The Current State of DNS Resolvers and RPKI Protection

Hero Clipart
© FreePNGImg.com

University of Amsterdam
Erik Dekker
Marius Brouwer

NLnetLabs
Willem Toorop

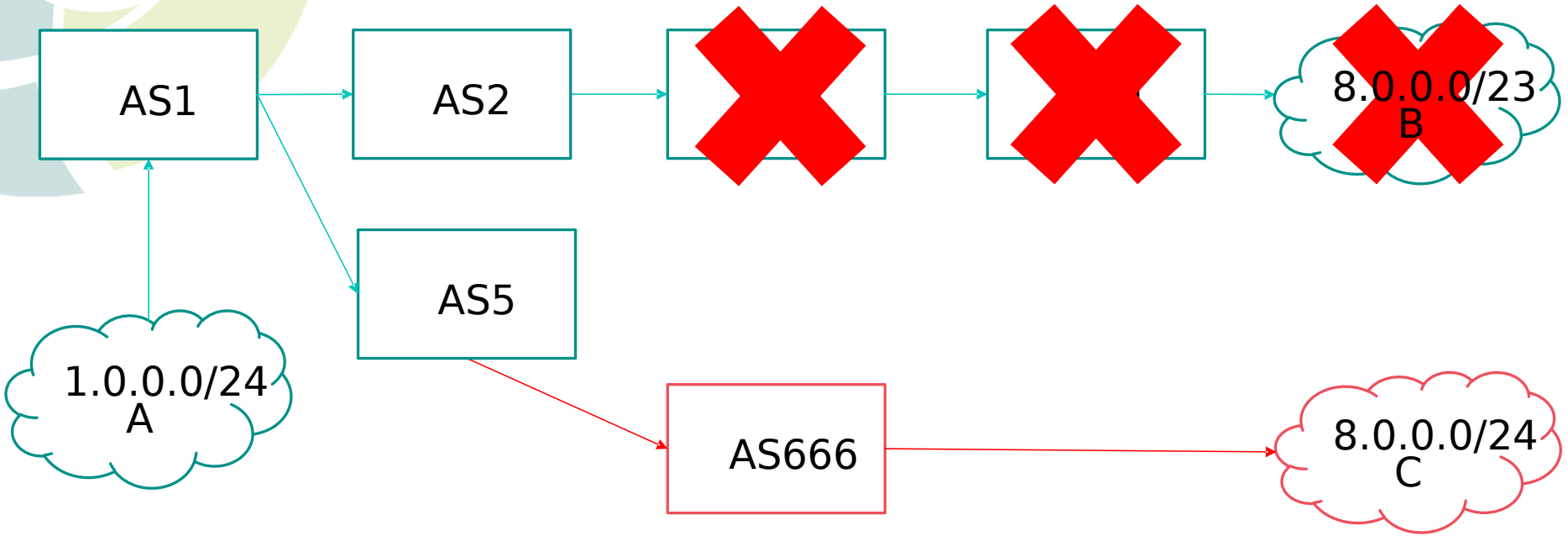
DNS-OARC 32b

11 August 2020

Motivation

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

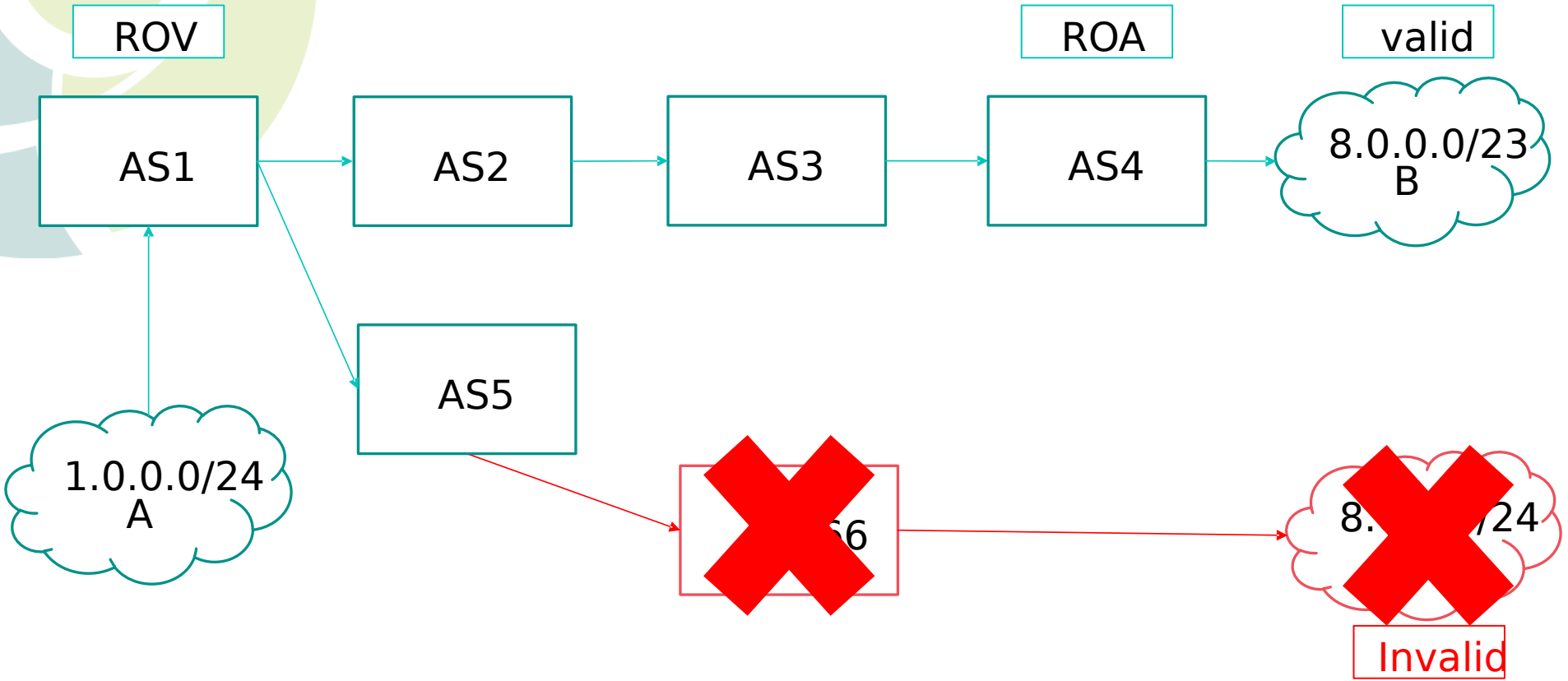
RPKI 101



Motivation

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

RPKI 101

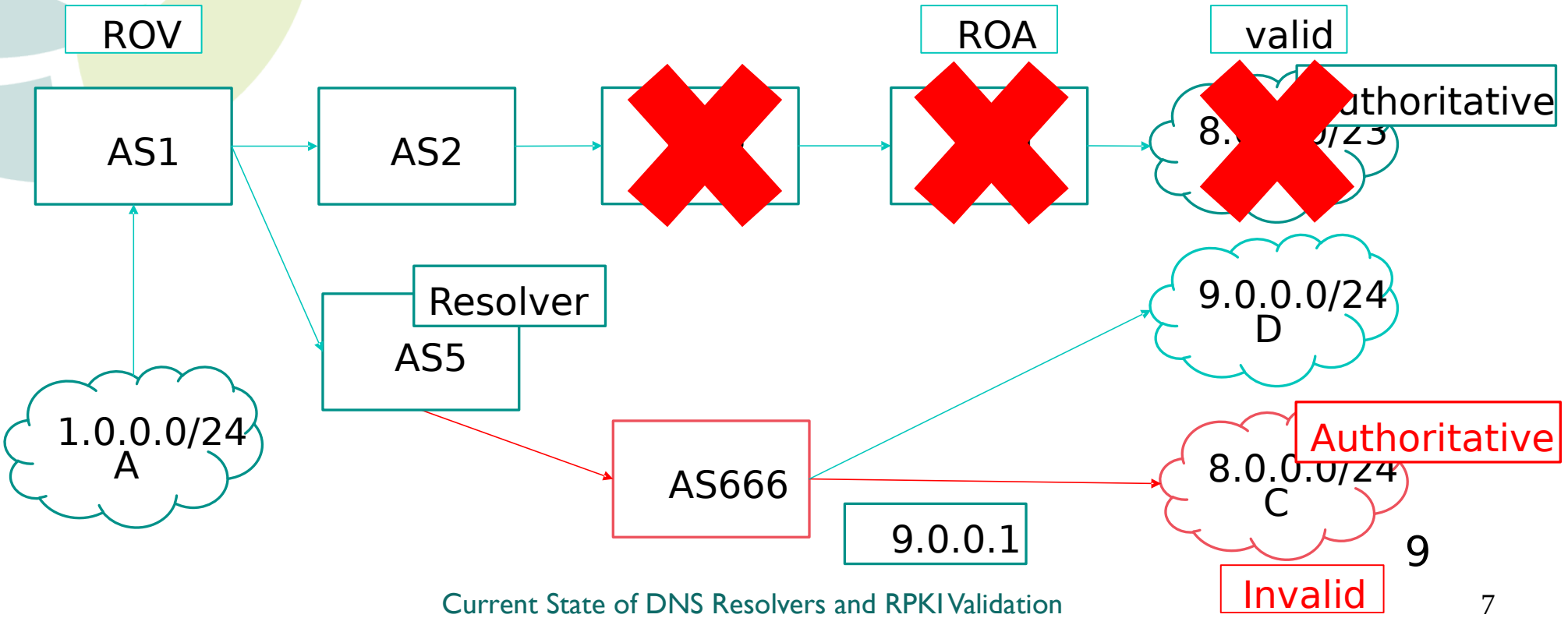


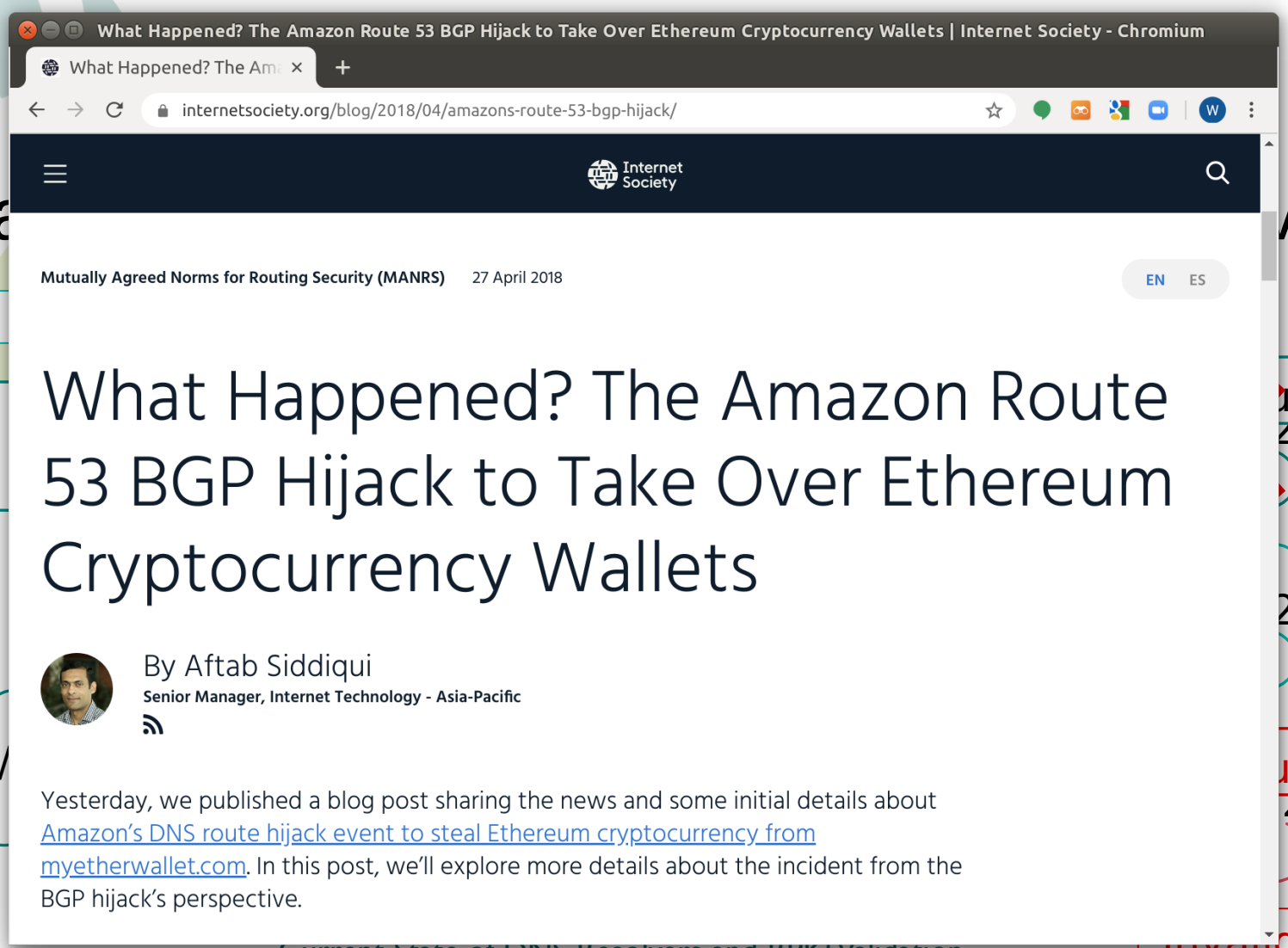
Motivation

- What does this have to do with DNS Resolvers?

Motivation

- What does this have to do with DNS Resolvers?





- Wha

ROV

AS1

1.0.0.0/
A

thoritative
24
24
thoritative
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.
```

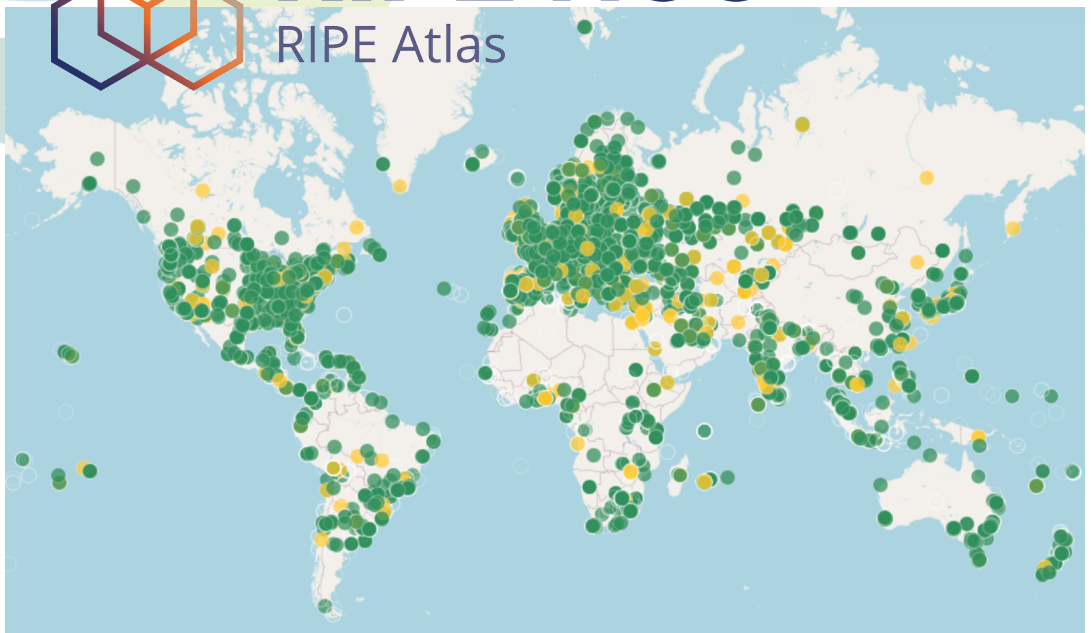
```
$ORIGIN invalid4.rootcanary.net
$TTL 300
@          SOA  invalid4.rootcanary.net. (
                sysadm.rootcanary.org.
                2020012100 10800 3600
                604800 300 )
           NS   @
           A    194.32.71.6
*          A    145.97.20.20
```

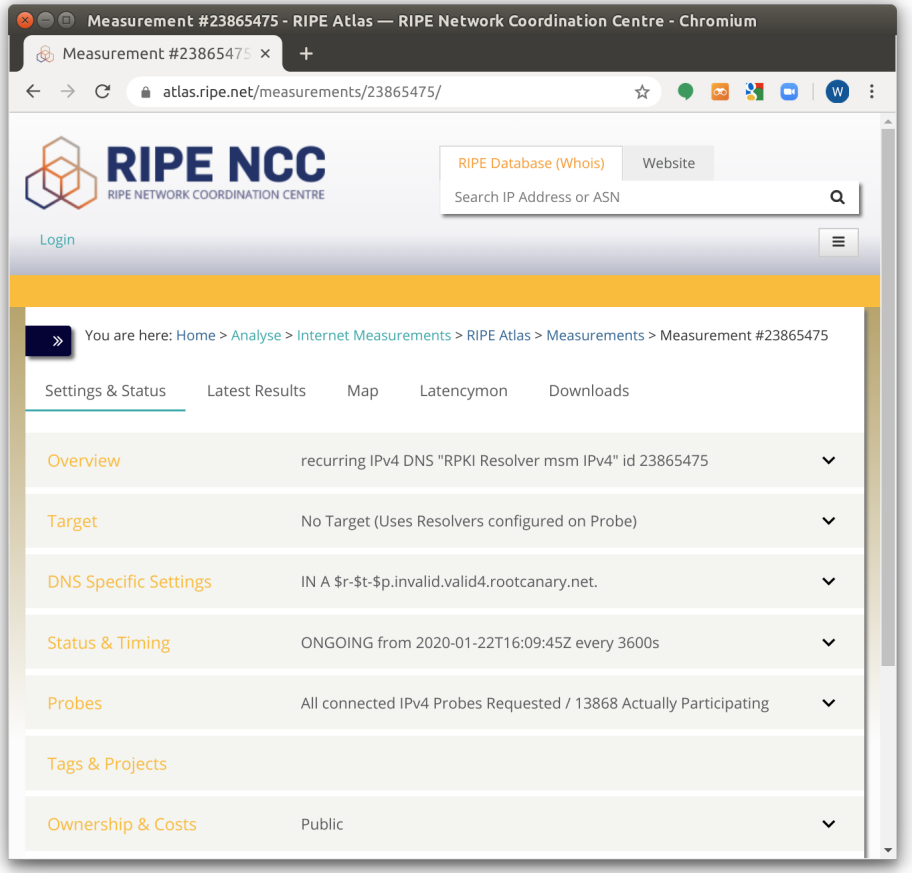
prefix	209.24.1.0/24
max len	24
ASN	15562

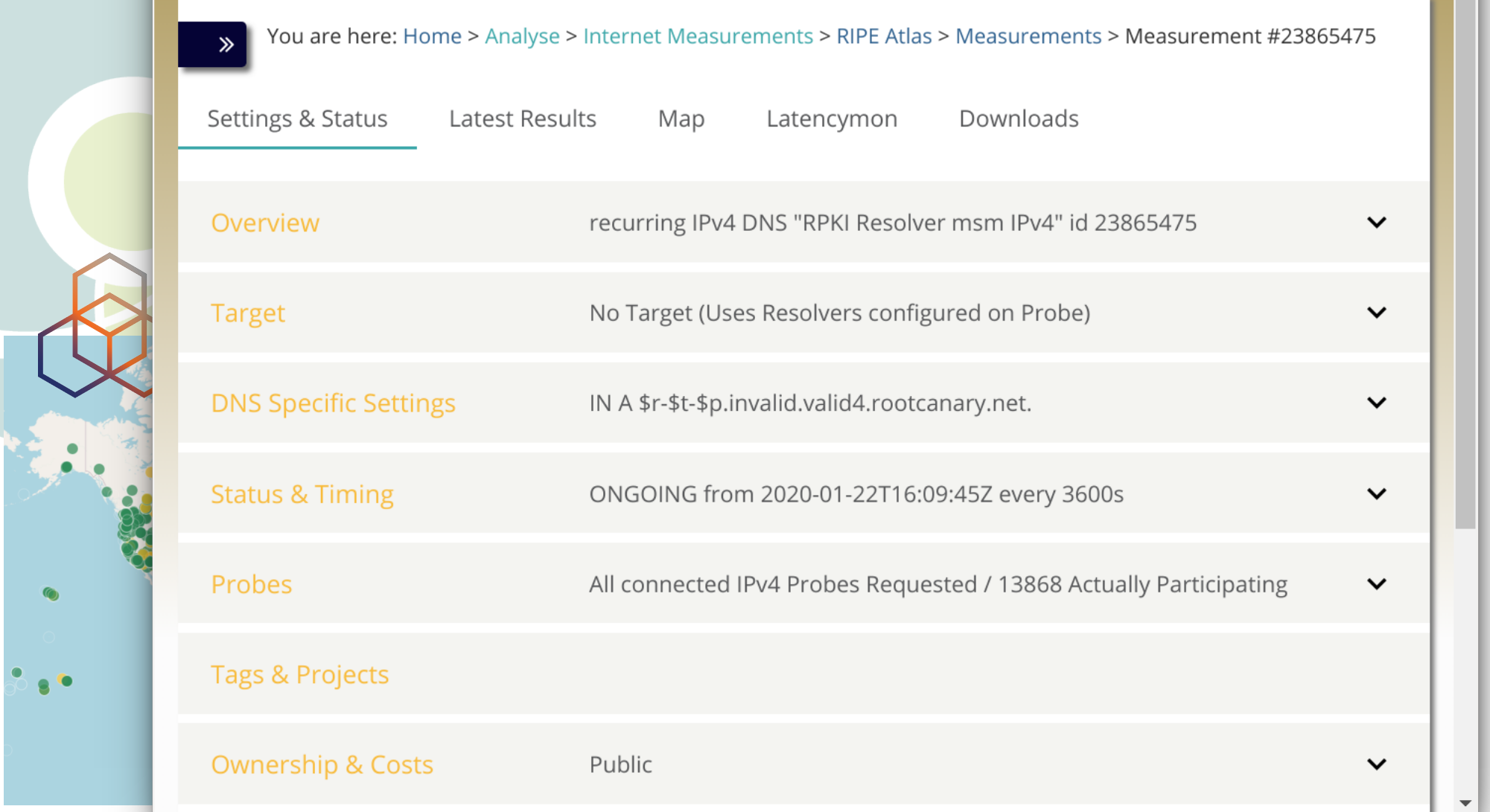
prefix	194.32.71.0/24
max len	24
ASN	0

Test setup

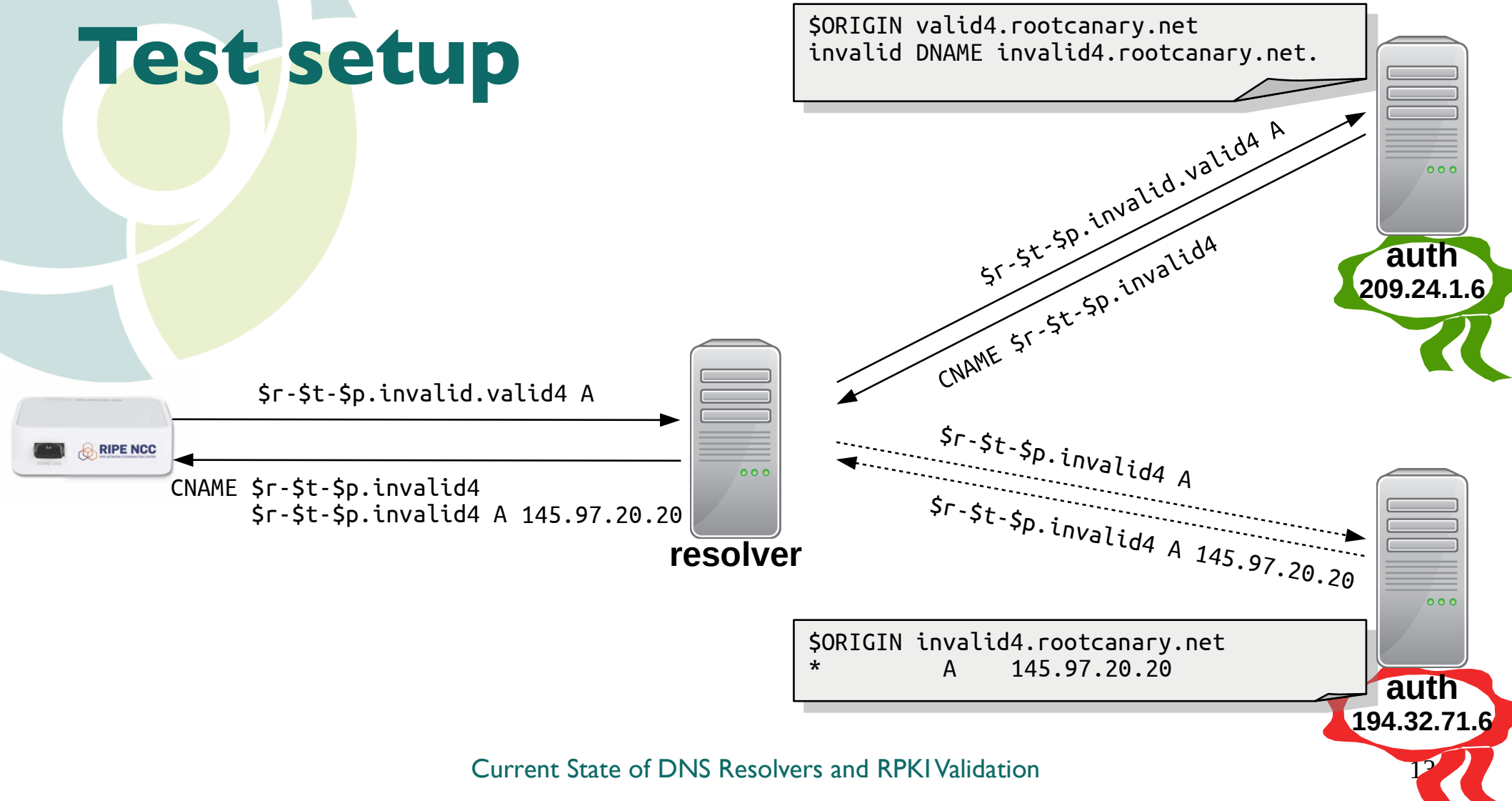
RIPE NCC
RIPE Atlas



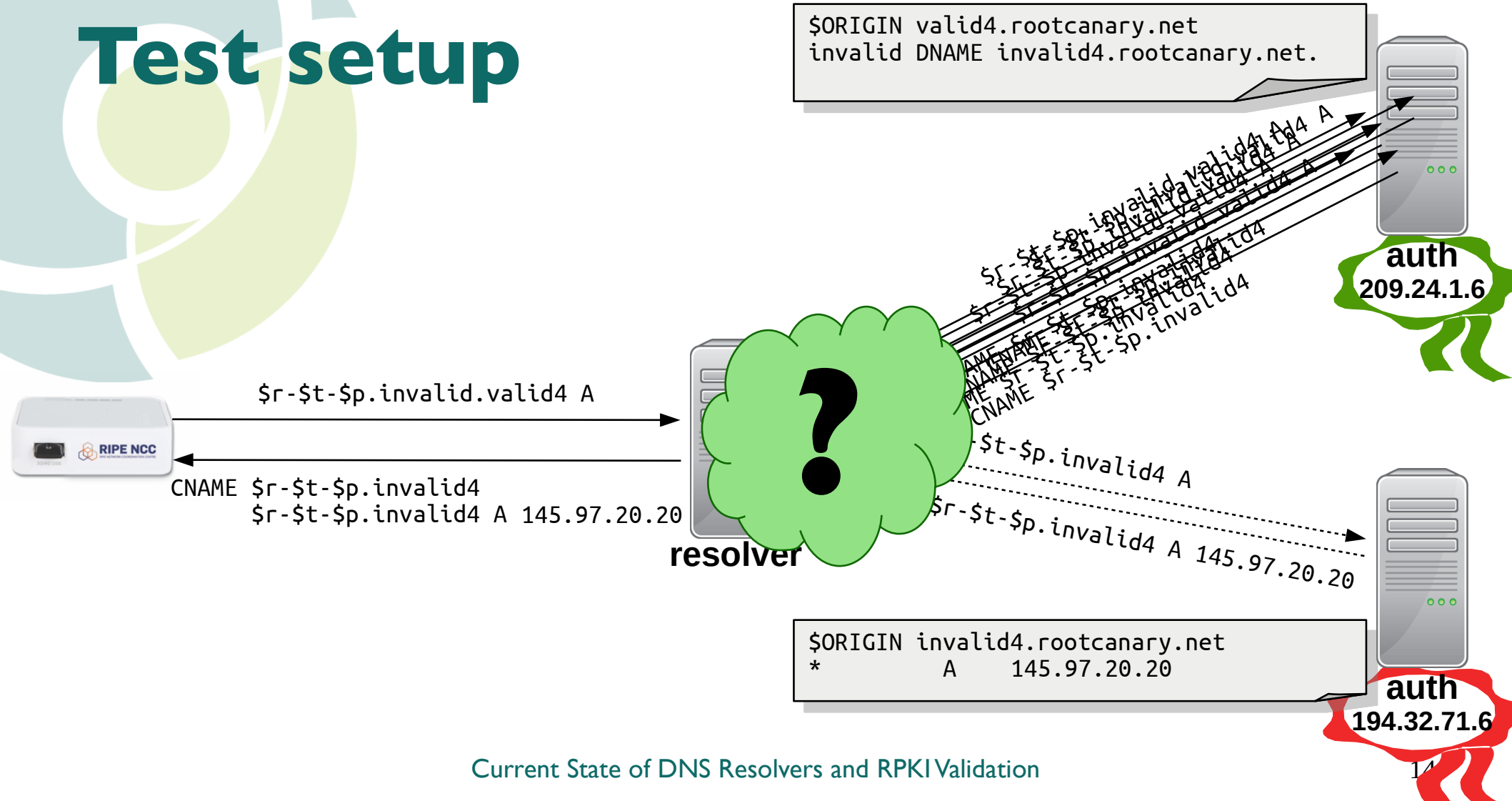



You are here: Home > Analyse > Internet Measurements > RIPE Atlas > Measurements > Measurement #23865475
Settings & Status
Latest Results
Map
Latencymon
Downloads
Overview
recurring IPv4 DNS "RPKI Resolver msm IPv4" id 23865475
Target
No Target (Uses Resolvers configured on Probe)
DNS Specific Settings
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


$ORIGIN valid4.rootcanary.net
invalid DNAME invalid4.rootcanary.net.
$r-$t-$p.invalid.valid4 A
CNAME $r-$t-$p.invalid4
auth
209.24.1.6
$r-$t-$p.invalid.valid4 A
CNAME $r-$t-$p.invalid4
RIPE NCC
resolver
$r-$t-$p.invalid4 A
$r-$t-$p.invalid4 A 145.97.20.20
$ORIGIN invalid4.rootcanary.net
* A 145.97.20.20
auth
194.32.71.6

Test setup

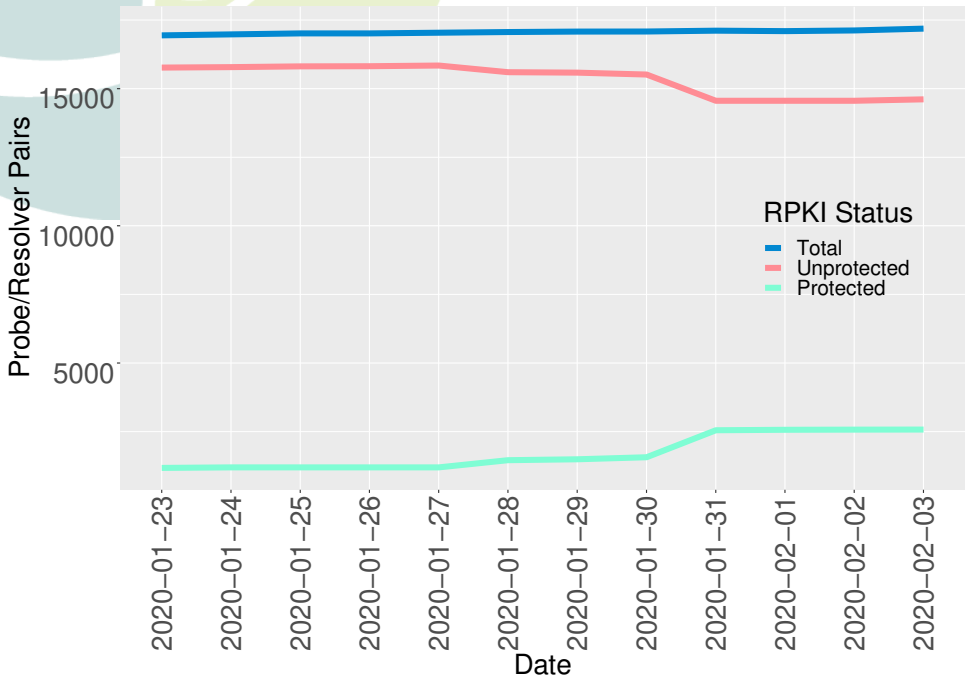

$ORIGIN valid4.rootcanary.net
invalid DNAME invalid4.rootcanary.net.
auth
209.24.1.6
$r-$t-$p.invalid.valid4 A
CNAME $r-$t-$p.invalid4
$r-$t-$p.invalid4 A 145.97.20.20
resolver
?
$r-$t-$p.invalid4 A
$r-$t-$p.invalid4 A 145.97.20.20
$ORIGIN invalid4.rootcanary.net
* A 145.97.20.20
auth
194.32.71.6

Test setup

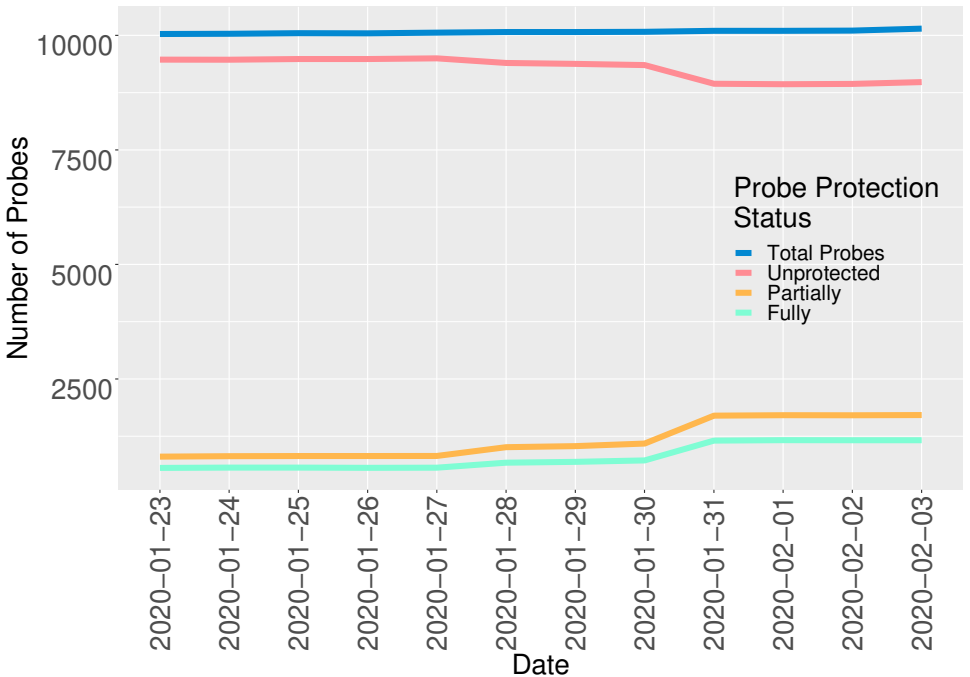
- Atlas measurement
  kindly provided by Emile Aben
- Beacon for the authoritatives
  kindly provided by Job Snijders

Results

Probe/resolver pair

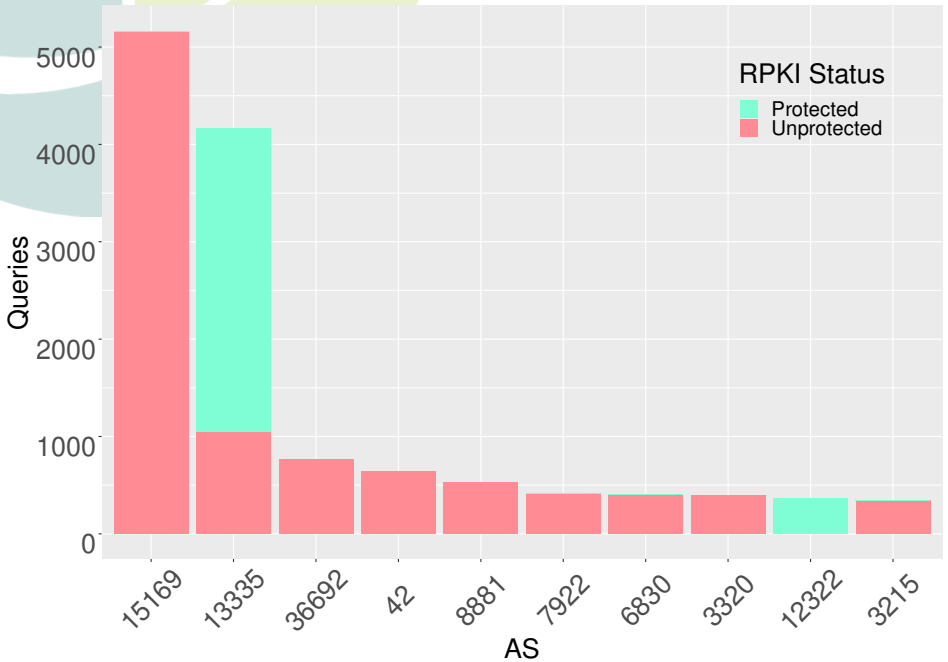


Probe time series

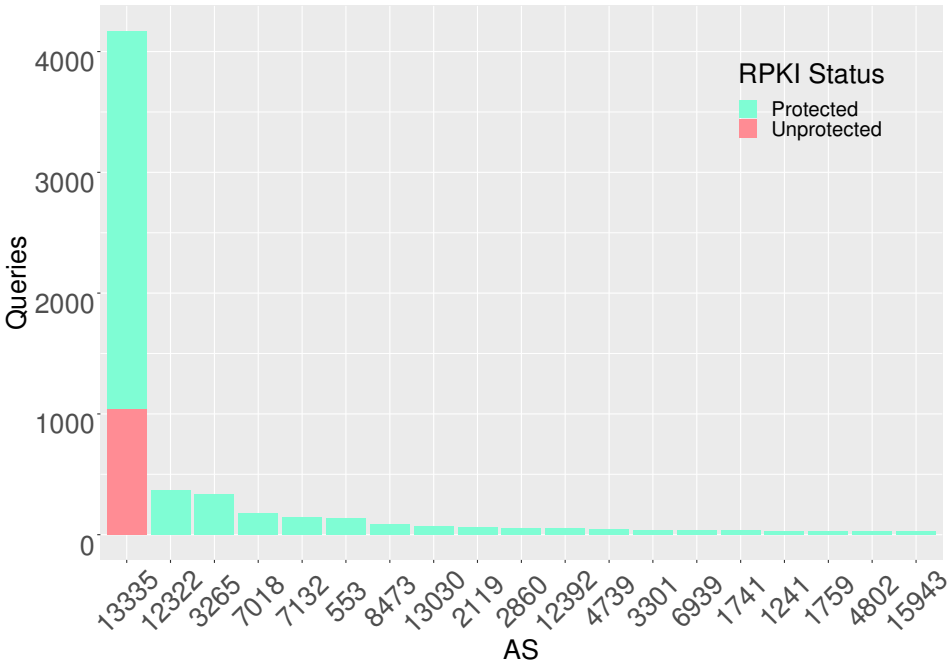


Results

Top ten most popular ASes



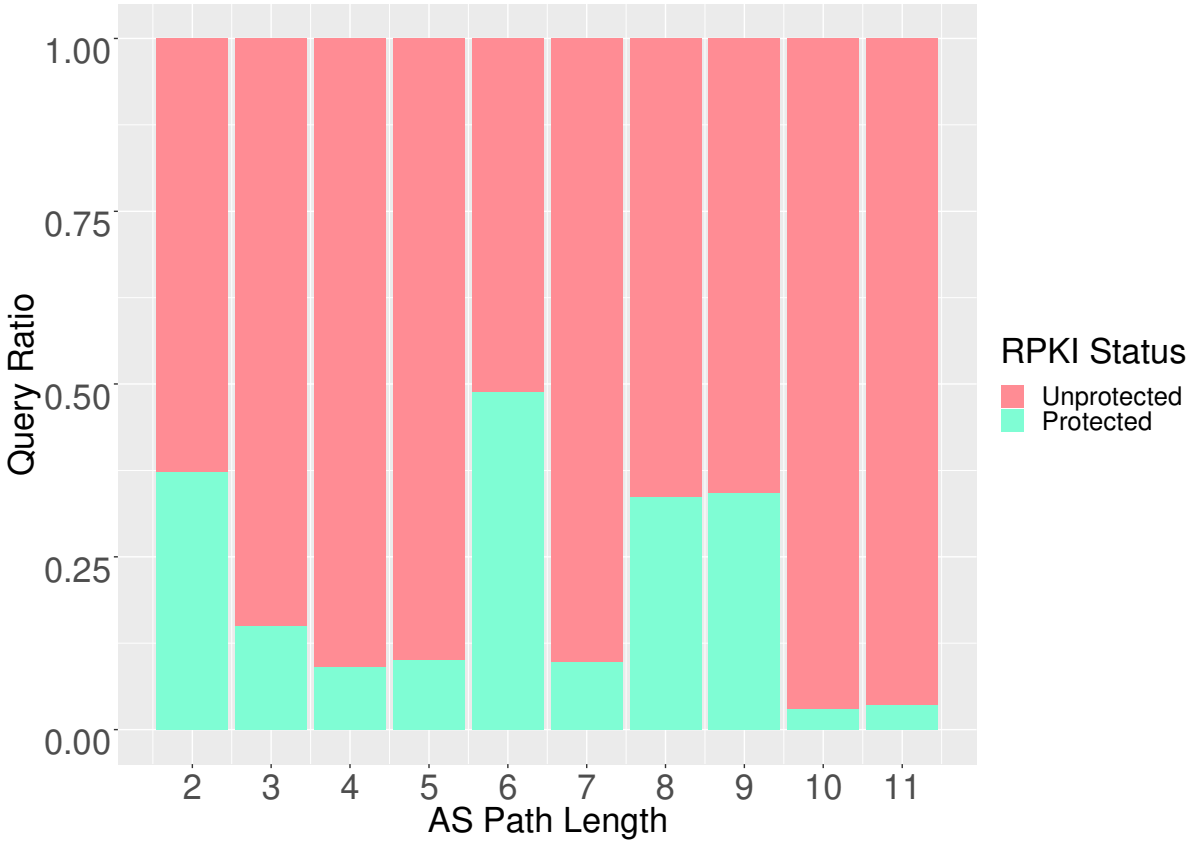
Top ten most protected ASes



Results

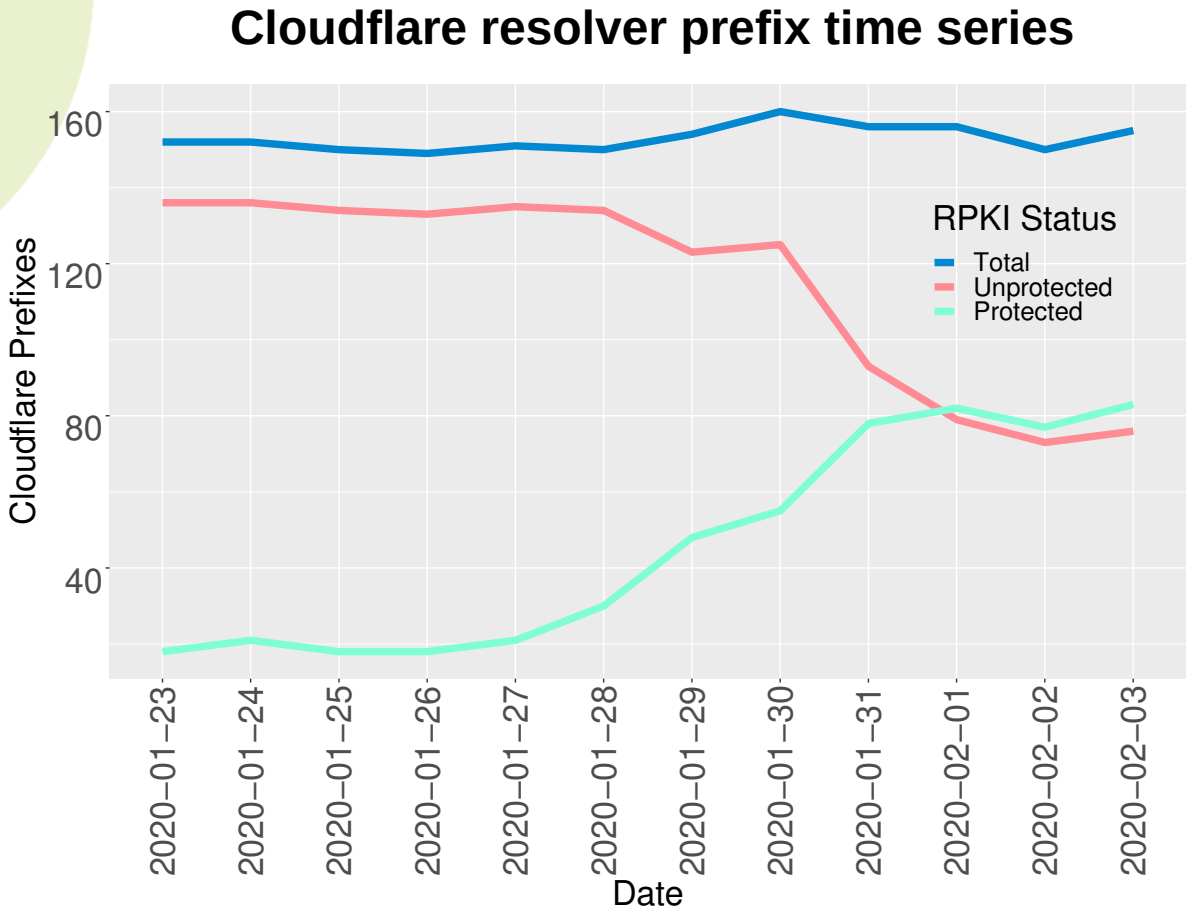
Sub RQ: Does the length of the AS path matter?

Relationship RPKI protection and AS path length



Results

Sub RQ: How does anycast influence protection?

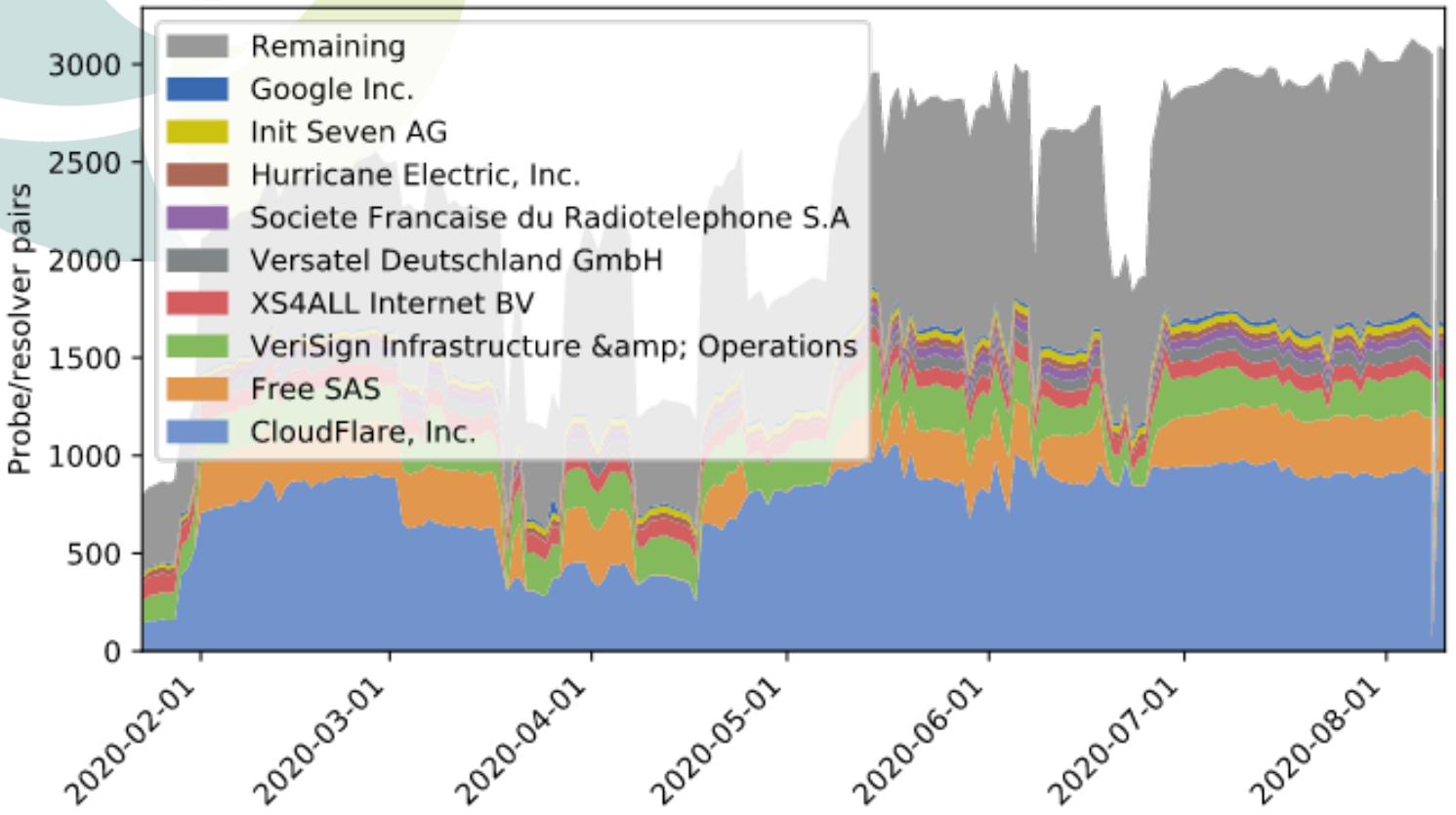


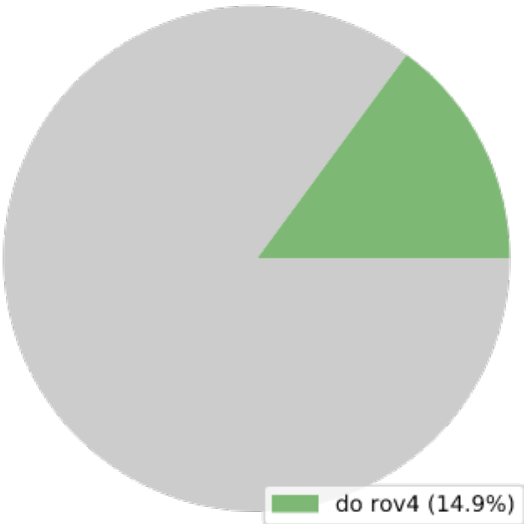
Current situation / IPv6

DNSThought

DNSThought

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





Test setup

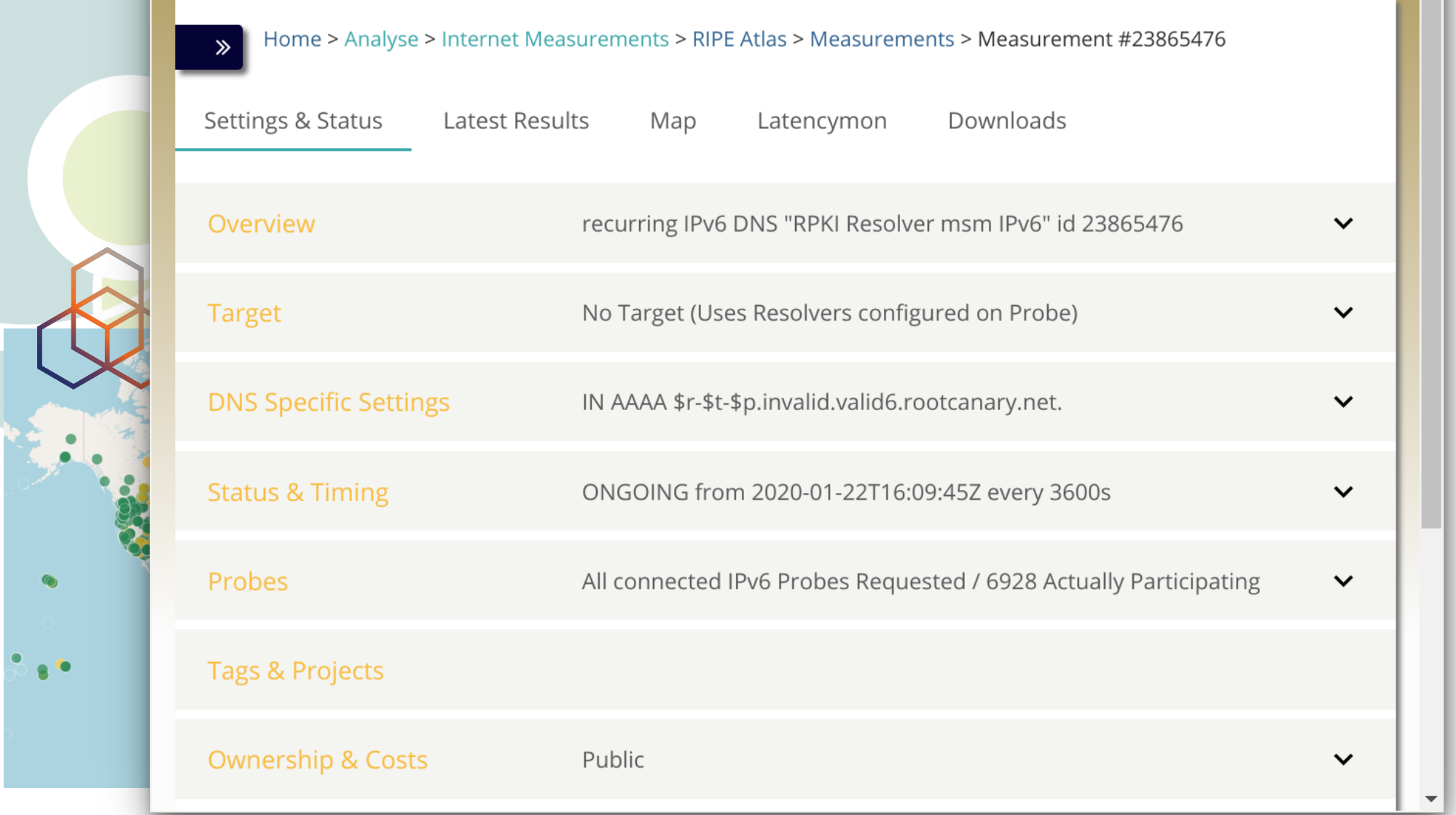
```
$ORIGIN rootcanary.net
$TTL 60
@     SOA  ns1.surfnet.nl. (
           dns-beheer.surfnet.nl.
           2020080503 ; serial
           10800      ; refresh
           3600       ; retry
           604800     ; expire
           86400      ; minimum
           )
      NS   ns1.surfnet.nl.
      NS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

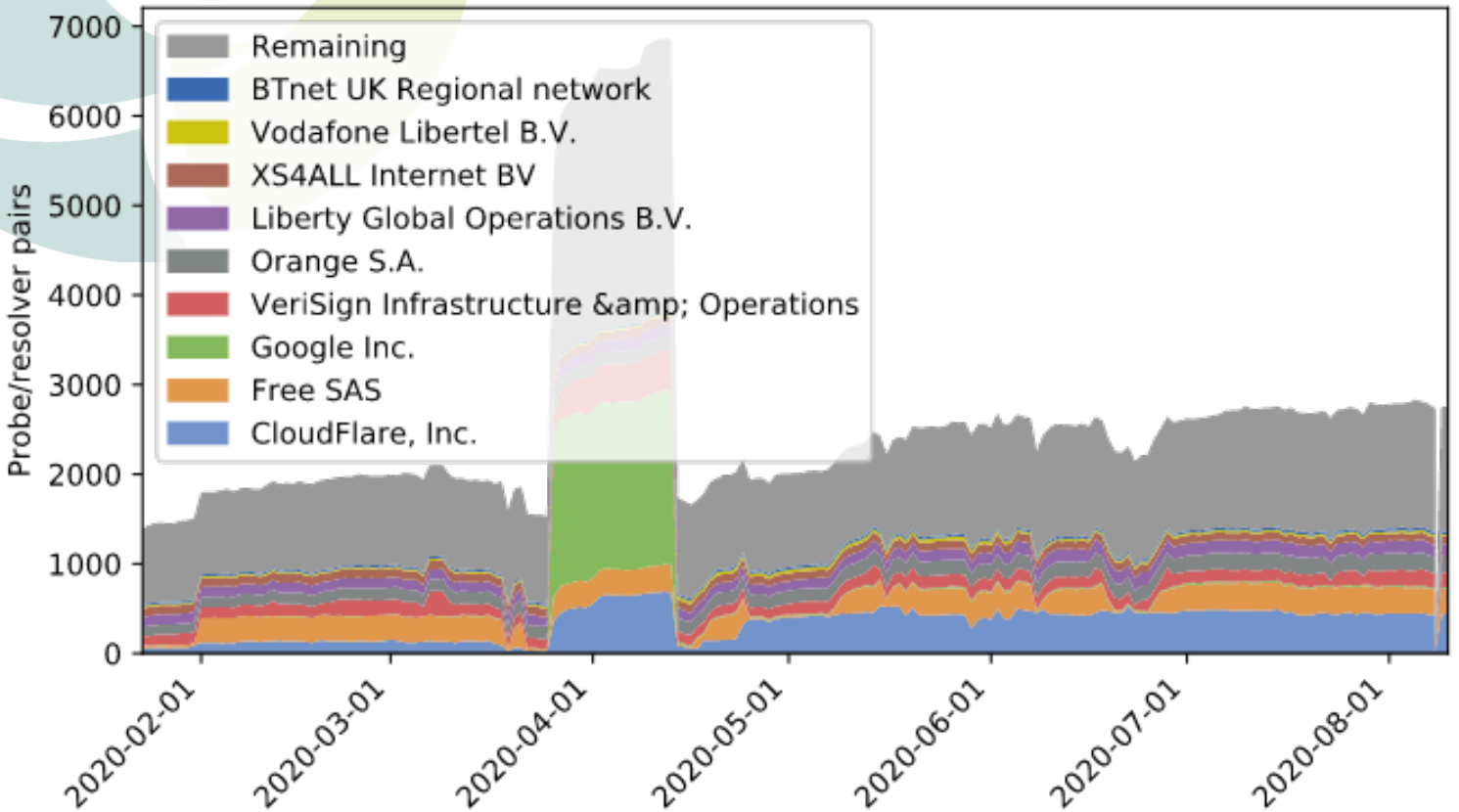
prefix	2001:728:1808::/48
ax len	64
ASN	15562

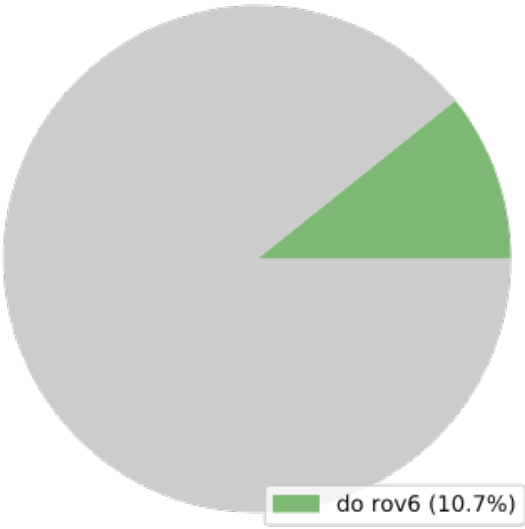
prefix	2001:7fb:fd04::/48
ax len	48
ASN	196615


Home > Analyse > Internet Measurements > RIPE Atlas > Measurements > Measurement #23865476
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

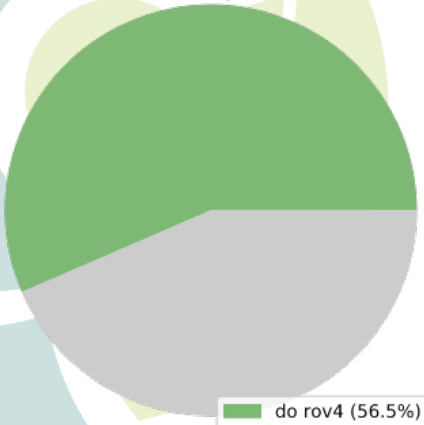
https://dnsthought.nlnetlabs.nl/does_rov6/#top_auth_asns



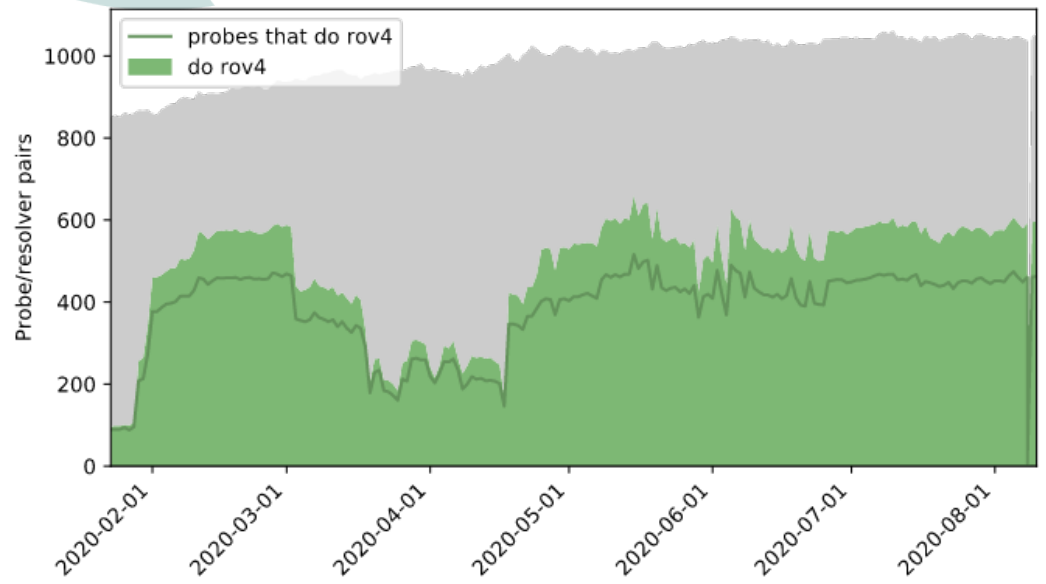


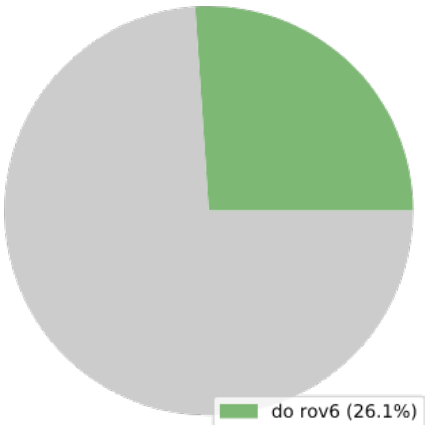
DNSThought

AS13335 Cloudflare

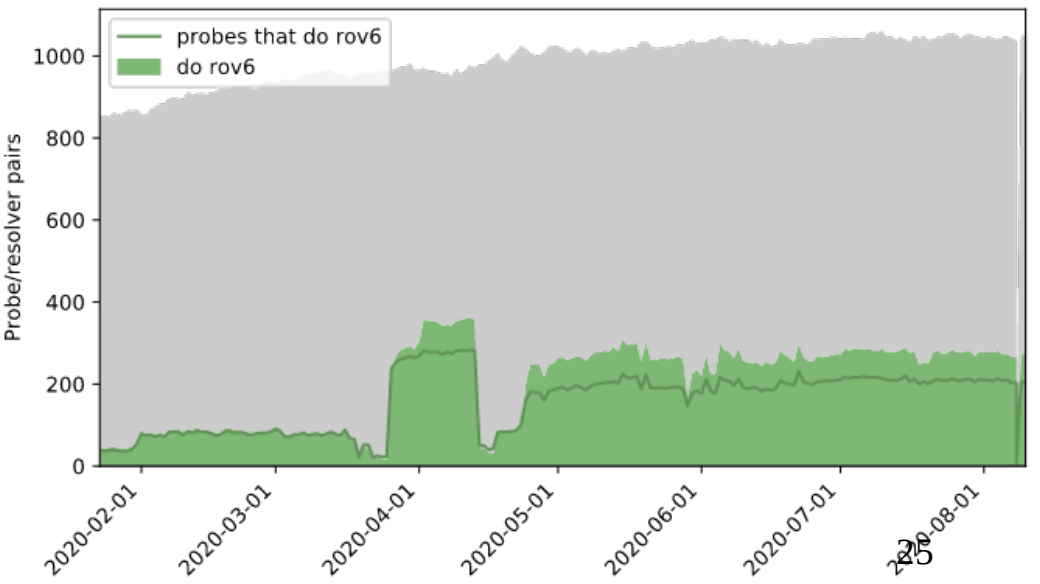


IPv4



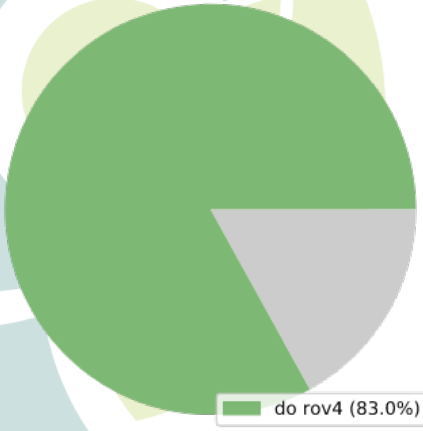


IPv6

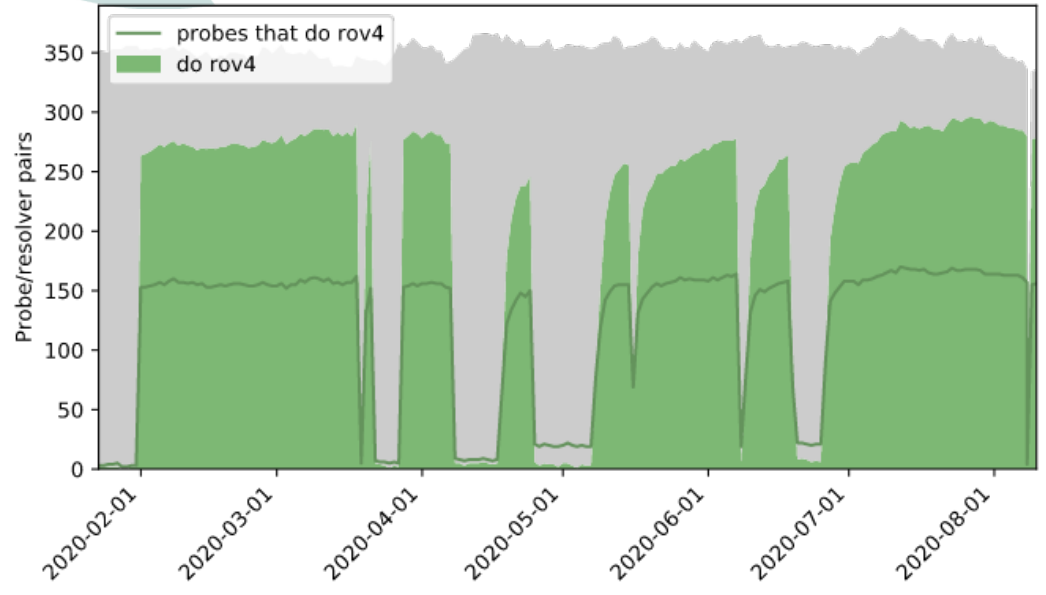


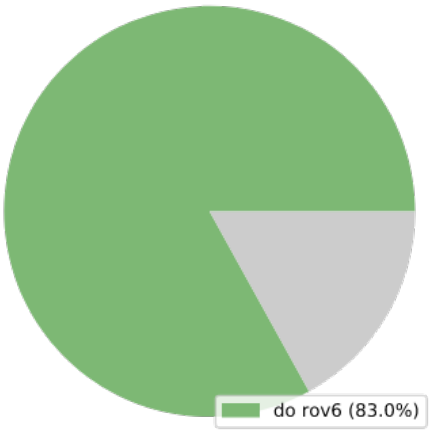
DNSThought

AS12322 Free SAS

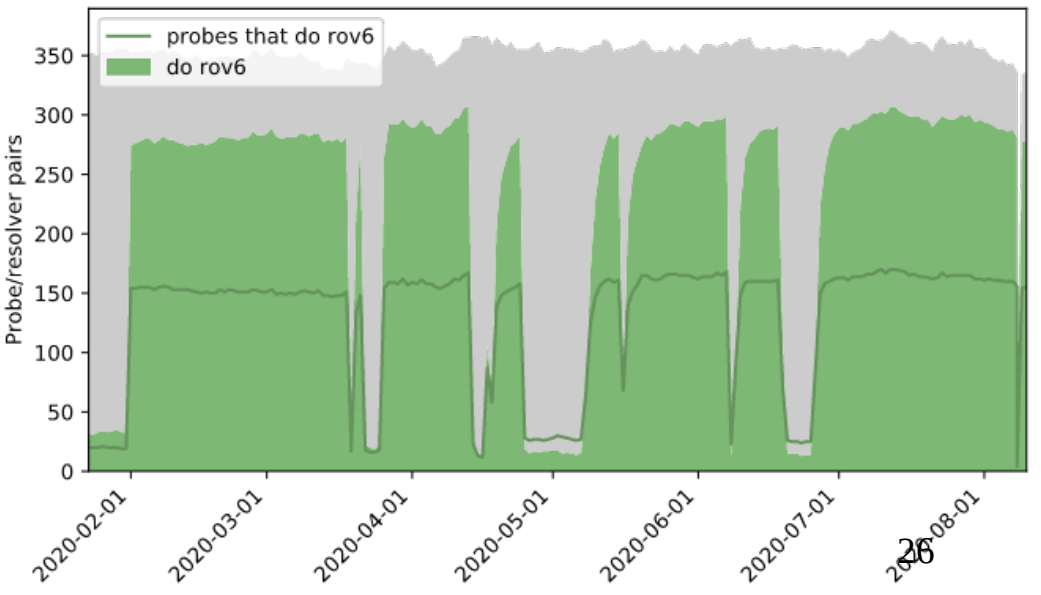


IPv4





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/