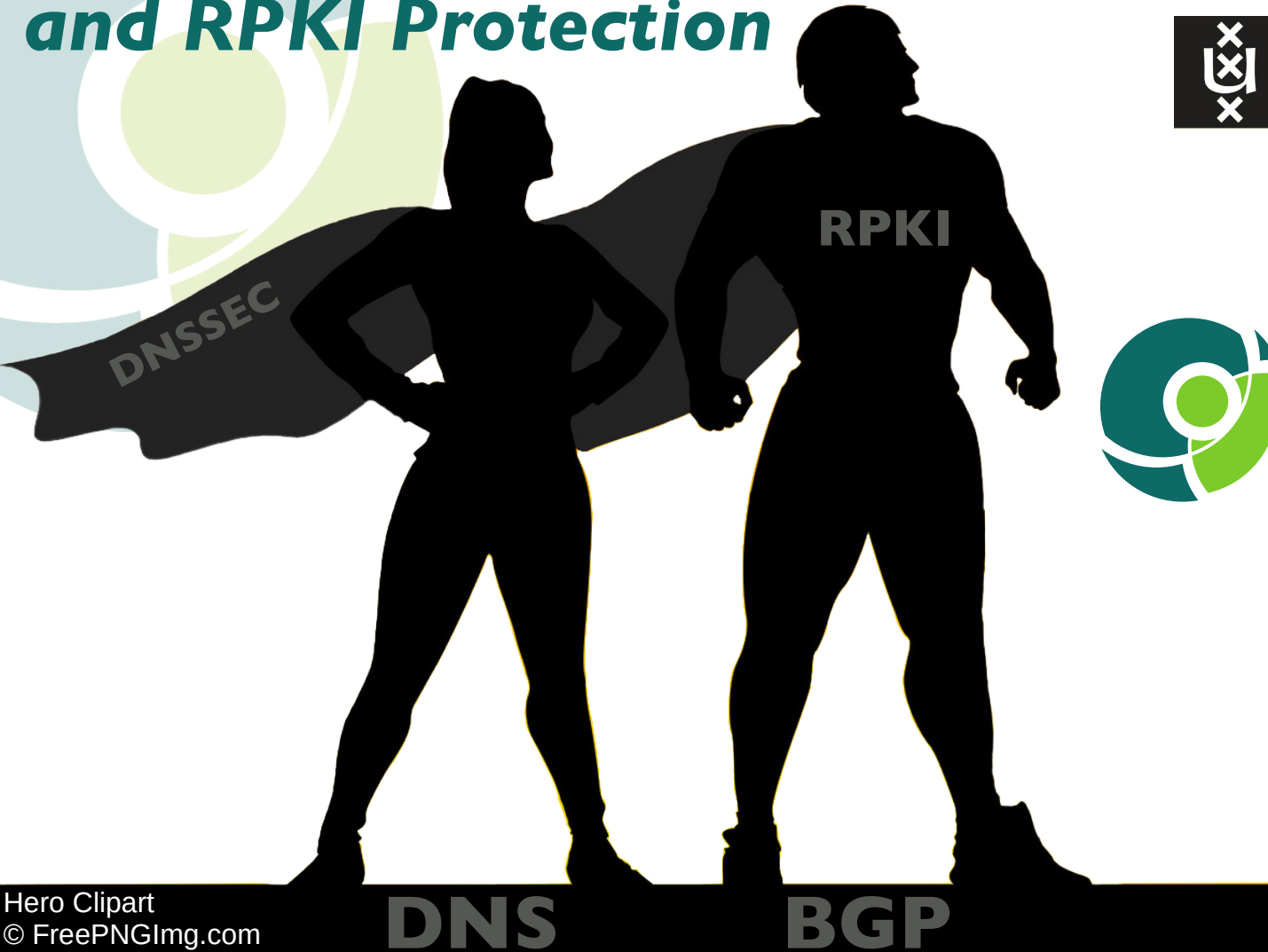


The Current State of DNS Resolvers and RPKI Protection



UNIVERSITY
OF AMSTERDAM

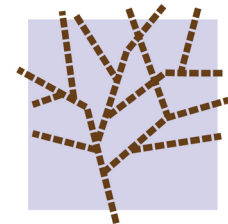
Erik Dekker

Marius Brouwer



NLNETLABS

Willem Toorop



DNS-OARC 32b

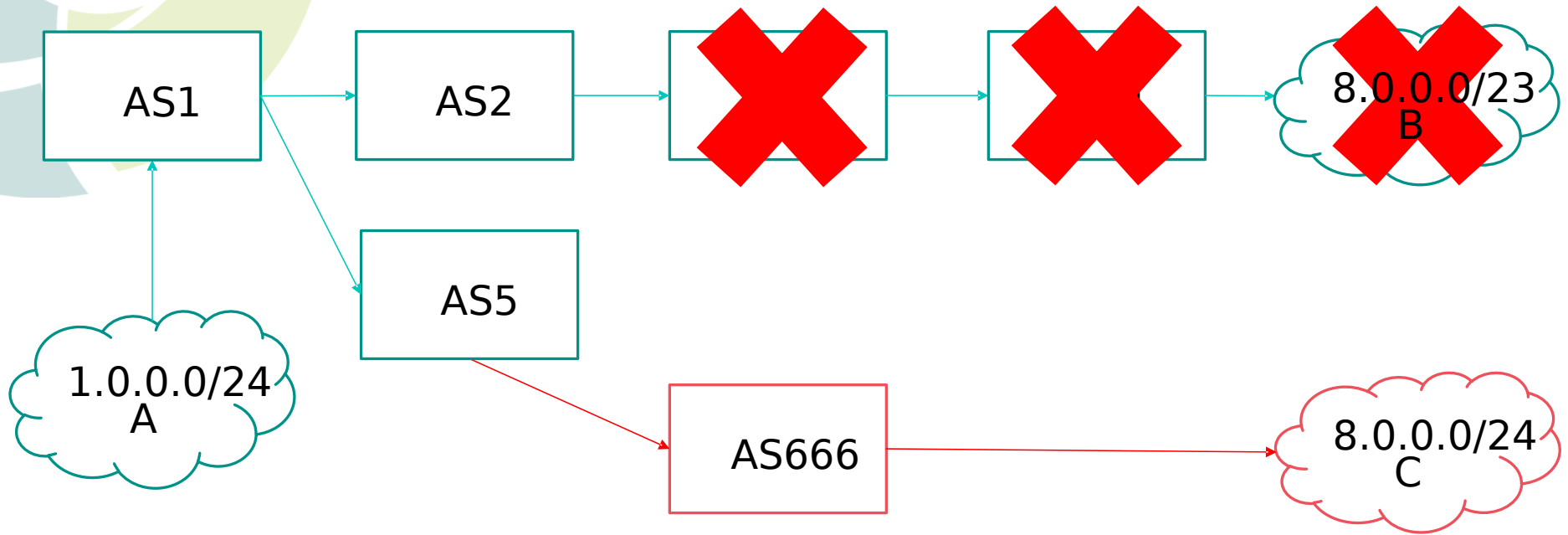
11 August 2020

Motivation

- DNSSEC protects against address forgery
- But the address can be trivially hijacked



RPKI 101

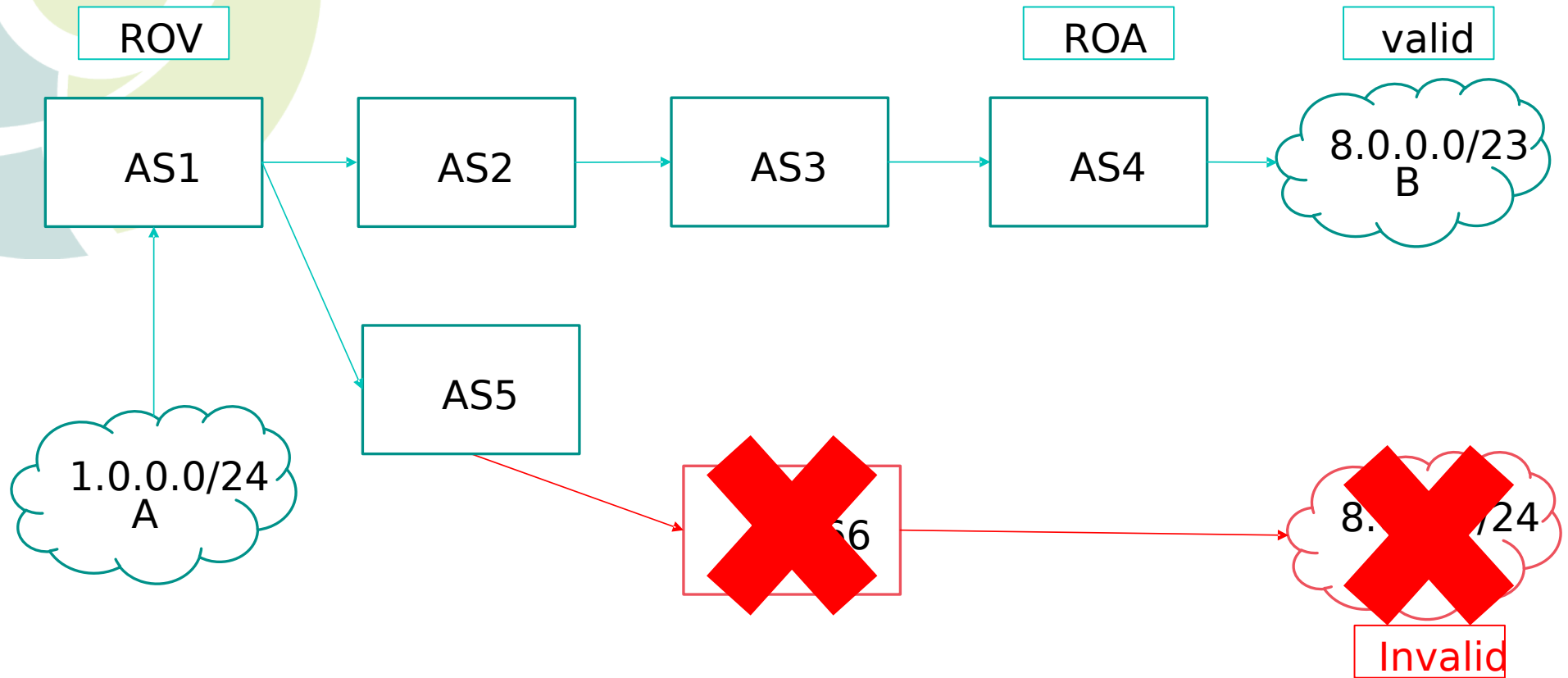


Motivation

- DNSSEC protects against address forgery
- But the address can be trivially hijacked
- RPKI to the rescue



RPKI 101



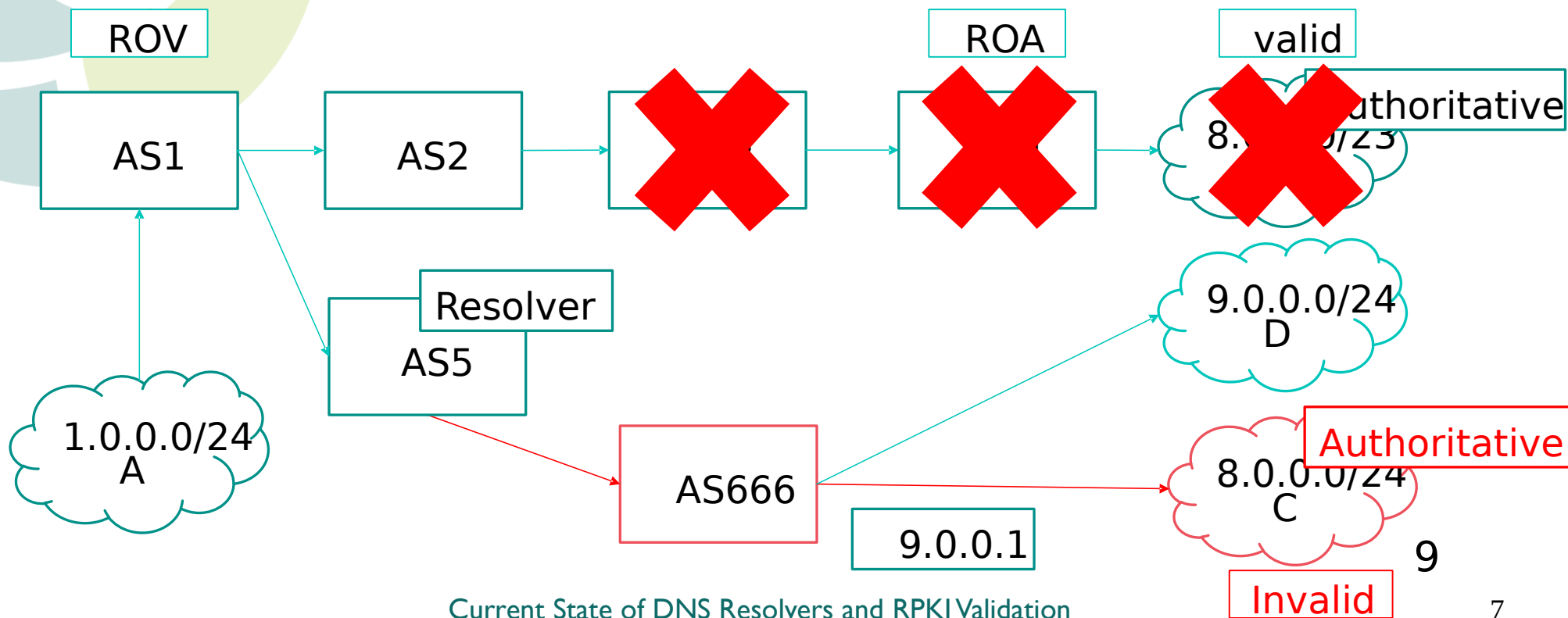


Motivation

- What does this have to do with DNS Resolvers?

Motivation

- What does this have to do with DNS Resolvers?



• What

ROV

AS1

1.0.0.0/
A

What Happened? The Amazon Route 53 BGP Hijack to Take Over Ethereum Cryptocurrency Wallets | Internet Society - Chromium

What Happened? The Am x +

internetociety.org/blog/2018/04/amazons-route-53-bgp-hijack/

Internet Society

Mutually Agreed Norms for Routing Security (MANRS) 27 April 2018

What Happened? The Amazon Route 53 BGP Hijack to Take Over Ethereum Cryptocurrency Wallets

By Aftab Siddiqui
Senior Manager, Internet Technology - Asia-Pacific

Yesterday, we published a blog post sharing the news and some initial details about [Amazon's DNS route hijack event to steal Ethereum cryptocurrency from myetherwallet.com](#). In this post, we'll explore more details about the incident from the BGP hijack's perspective.

vers?

authoritative

24

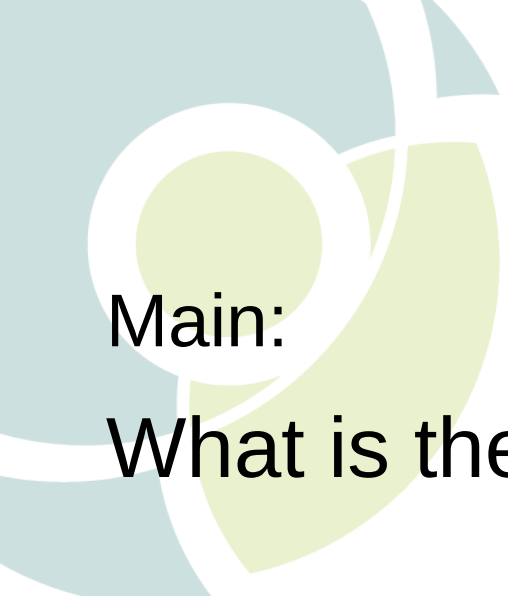
24

authoritative

24

9

invalid



Research question

Main:

What is the state of Route Origin Validation (RoV) on DNS resolvers?

Sub:

- Does the length of the AS path matter?
- How does anycast influence the protection?

Test setup

```
$ORIGIN rootcanary.net
$TTL 60
@      SOA  ns1.surfnet.nl. (
            dns-beheer.surfnet.nl.
            2020080503 ; serial
            10800      ; refresh
            3600       ; retry
            604800     ; expire
            86400      ; minimum
            )
NS      ns1.surfnet.nl.
NS      ns2.surfnet.nl.
NS      ns3.surfnet.nl.
NS      ns1.zurich.surf.net.

$TTL 25200

valid4   NS      valid4
valid4   A        209.24.1.6

invalid4 NS      invalid4
invalid4 A        194.32.71.6
```

```
$ORIGIN valid4.rootcanary.net
$TTL 300
@      SOA  valid4.rootcanary.net. (
            sysadm.rootcanary.org.
            2020012100 10800 3600
            604800 300 )
NS      @
A        209.24.1.6

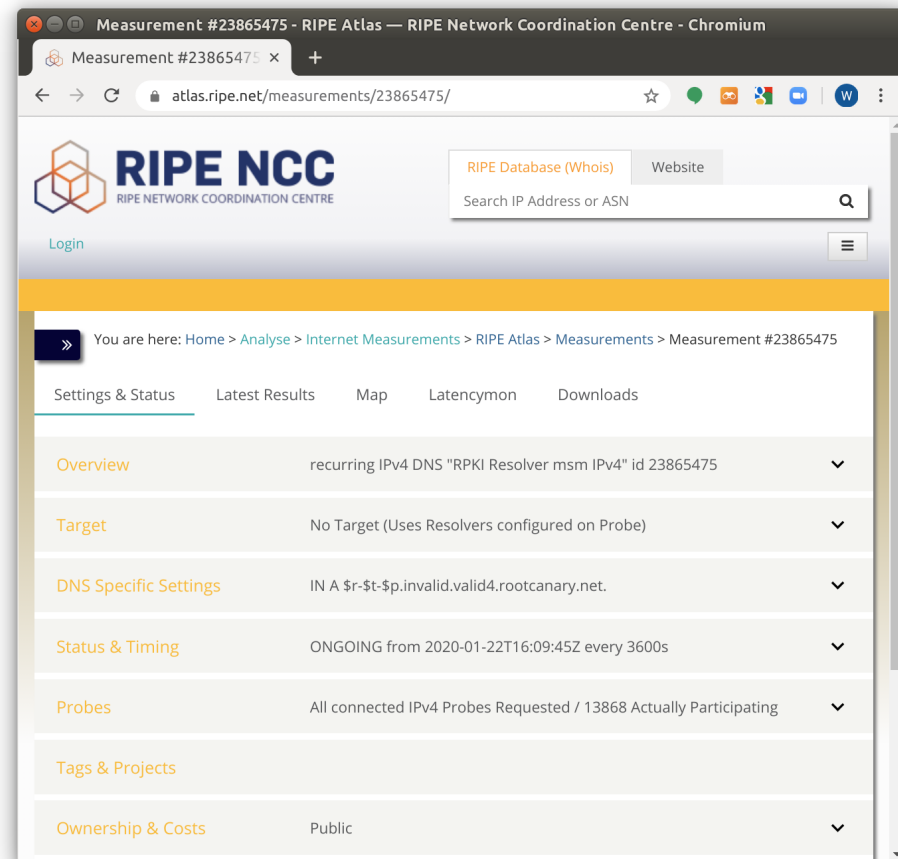
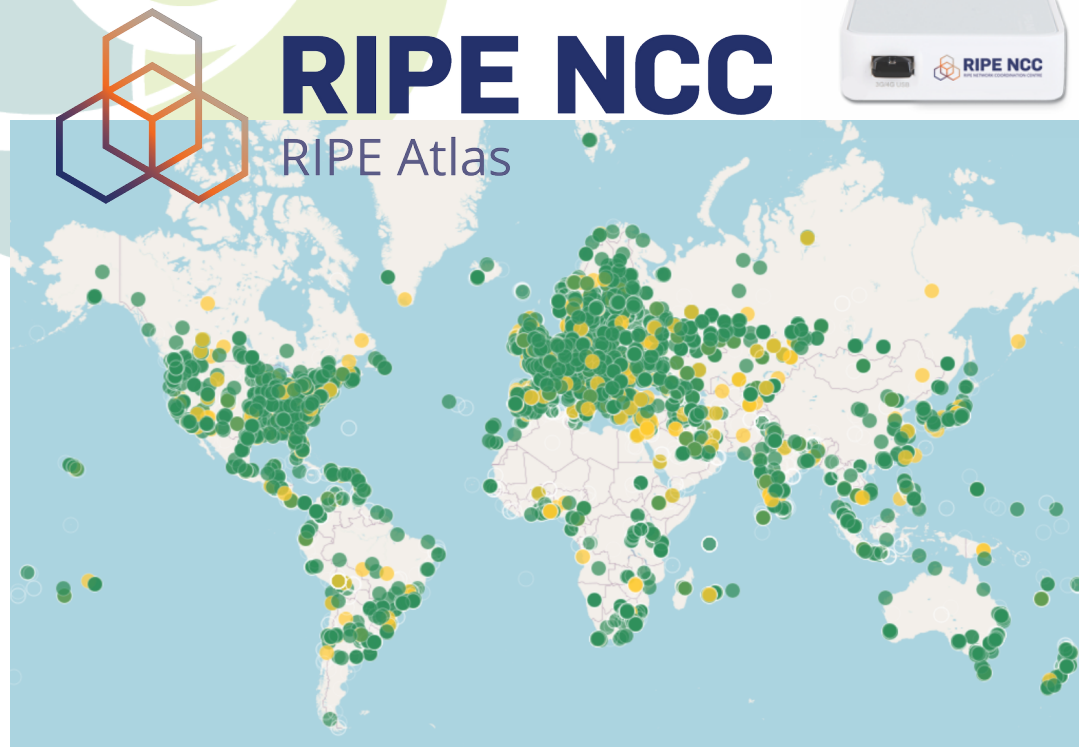
$TTL 1
invalid  DNAME invalid4.rootcanary.net.
```

```
$ORIGIN invalid4.rootcanary.net
$TTL 300
@      SOA  invalid4.rootcanary.net. (
            sysadm.rootcanary.org.
            2020012100 10800 3600
            604800 300 )
NS      @
A        194.32.71.6
*        A        145.97.20.20
```

prefix	209.24.1.0/24
max len	24
ASN	15562

prefix	194.32.71.0/24
max len	24
ASN	0

Test setup





You are here: [Home](#) > [Analyse](#) > [Internet Measurements](#) > [RIPE Atlas](#) > [Measurements](#) > Measurement #23865475

Settings & Status

Latest Results

Map

Latencymon

Downloads

Overview

recurring IPv4 DNS "RPKI Resolver msm IPv4" id 23865475



Target

No Target (Uses Resolvers configured on Probe)



DNS Specific Settings

IN A \$r-\$t-\$p.invalid.valid4.rootcanary.net.



Status & Timing

ONGOING from 2020-01-22T16:09:45Z every 3600s



Probes

All connected IPv4 Probes Requested / 13868 Actually Participating



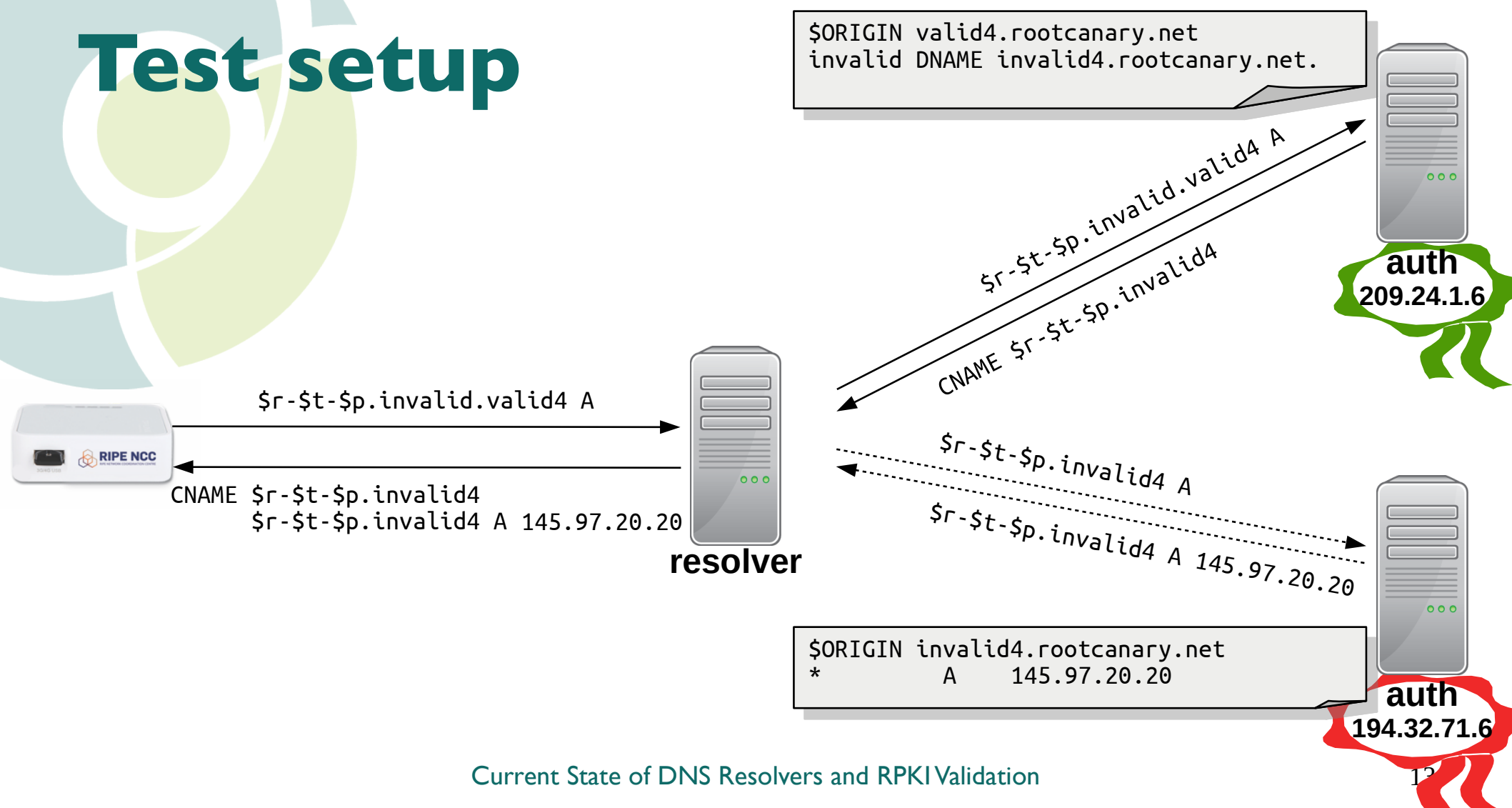
Tags & Projects

Ownership & Costs

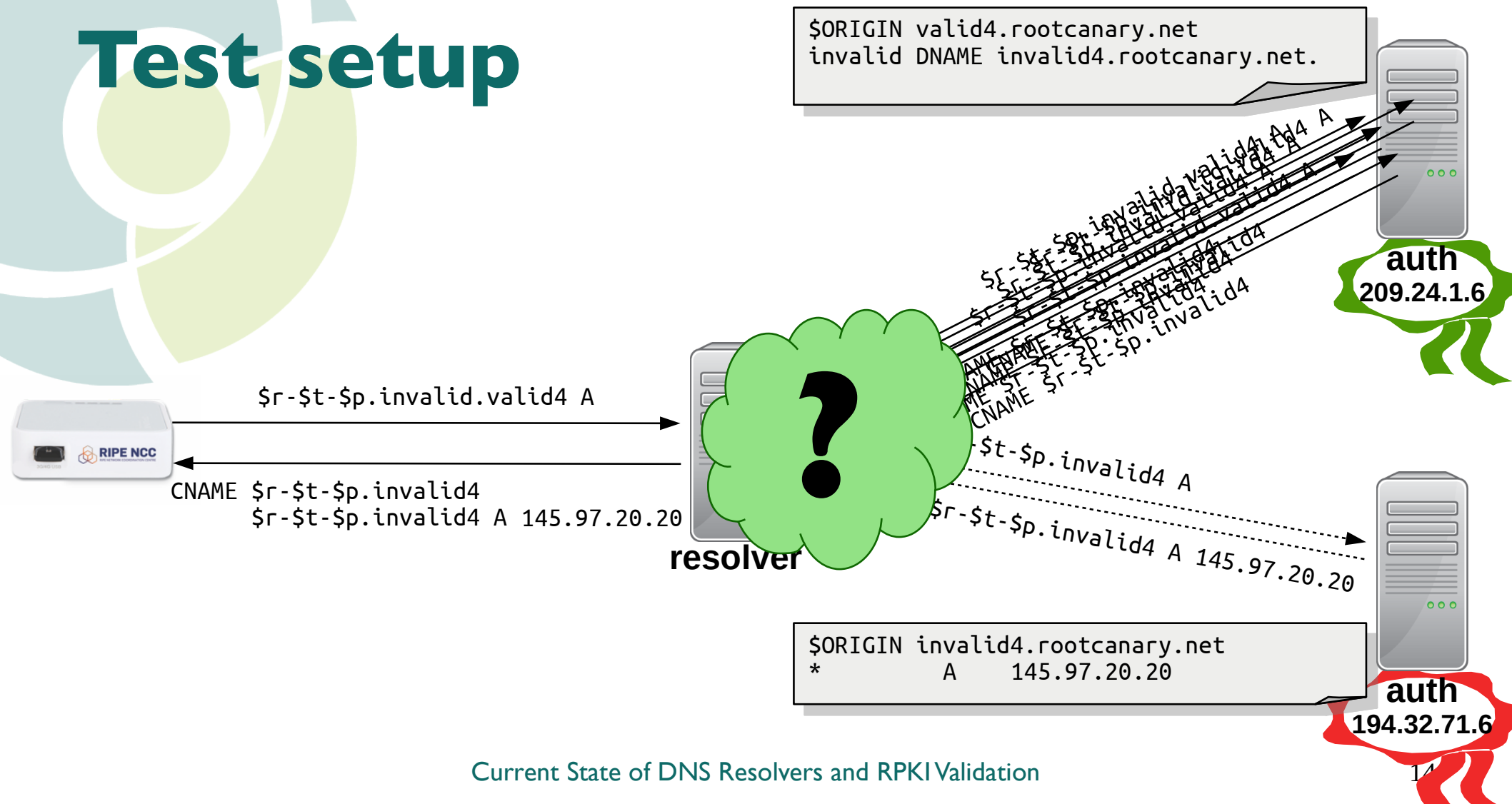
Public

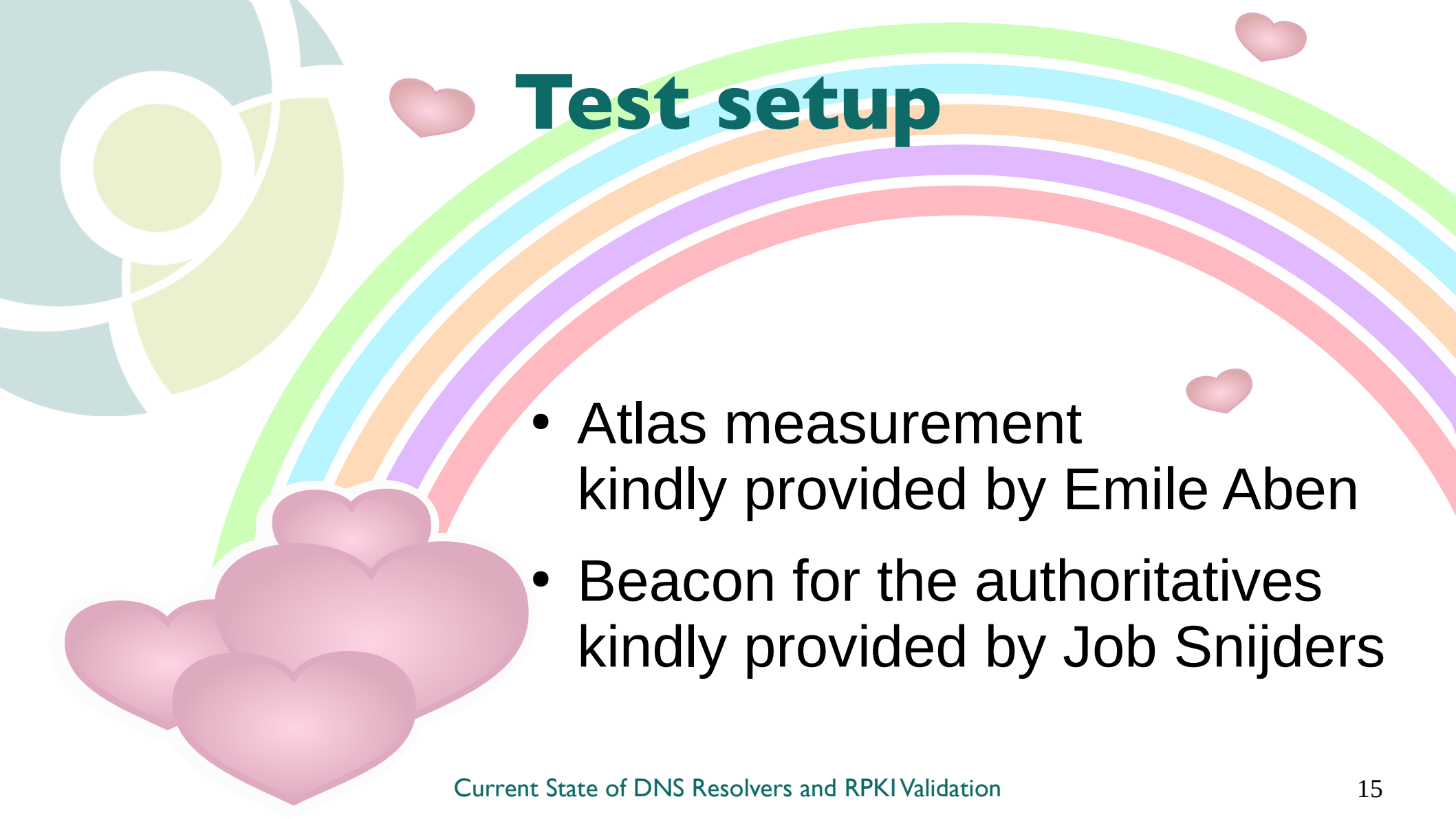


Test setup



Test setup



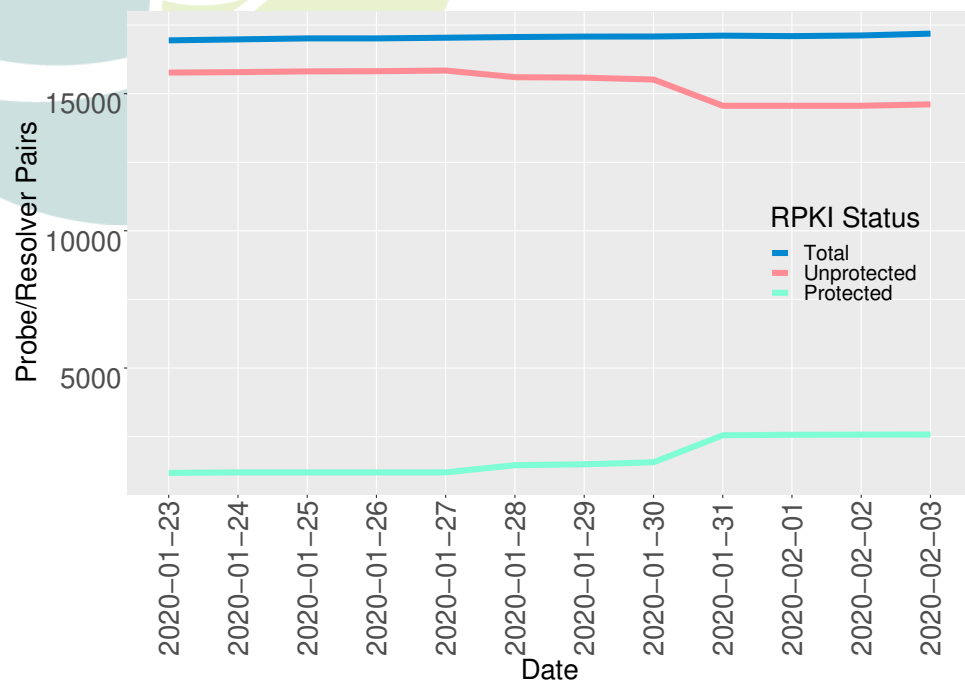


Test setup

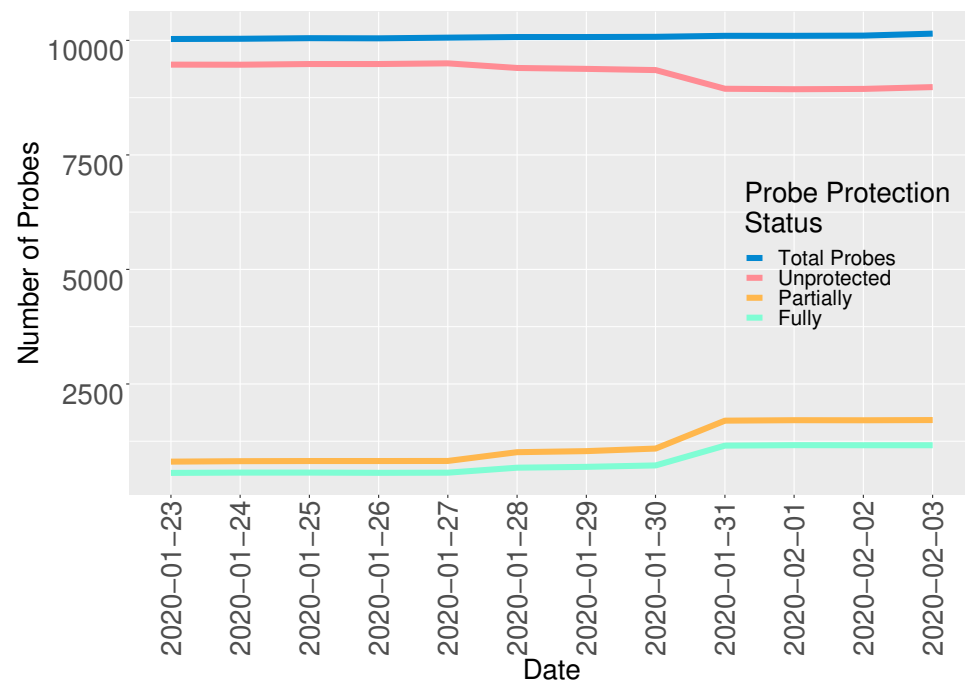
- Atlas measurement kindly provided by Emile Aben
- Beacon for the authoritatives kindly provided by Job Snijders

Results

Probe/resolver pair

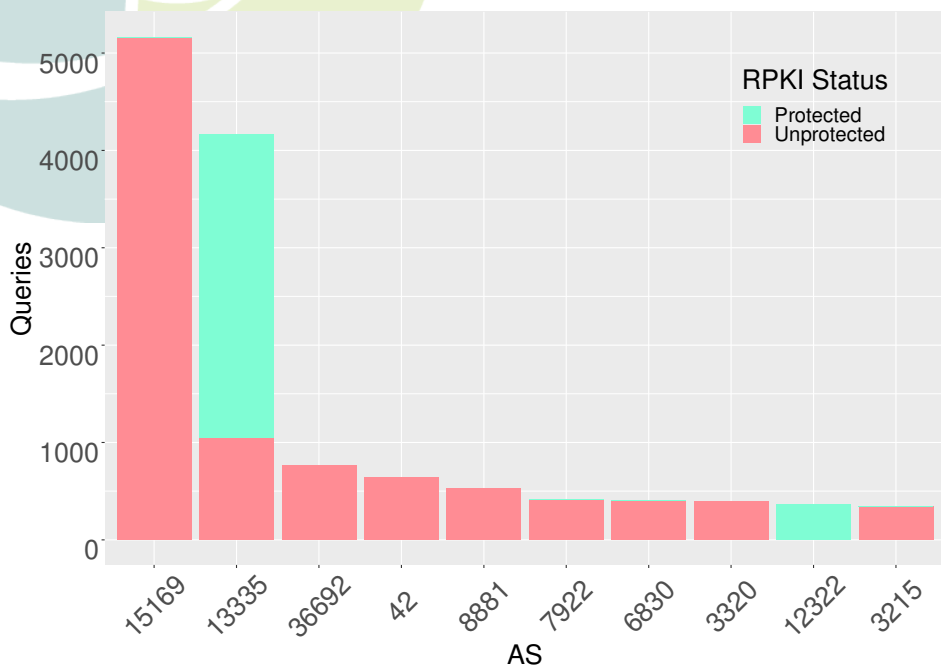


Probe time series

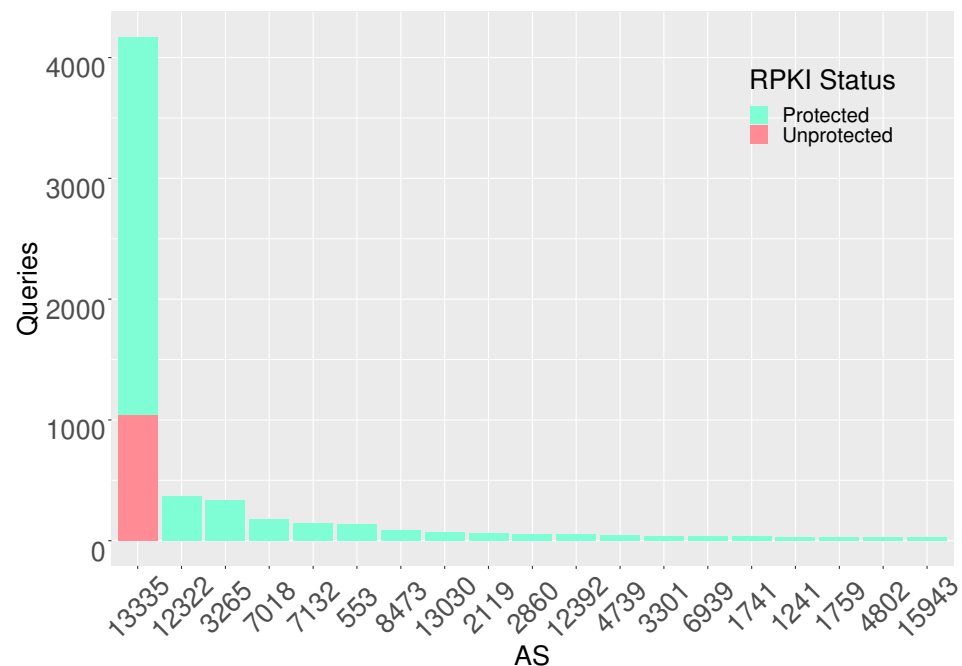


Results

Top ten most popular ASes



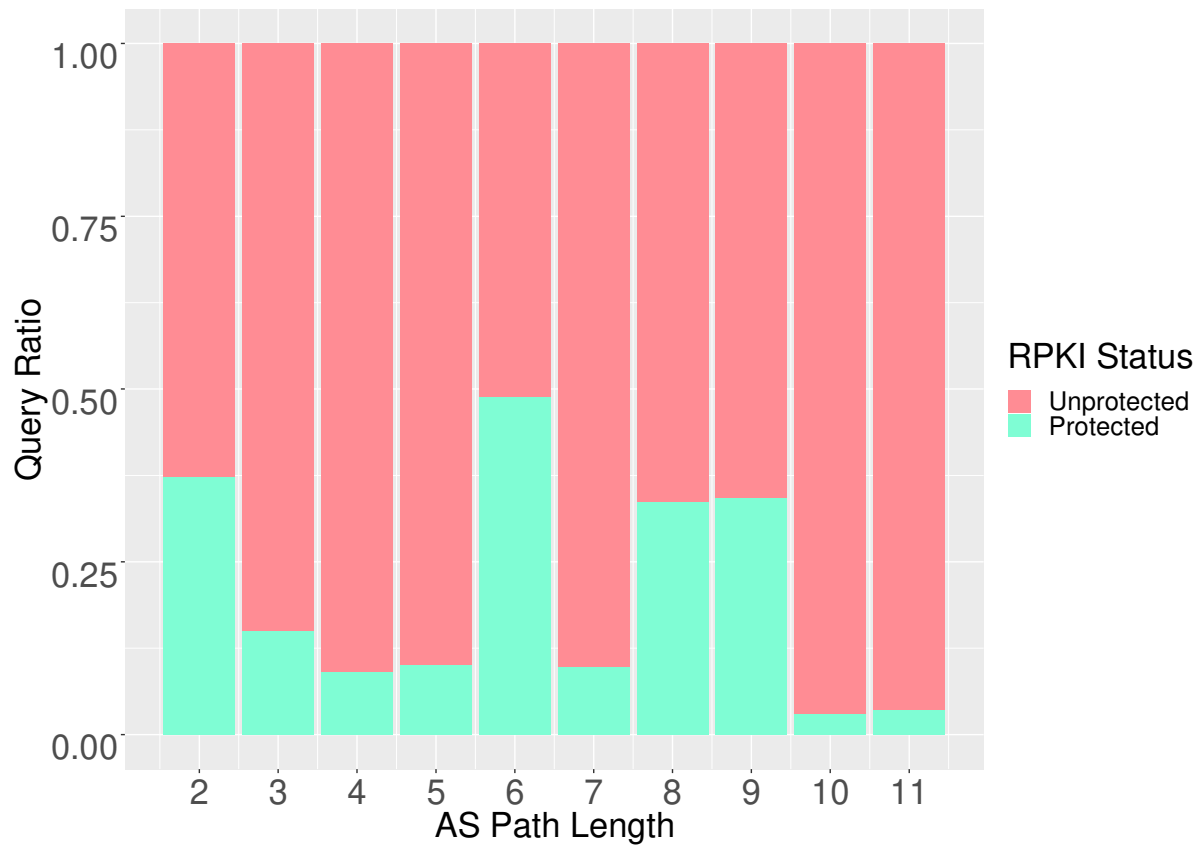
Top ten most protected ASes



Results

Sub RQ: Does the length of the AS path matter?

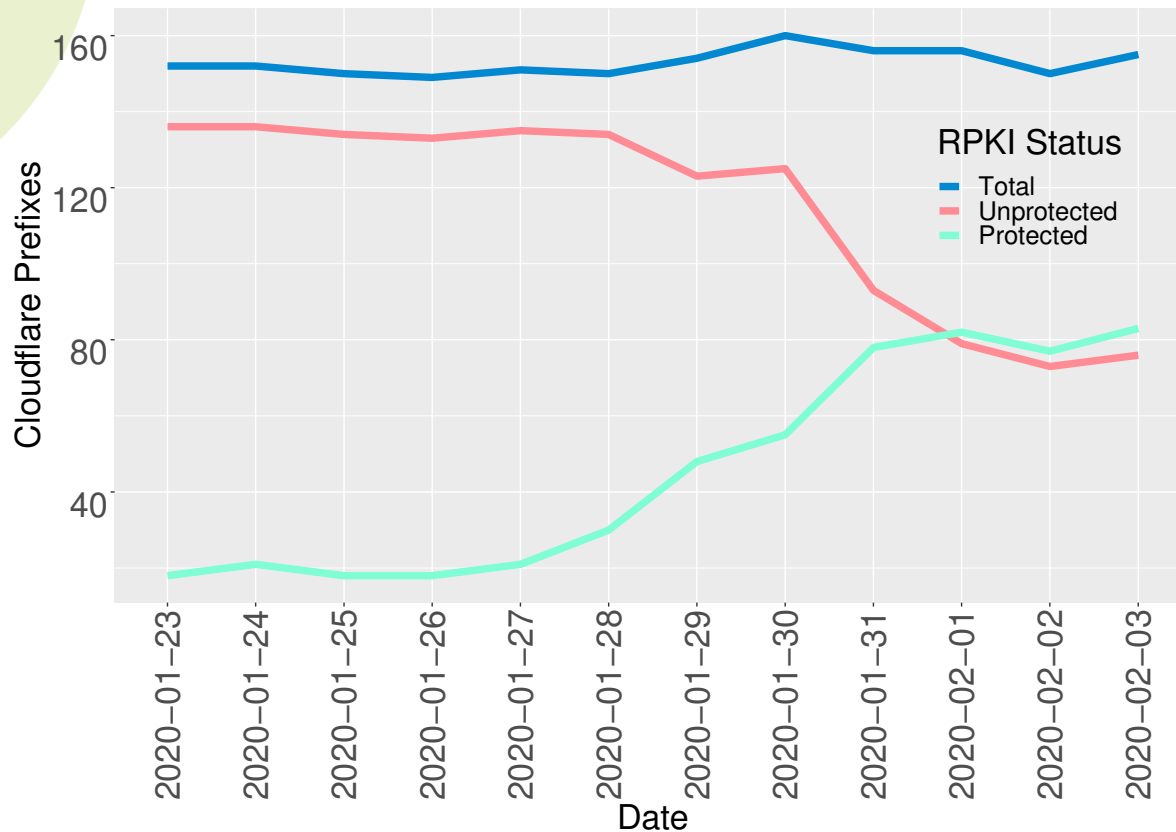
Relationship RPKI protection and AS path length



Results

Sub RQ: How does anycast influence protection?

Cloudflare resolver prefix time series



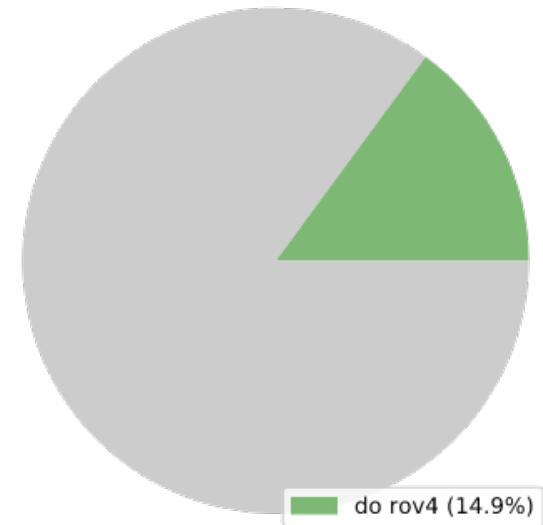
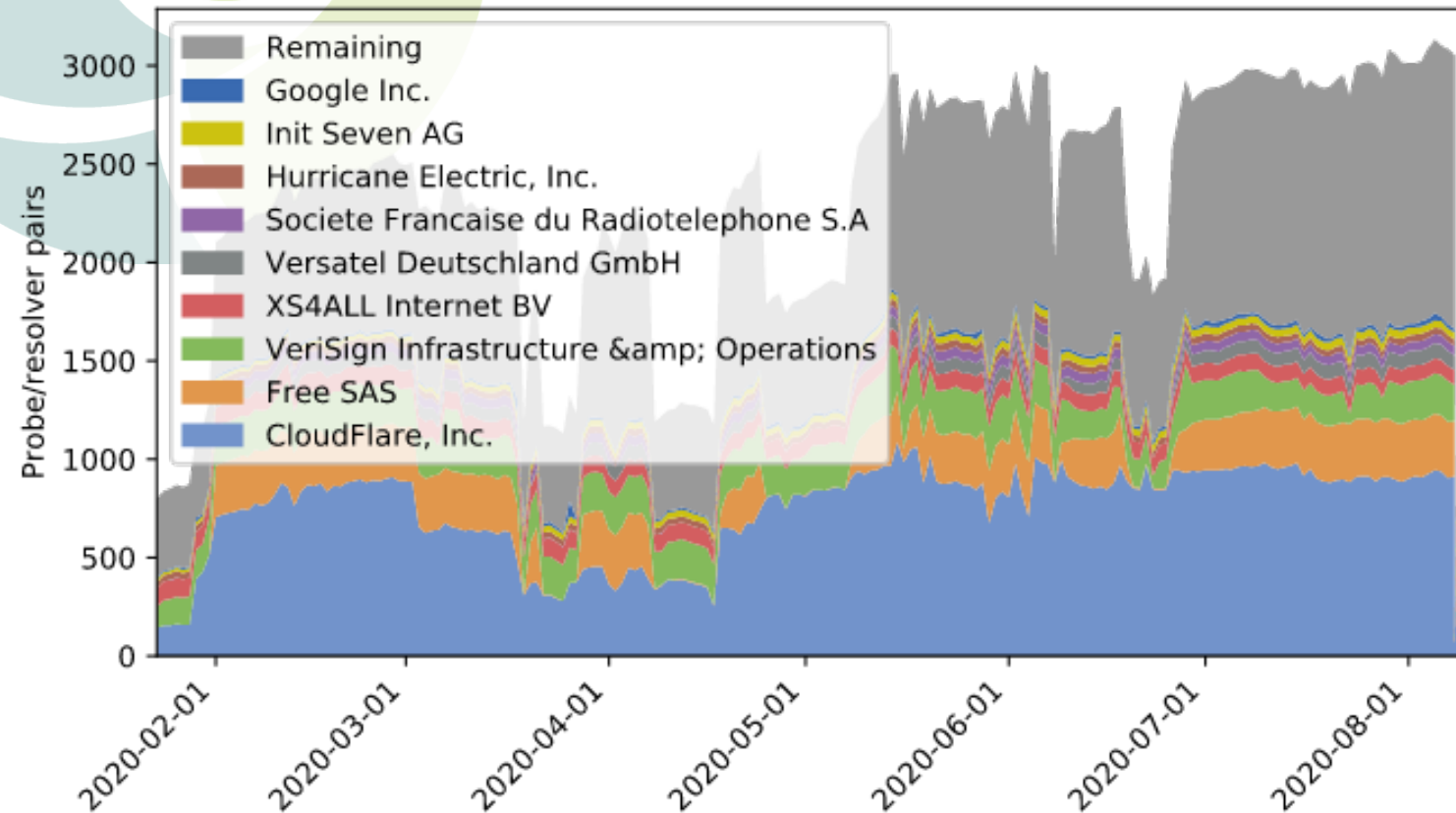
Current situation / IPv6



DNSThought

DNSThought

https://dnsthought.nlnetlabs.nl/does_rov4/#top_auth_asns



Test setup

```
$ORIGIN rootcanary.net
$TTL 60
@      SOA  ns1.surfnet.nl. (
            dns-beheer.surfnet.nl.
            2020080503 ; serial
            10800      ; refresh
            3600       ; retry
            604800     ; expire
            86400      ; minimum
            )
NS      ns1.surfnet.nl.
NS      ns2.surfnet.nl.
NS      ns3.surfnet.nl.
NS      ns1.zurich.surf.net.
```

```
$TTL 25200
```

```
valid6    NS    valid6
valid6    AAAA  2001:728:1808:5::6
```

```
invalid6  NS    invalid6
invalid6  AAAA  2001:7fb:fd04::6
```

```
$ORIGIN valid6.rootcanary.net
$TTL 300
@      SOA  valid6.rootcanary.net.
            sysadm.rootcanary.org.
            2020012100 10800 3600
            604800 300 )
NS      @
A      2001:728:1808:5::6
$TTL 1
invalid  DNAME invalid6.rootcanary.net.
```

```
$ORIGIN invalid6.rootcanary.net
$TTL 300
@      SOA  invalid6.rootcanary.net.
            sysadm.rootcanary.org.
            2020012100 10800 3600
            604800 300 )
NS      @
A      2001:7fb:fd04::6
*      A    2001:610:188:408::20
```

prefix	2001:728:1808::/48
max len	64
ASN	15562

prefix	2001:7fb:fd04::/48
max len	48
ASN	196615



Settings & Status

Latest Results

Map

Latencymon

Downloads

Overview

recurring IPv6 DNS "RPKI Resolver msm IPv6" id 23865476



Target

No Target (Uses Resolvers configured on Probe)



DNS Specific Settings

IN AAAA \$r-\$t-\$p.invalid.valid6.rootcanary.net.



Status & Timing

ONGOING from 2020-01-22T16:09:45Z every 3600s



Probes

All connected IPv6 Probes Requested / 6928 Actually Participating



Tags & Projects

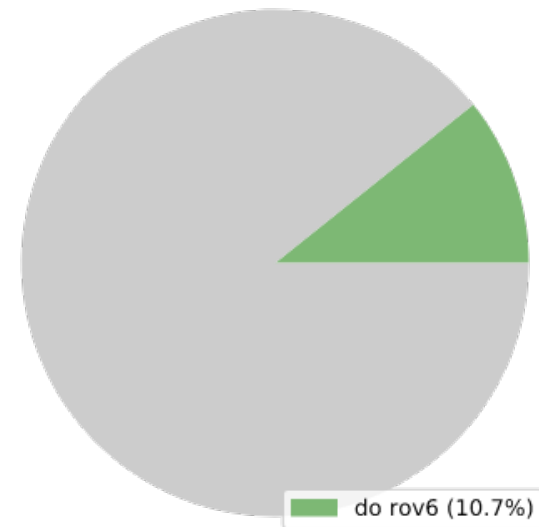
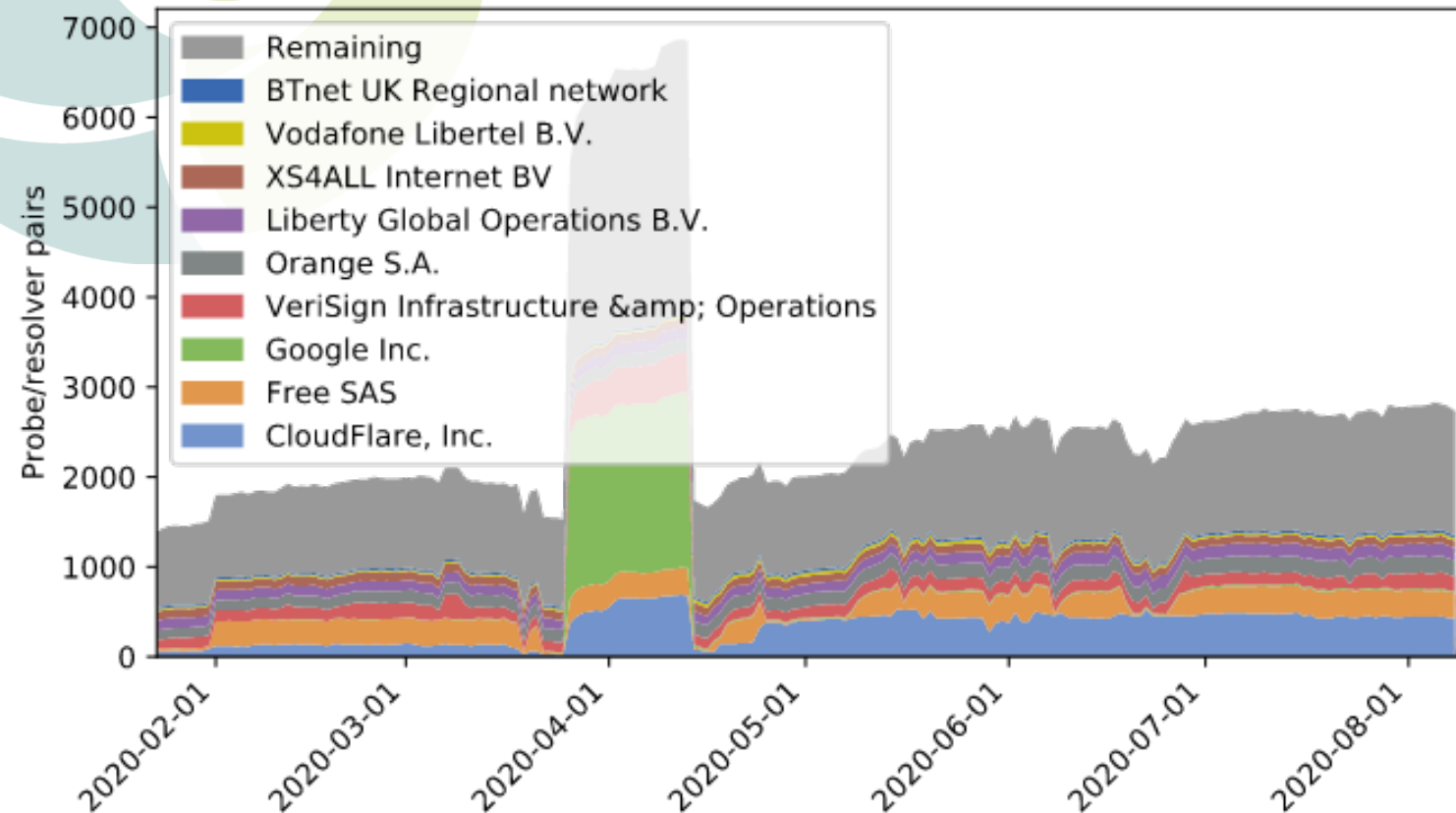
Ownership & Costs

Public



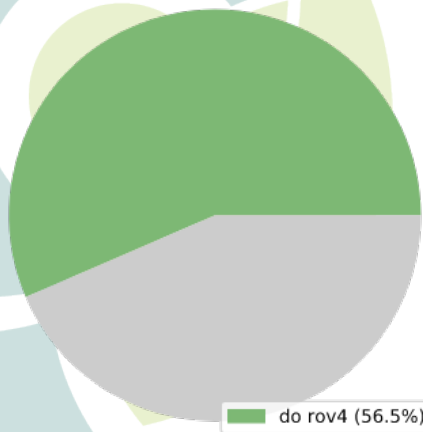
DNSThought

https://dnsthought.nlnetlabs.nl/does_rov6/#top_auth_asns

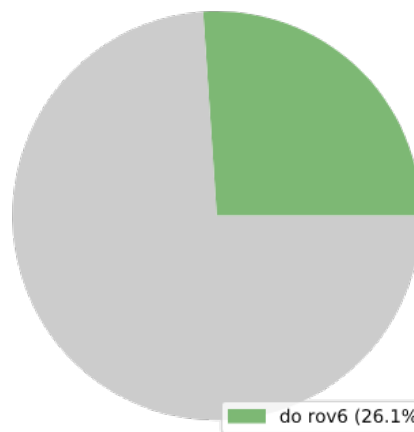
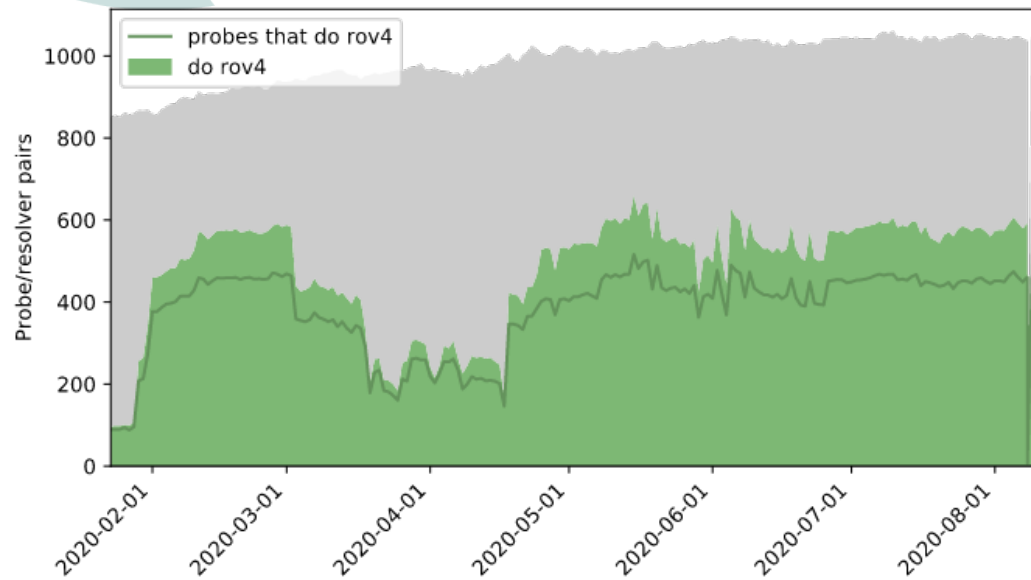


DNSThought

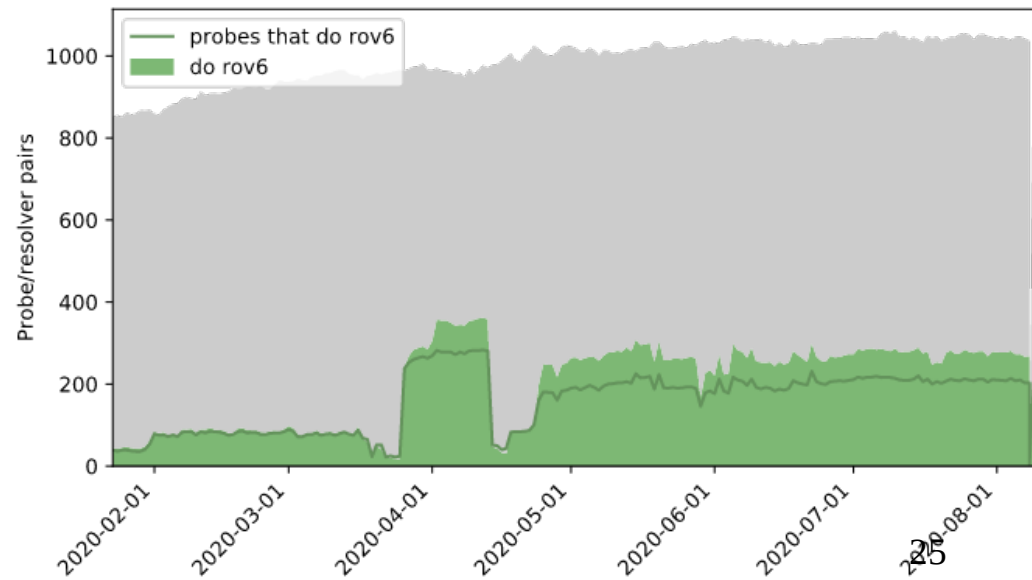
AS I3335
Cloudflare



IPv4

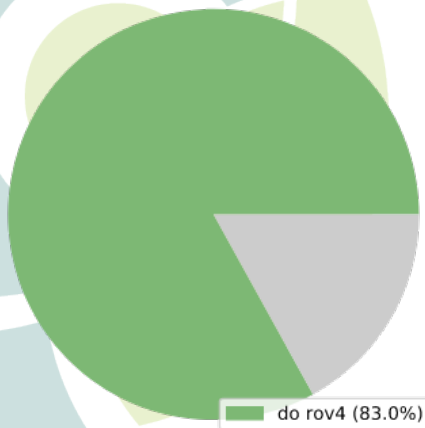


IPv6

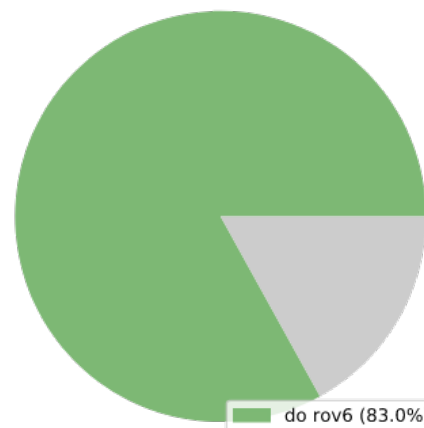
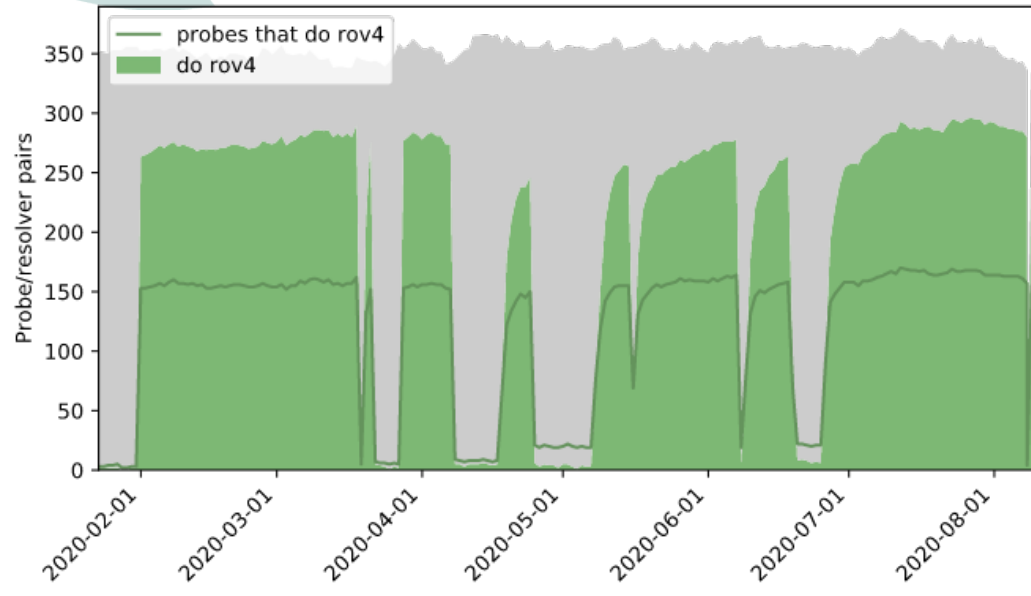


DNSThought

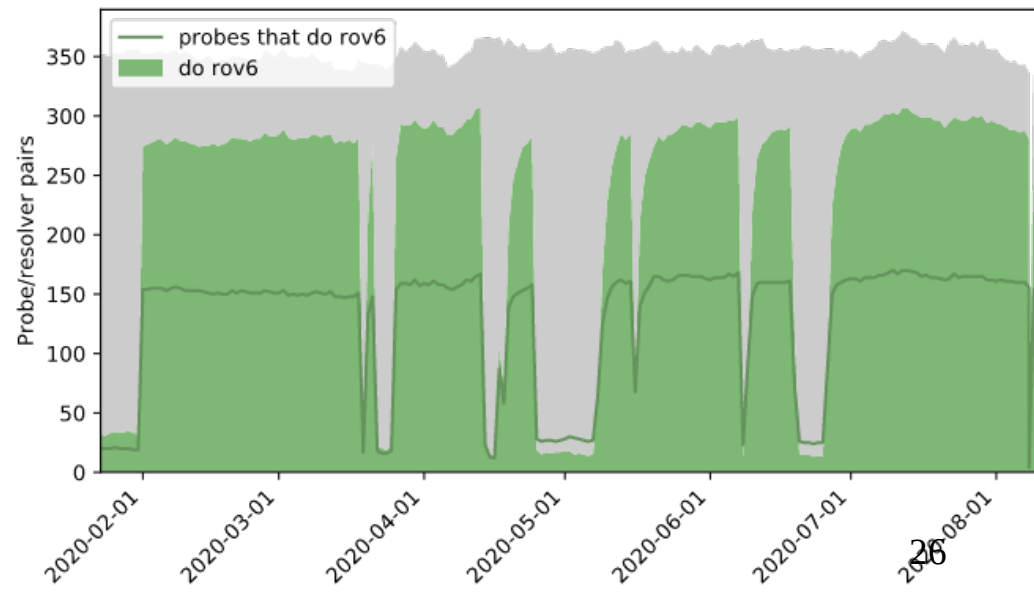
ASI2322
Free SAS



IPv4



IPv6





Questions?

- Research performed by:
 - Erik Dekker <Erik.Dekker@os3.nl>
 - Marius Brouwer <mbrouwer@os3.nl>
- From
 -  UNIVERSITY OF AMSTERDAM
- At
 -  **NLNETLABS**
- On
 - January 2020
- Report:
 - <https://delaat.net/rp/2019-2020/p04/report.pdf>
- DNSThought:
 - <https://dnsthought.nlnetlabs.nl/>