
172.224.3.0/24	Akamai Technologies, Inc.

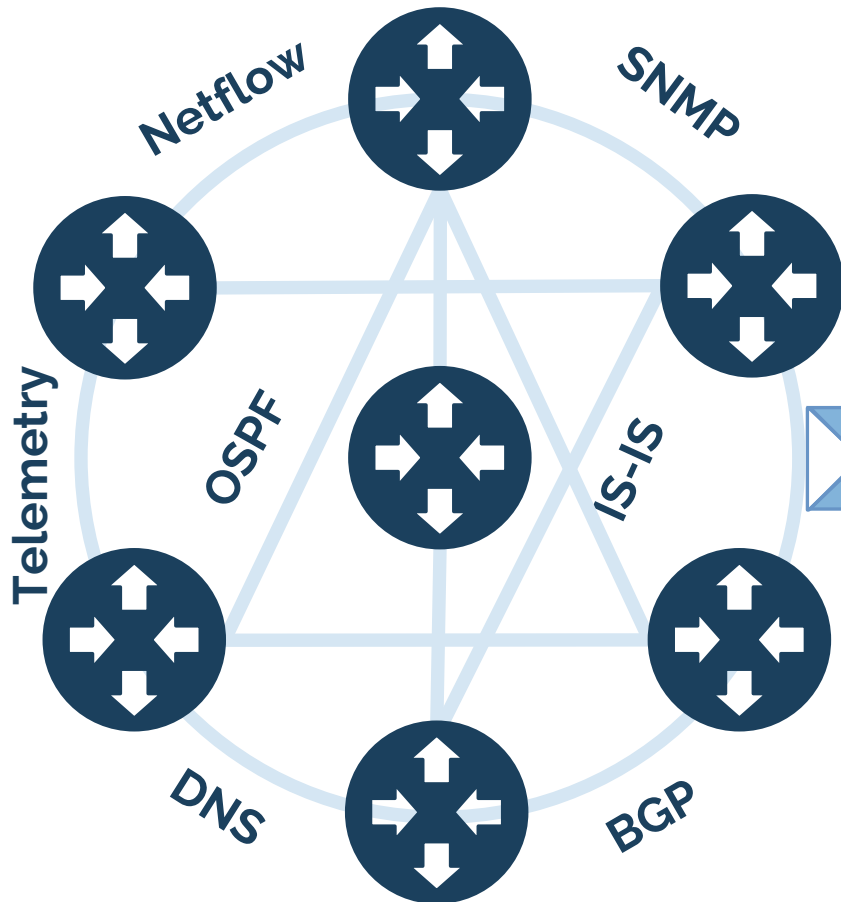
AS36183 (Akamai-AS used for iCloud private relay) announces ~550 x /24

- This could be an indication for the number of locations for Relay 1
- Fairly good coverage, but surely less than the typical footprint of major CDNs

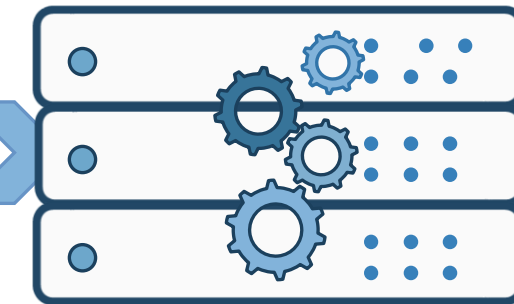


Our Findings

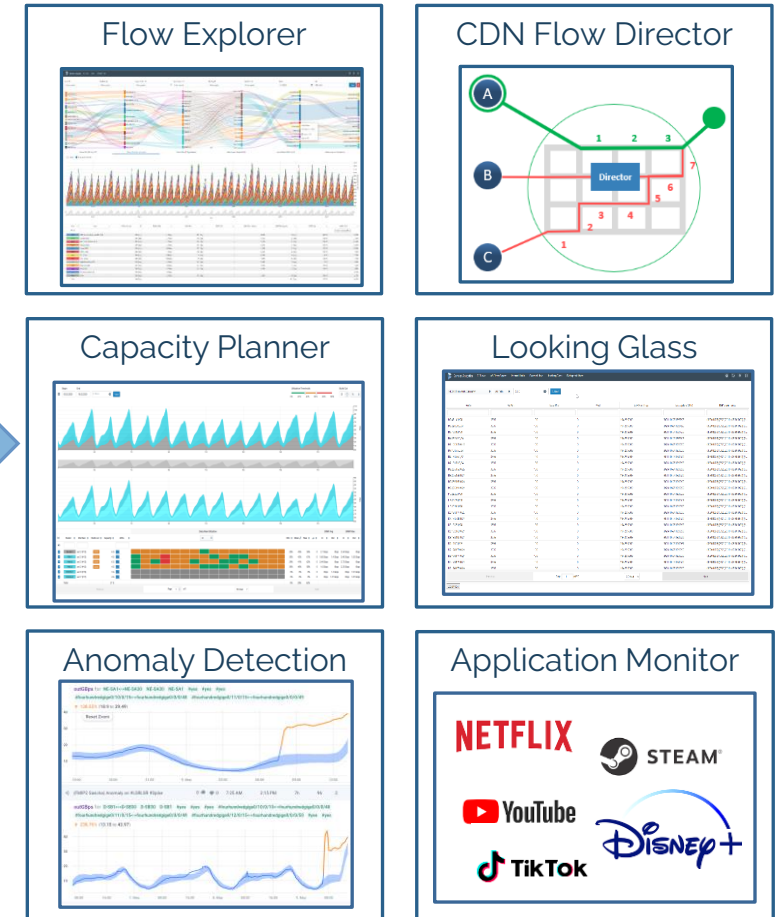
What BENOCS does:



BENOCs CORE ENGINE



Our proprietary aggregation and cross correlation process requires significantly less compute power compared to competitors



PROTOCOL POOL

PROCESSING

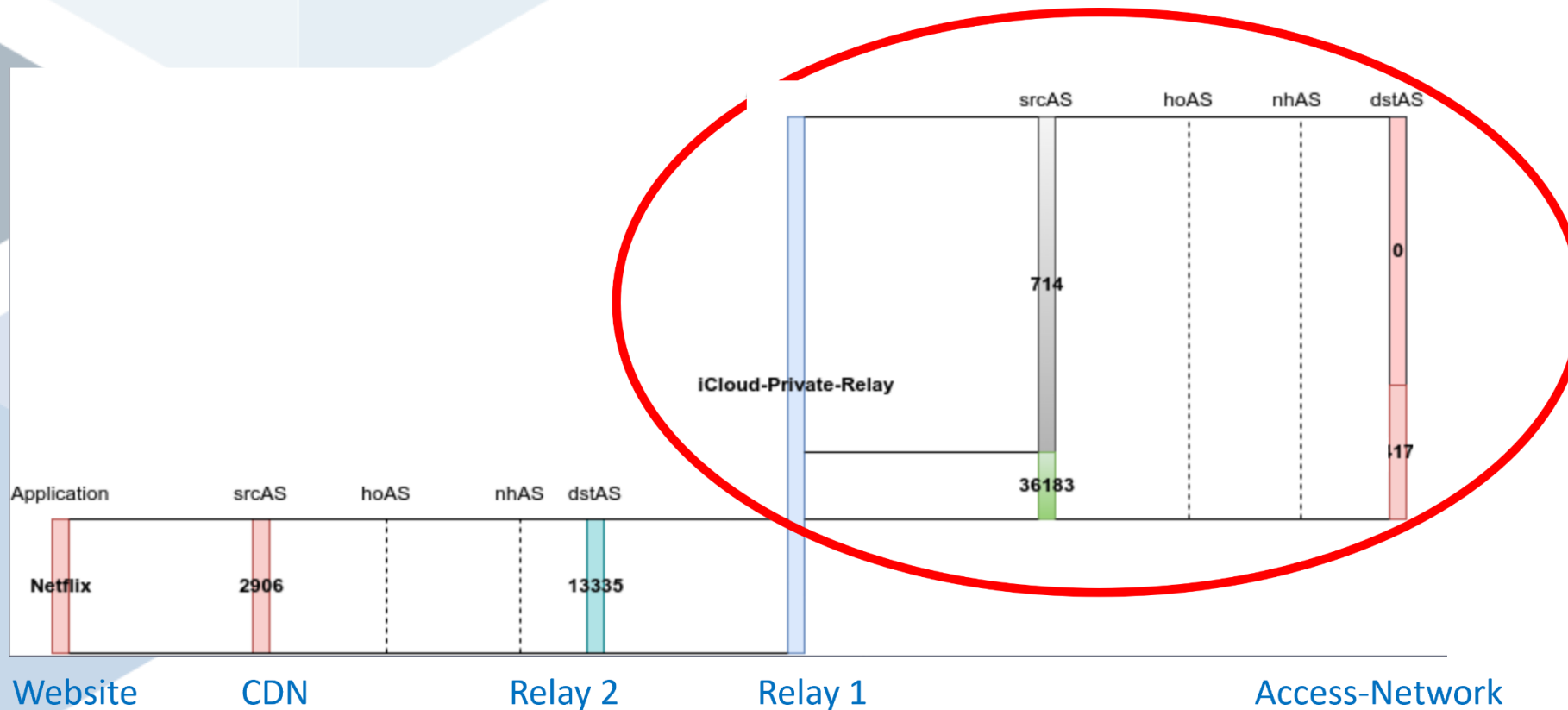
NETWORK INTELLIGENCE

Our methodology

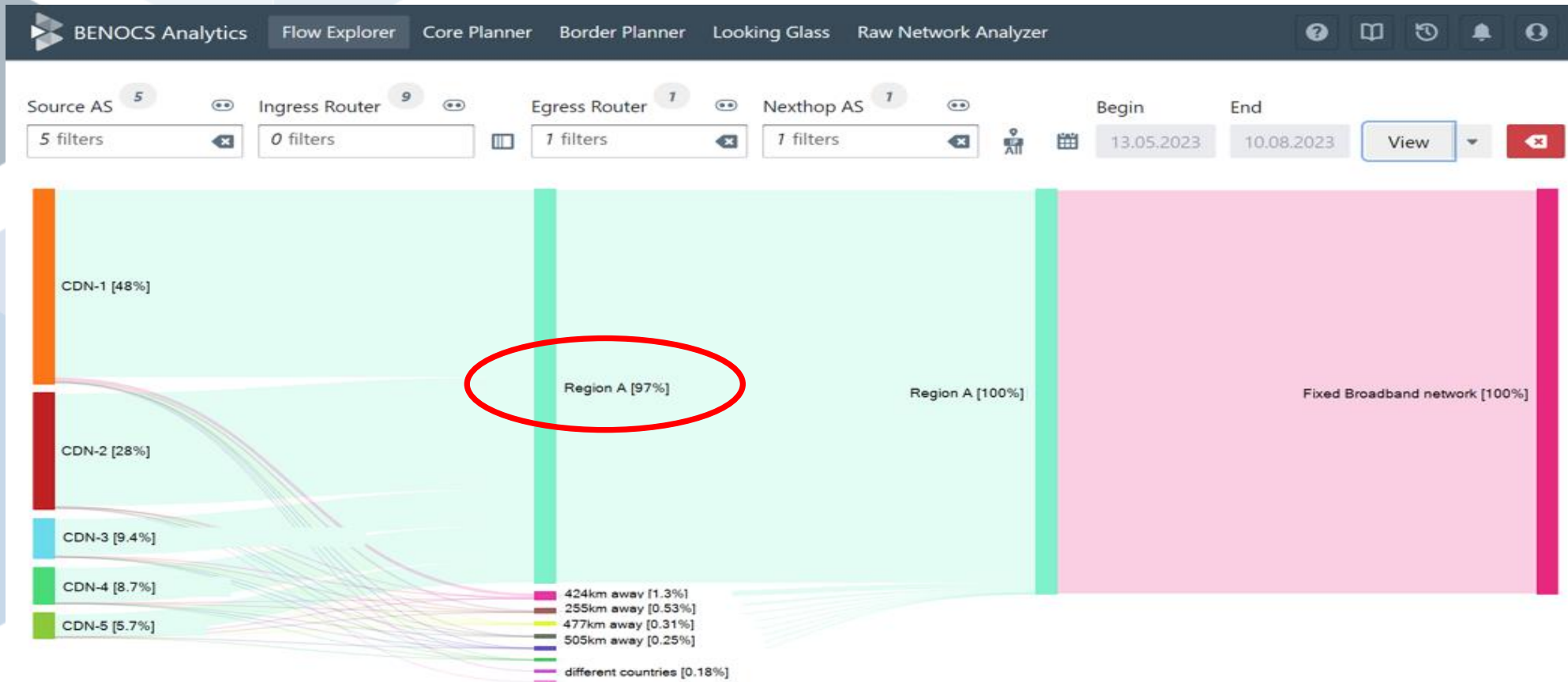
We compared the “ingress distance” between 5 major CDNs and Private-Relay IPs for a representative region in a larger access network.

- Split between fixed-broadband and mobile
- Over 90 days
- All following traffic data is from BENOCS Analytics

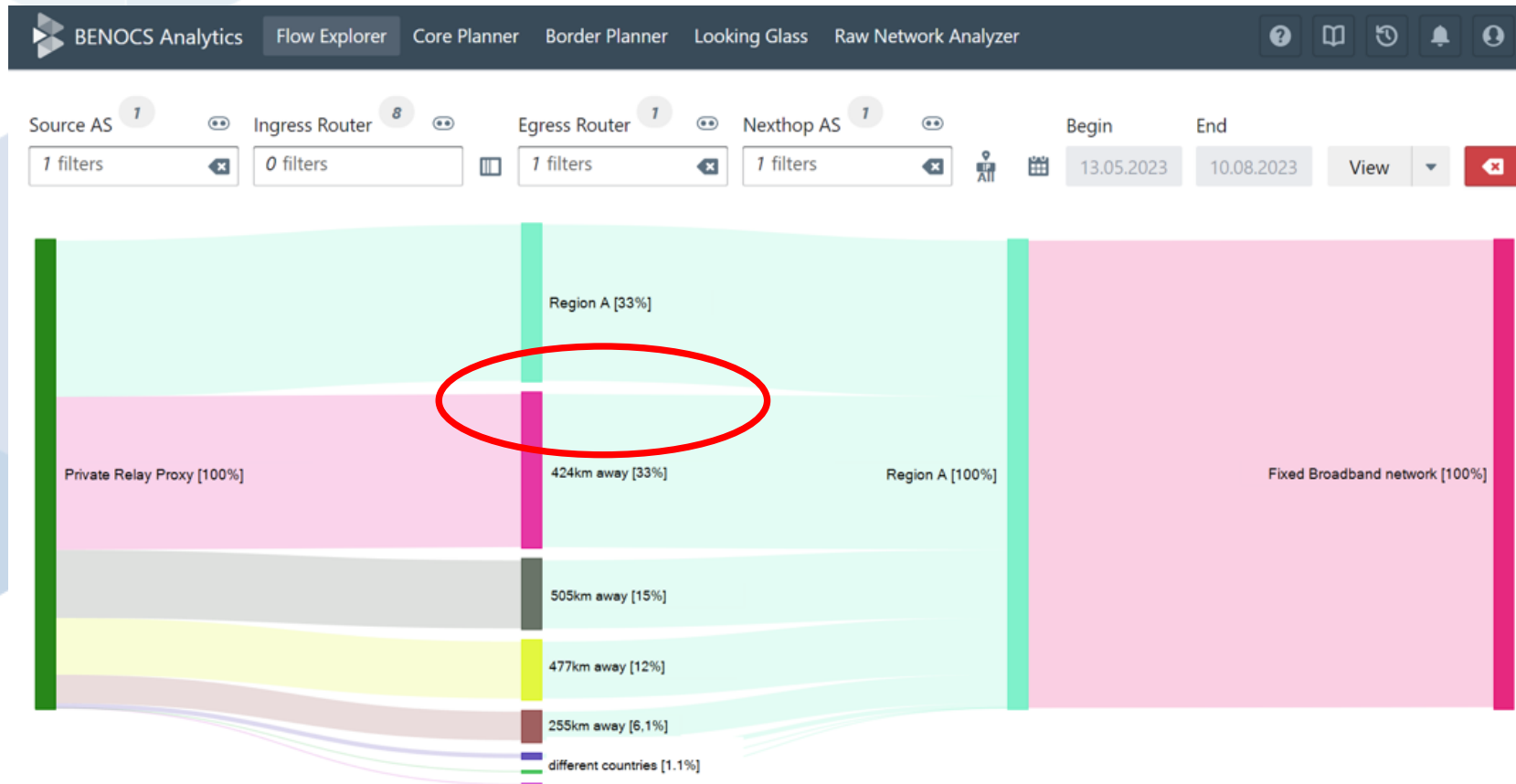
What does an access network see?



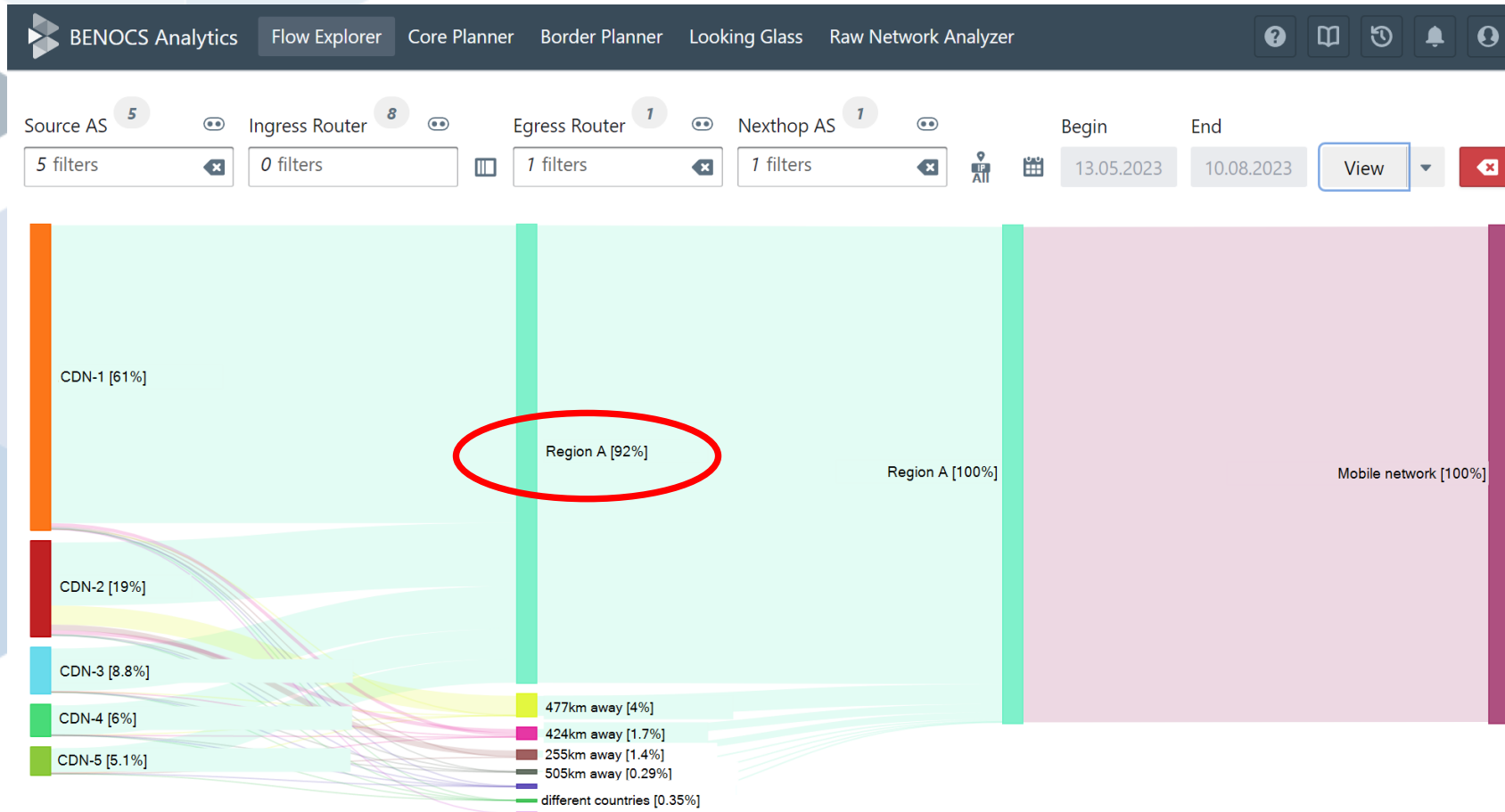
Benchmark: localization of 5 CDNs - fixed



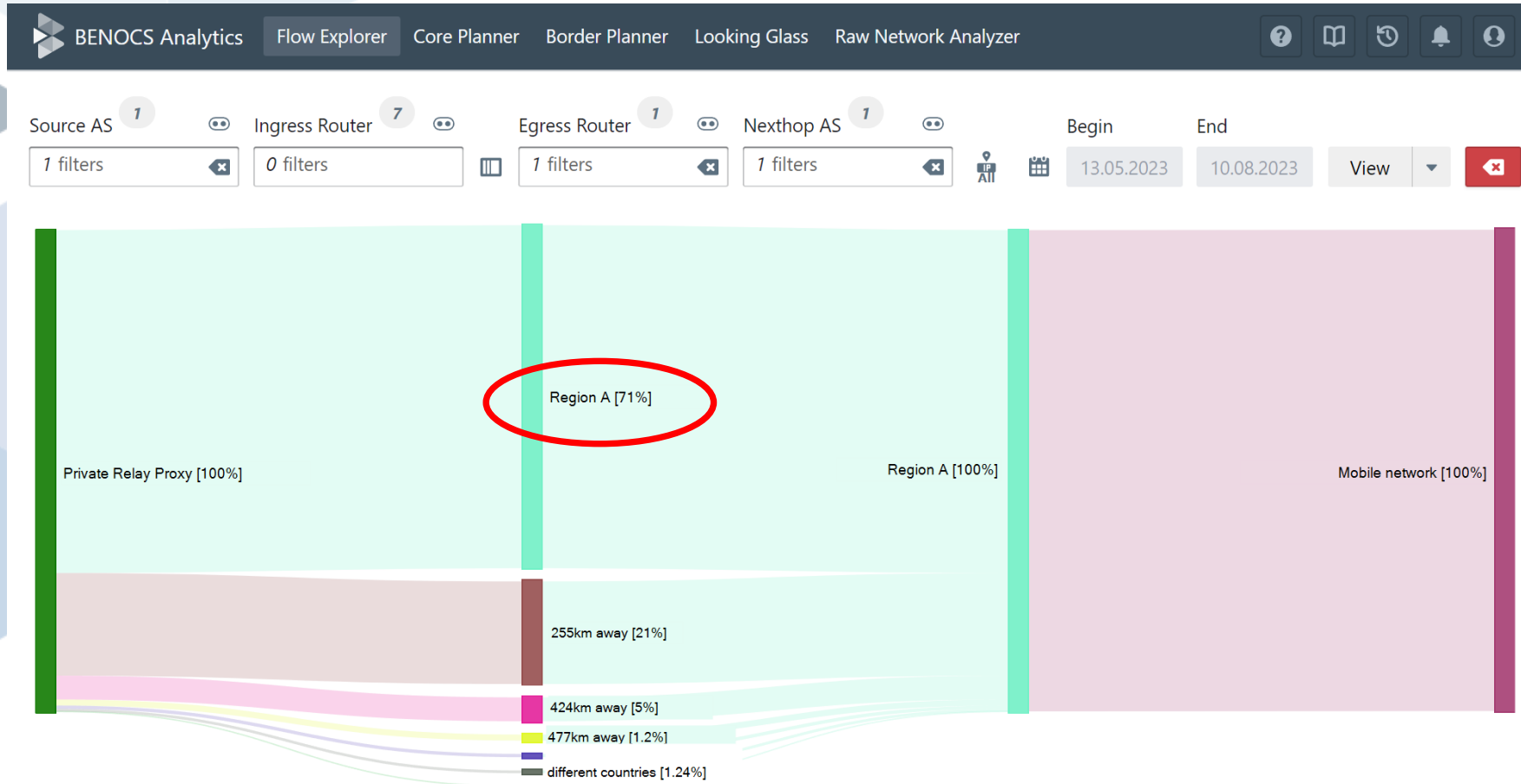
Result: Localization of private relay - fixed



Benchmark: localization of 5 CDNs - mobile



Result: Localization of Private relay-mobile



Our conclusion

Localization in private relay networks is not fully effective.

Potential reasons:

- Mapping via geo-hash depends on quality of geo-data
- Geo-distance does not always equal network distance.
- Volatility in localization: capacity/availability issues?
- Data might not be representative - traffic levels are low, traffic profile is limited.

Hari Jayaraman
hjayaraman@benocs.com

BENOCs GmbH

Reuchlinstr. 10, 10553 Berlin

+49 30 577 000 4 – 0

benocs.com

