RootViz: visualizing real-time monitoring of the Root DNS Servers

Giovane C. M. Moura
SIDN Labs and TU Delft

RIPE 93
Sofia, Bulgaria
2026-10-27





Outline

Introduction

RootViz Pipeline

Root Server Operators Main Goal

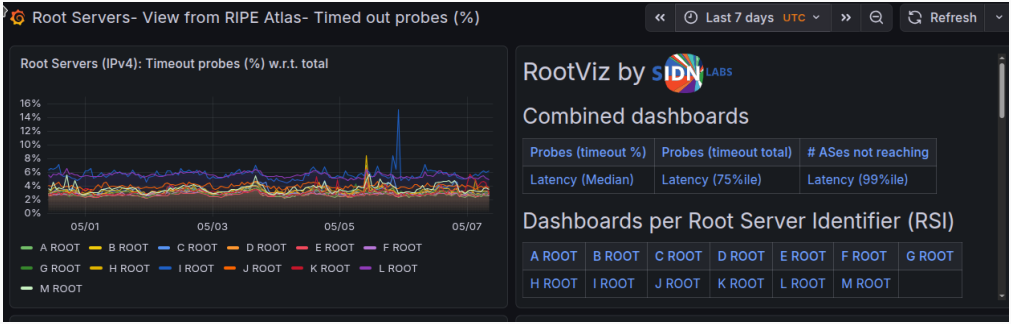
Dashboards

Findings

Case study: L-ROOT Jan 2026 event

RootViz dashboard

https://rootviz.sidnlabs.nl



The Root Server System

13 Root Server Identifier (RSIs)

`[a-m].root-servers.net`

- **12 independent operators**

  (Verisign runs both A and J)
- Self-funded, voluntary
- Each operator: **full autonomy**
  - on how they run their service
- Web: https://root-servers.org

RSI	Operator	Country
A	Verisign	
B	USC-ISI	
C	Cogent	
D	U. Maryland	
E	NASA OCIO	
F	ISC	
G	US DoD (DISA)	
H	US Army (ARL)	
I	Netnod	
J	Verisign	
K	RIPE NCC	
L	ICANN	
M	WIDE Project	

Why monitor the Root?

The **Root DNS** and TLDs are the foundation of the DNS.

- Every uncached lookup eventually depends on them
- If the Root breaks ⇒ **the entire DNS suffers**, globally

You can't measure global reachability from *inside* the system.

You need external vantage points.



External VPs probing Root servers (RIPE Atlas Probes)

https://atlas.ripe.net

What are RIPE Atlas probes?

The largest active Internet measurement network.

Probes are diverse: hardware, VMs, rack servers

- Run by **RIPE NCC** since 2010
- **∼14K probes** in 180 countries
- Continuously measure DNS, ping, traceroute
- Data is **public & free**



A RIPE Atlas (v3) hardware probe

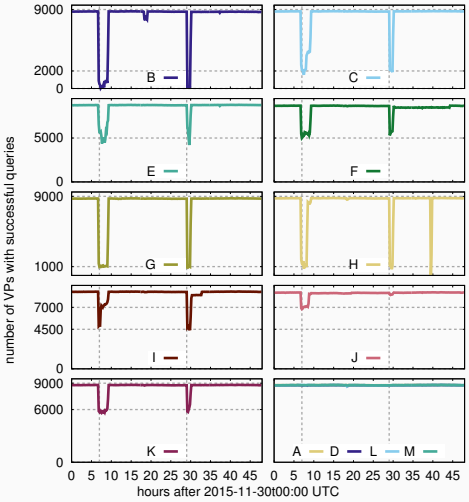
Context

Ten years ago, we published on IMC2016:

> **Anycast vs. DDoS: Evaluating the November 2015 Root DNS Event**
>
> https://dl.acm.org/doi/10.1145/2987443.2987446

RootViz uses the same data sources — now visualized in real time.

- RIPE Atlas probes (All of them)

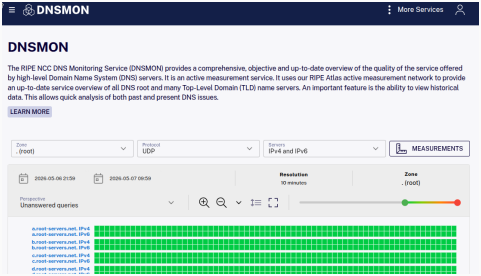


Motivation

The data is already there — but it's sort of *dark data*.

- RIPE Atlas continuously measures Root servers from **all Atlas probes** (∼14K worldwide)
- Most operators only look at **DNSMON**
- But DNSMON uses only **anchors**

Why not use *all* of them? and have more metrics? and Grafana?



DNSMON — anchors only

https://dnsmon.ripe.net/

Anchors vs. probes: trade-offs

Anchors

datacenters · controlled

✓ Pros

- Datacenter-grade, clean networks
- Highly reliable individually

× Cons

- Few (∼1K), concentrated
- Miss the “messy” real Internet

Rest of probes

homes, offices · messy reality

✓ Pros

- Many (∼13K), wide coverage
- See the *real* user experience

× Cons

- Local quirks, DNS hijacking[1]
- Islands/peninsulas[2]
- Single probe = unreliable

[1] Intercept and Inject (Nosyk et al. (2023)
[2] Saluja et al.(2022)

Anchors vs. all probes: how much do we gain?

	Anchors (DNSMON)	All probes (RootViz)	Gain
Vantage points	999	14,528	**14.5×**
ASNs (IPv4)	743	4,505	**6.1×**
ASNs (IPv6)	681	2,304	**3.4×**
Prefixes (IPv4)	964	9,911	**10.3×**
Prefixes (IPv6)	858	3,496	**4.1×**
Countries	109	180	**1.7×**

Source: RIPE Atlas probe file, 2026-05-06

Anchors vs. all probes: how much do we gain?

	Anchors (DNSMON)	All probes (RootViz)	Gain
Vantage points	999	14,528	**14.5×**
ASNs (IPv4)	743	4,505	**6.1×**
ASNs (IPv6)	681	2,304	**3.4×**
Prefixes (IPv4)	964	9,911	**10.3×**
Prefixes (IPv6)	858	3,496	**4.1×**
Countries	109	180	**1.7×**

Source: RIPE Atlas probe file, 2026-05-06

Using all probes: *a wider view of reachability.*

Our approach: crowdsourcing reachability

Same idea as those airport restroom **HappyOrNot** terminals[1]:

- One press is noise

If many probes agree something's wrong — something *is* wrong.



HappyOrNot dashboard

[1] D. Owen, "The Happiness Button," *The New Yorker*, Feb. 8, 2018

RootViz: goals

Light up dark data

Atlas measures all RSIs from ∼14 K probes — most results are never seen.

Real-time monitoring

30-min aggregates, live Grafana dashboard.

Crowdsourced reachability

All probes, not just anchors — **14.5**× more vantage points.

Not a blame tool. Failures can be at the probe, in-network, or at the server location — not necessarily **the root server operator**.

Outline

Introduction

RootViz Pipeline

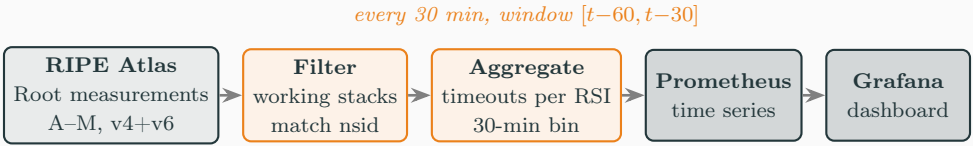
Root Server Operators Main Goal

Dashboards

Findings

Case study: L-ROOT Jan 2026 event

RootViz pipeline



Input

- `chaos TXT hostname.bind`
- Sent direct to each RSI (no resolver)
- All probes, IPv4 & IPv6

Reduction

- Keep probes with working stack `system-ipv{4,6}-works`
- Drop responses with mismatched `nsid`
  - queries being intercepted
- Count unique `prb_id` timeouts within 30min

Outline

Introduction

RootViz Pipeline

Root Server Operators Main Goal

Dashboards

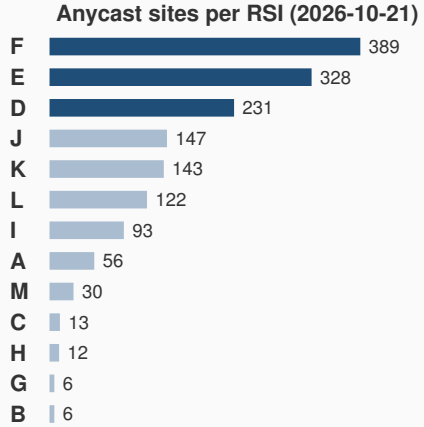
Findings

Case study: L-ROOT Jan 2026 event

Root Operators: Main Goals

1. **Reachability first**
   - A resolver only needs to reach *one* of the 13 RSIs
   - Each RSI is heavily replicated: 6 to 389 anycast sites, 1,576 in total
2. **Latency second**
   - Root data is cached for 2 days (TTL)

RootViz dashboard follows the same order: reachability first, then latency.

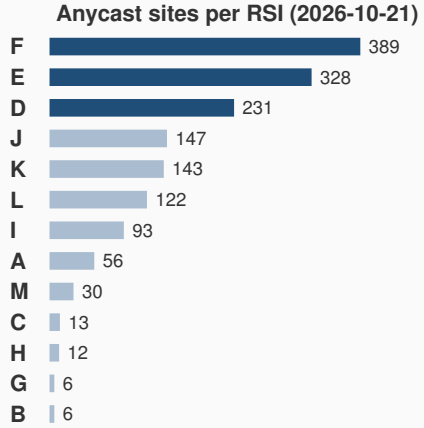


Source: https://root-servers.org

Root Operators: Main Goals

1. **Reachability first**
   - A resolver only needs to reach *one* of the 13 RSIs
   - Each RSI is heavily replicated: 6 to 389 anycast sites, 1,576 in total
2. **Latency second**
   - Root data is cached for 2 days (TTL)

RootViz dashboard follows the same order: reachability first, then latency.



Source: https://root-servers.org

Identifying the Root Cause of Timeouts

Goal: detect spikes in timeouts and determine *what* happened and *where*.

A timeout can originate in three places, and it is hard to tell which:

Identifying the Root Cause of Timeouts

Goal: detect spikes in timeouts and determine *what* happened and *where*.

A timeout can originate in three places, and it is hard to tell which:

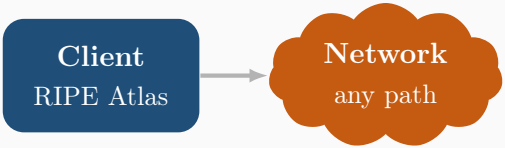
Client
RIPE Atlas

fails for **all** RSIs
at once

Identifying the Root Cause of Timeouts

Goal: detect spikes in timeouts and determine *what* happened and *where*.

A timeout can originate in three places, and it is hard to tell which:

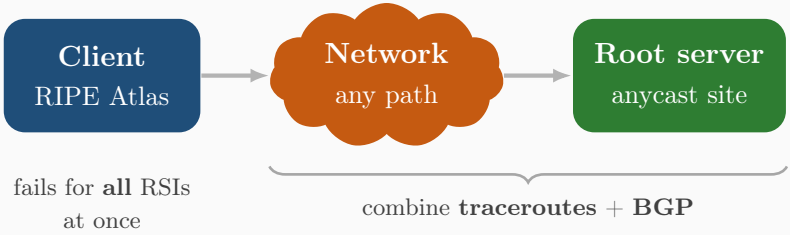


fails for **all** RSIs
at once

Identifying the Root Cause of Timeouts

Goal: detect spikes in timeouts and determine *what* happened and *where*.

A timeout can originate in three places, and it is hard to tell which:



Outline

Introduction

RootViz Pipeline

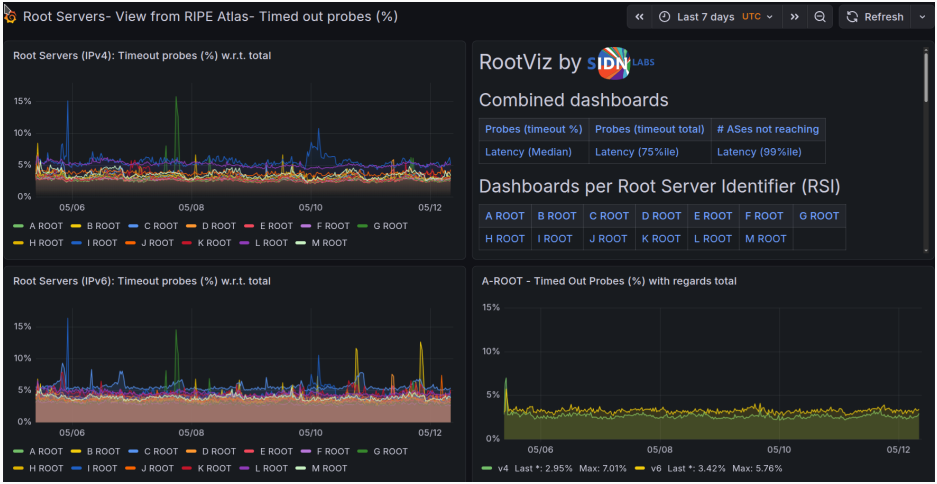
Root Server Operators Main Goal

Dashboards

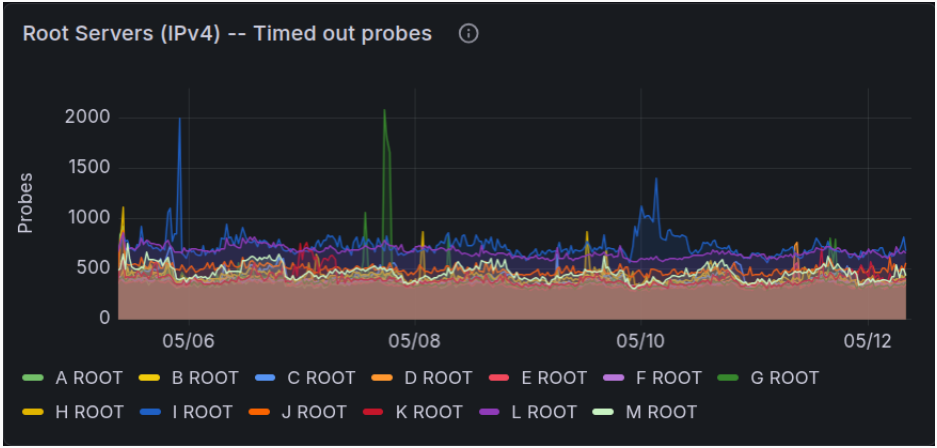
Findings

Case study: L-ROOT Jan 2026 event

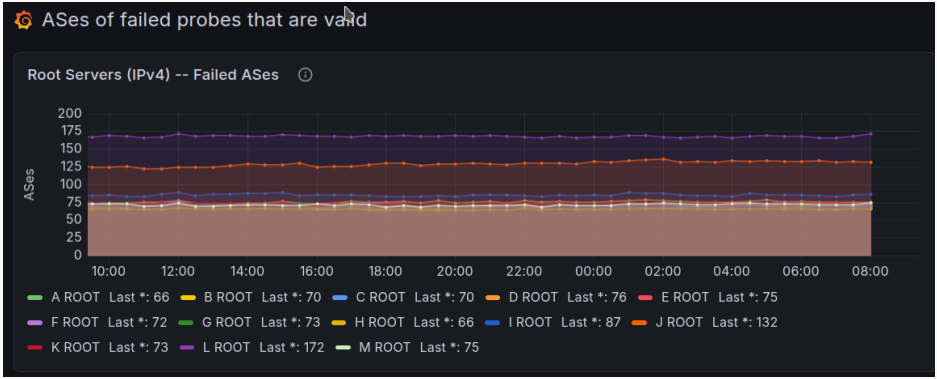
Dashboards


Root Servers- View from RIPE Atlas- Timed out probes (%)
Last 7 days UTC
Refresh
Root Servers (IPv4): Timeout probes (%) w.r.t. total
15%
10%
5%
0%
05/06
05/08
05/10
05/12
A ROOT B ROOT C ROOT D ROOT E ROOT F ROOT G ROOT
H ROOT I ROOT J ROOT K ROOT L ROOT M ROOT
RootViz by SIDN LABS
Combined dashboards
Probes (timeout %)
Probes (timeout total)
ASes not reaching
Latency (Median)
Latency (75%ile)
Latency (99%ile)
Dashboards per Root Server Identifier (RSI)
A ROOT B ROOT C ROOT D ROOT E ROOT F ROOT G ROOT
H ROOT I ROOT J ROOT K ROOT L ROOT M ROOT
Root Servers (IPv6): Timeout probes (%) w.r.t. total
15%
10%
5%
0%
05/06
05/08
05/10
05/12
A ROOT B ROOT C ROOT D ROOT E ROOT F ROOT G ROOT
H ROOT I ROOT J ROOT K ROOT L ROOT M ROOT
A-ROOT - Timed Out Probes (%) with regards total
15%
10%
5%
0%
05/06
05/08
05/10
05/12
v4 Last *: 2.95% Max: 7.01%
v6 Last *: 3.42% Max: 5.76%

Timeout probes dashboard



ASes of timedout probes



No root cause, only smoke detector...

RootViz — what we learned by looking

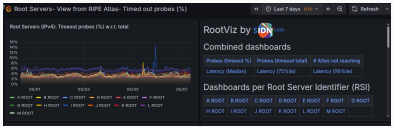
The data was always there.

RootViz raises many questions:

- RSIs have **different baseline timeout levels** — why?

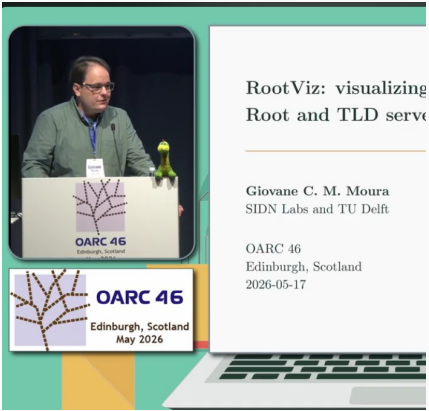
Every answer raises more questions.

https://rootviz.sidnlabs.nl



RootViz at OARC 46

- We presented **RootViz** at OARC 46 (May 2026)
- Various Root OPS asked questions during and after the talk.
- Since then:
  - Two groups of students looking into it (Software project and Research Project from TU Delft)
  - Master student wills start looking into this data too



Slides – Youtube video

Outline

Introduction

RootViz Pipeline

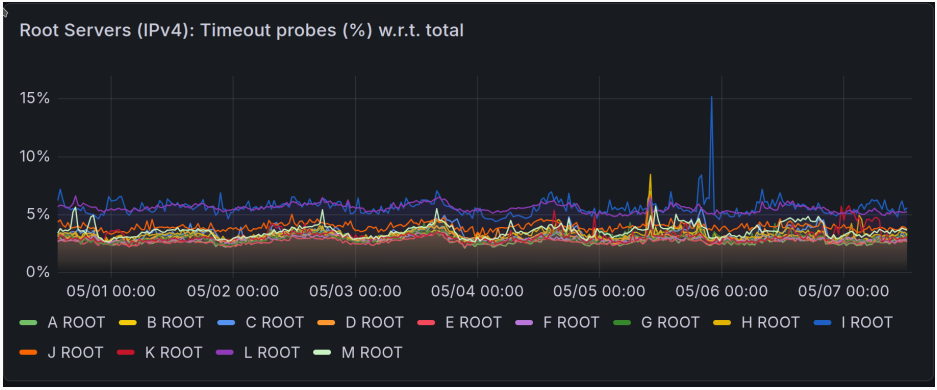
Root Server Operators Main Goal

Dashboards

Findings

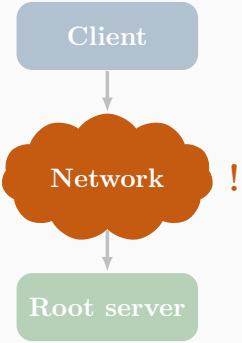
Case study: L-ROOT Jan 2026 event

Finding 1: baseline timeouts differ per RSI



Each RSI has its **own steady-state** timeout level — not zero, and not equal.

Finding 2: often in-network problems



We saw **several temporary timeout events** (B-Root, K-Root, others) and **contacted the operators**.

Their typical reply:

> *"We saw it, but it was **upstream**, outside our control."*

⇒ **In-network issues**

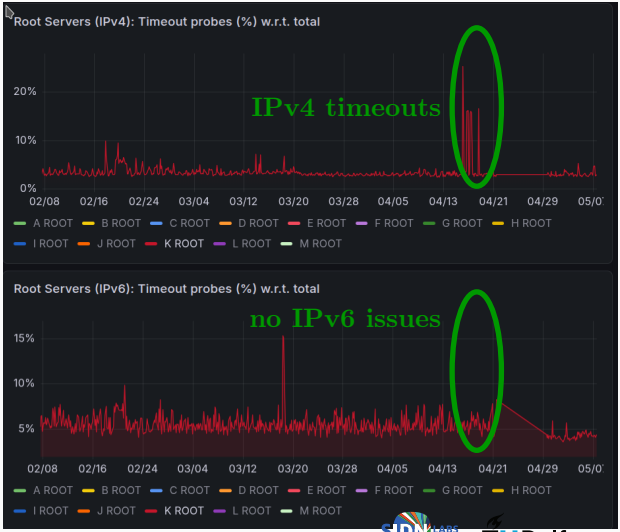
Finding 2: example K-Root

K-Root, April 26

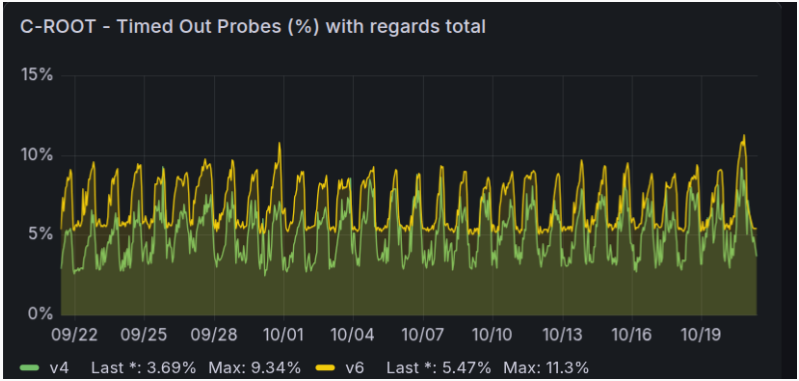
IPv4 only — IPv6 unaffected

We reached out to the **K-Root operators**.

Issue with a **transit provider** connecting some Atlas probes to K-Root.



Finding 3: C-Root periodic behavior



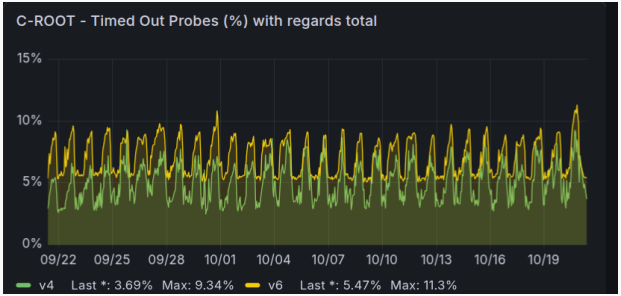
Finding 3: C-Root periodic behavior

What we see

- Timeouts to C-Root follow a **periodic pattern**
- **Only C-Root** shows it; the other 12 RSIs do not

Why?

Any guesses?



Finding 3: C-Root periodic behavior

- Jesse Prins did a deep dive on C-ROOT for bachelor thesis (TU Delft)
- Report: PDF
- Check for all details: Fourier analysis, traceroutes, month-long datasets, etc.
- I'll simplify for this presentation

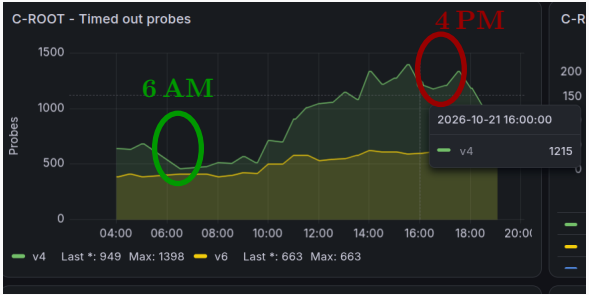
Which Probes Are Affected?

We compare **10 minutes** of data from two windows:

- 06:00 UTC
- 16:00 UTC

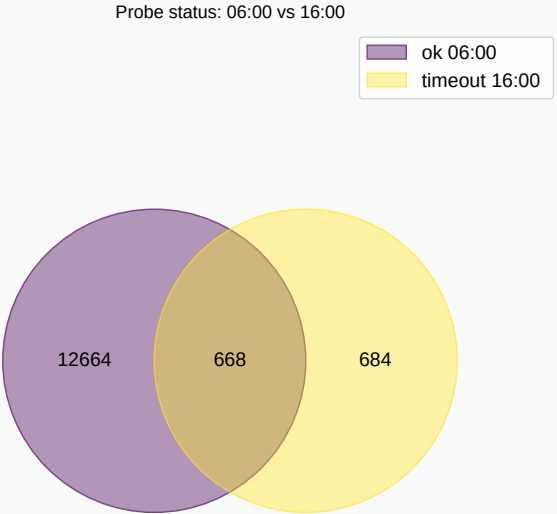
Which probes are **fine in the morning** but **time out in the afternoon**?

A sample only; Jesse's full analysis shows the same patterns.



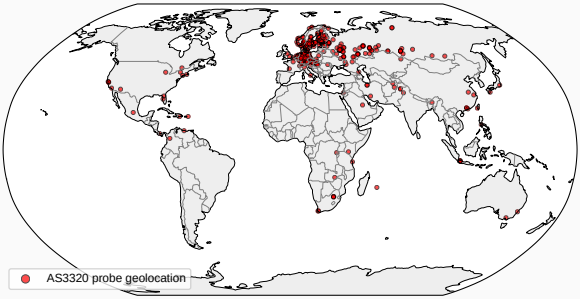
Oct 21, 2026: 1,215 IPv4 probes time out around 16:00 UTC

Finding 3: Periodic Behavior at C-Root



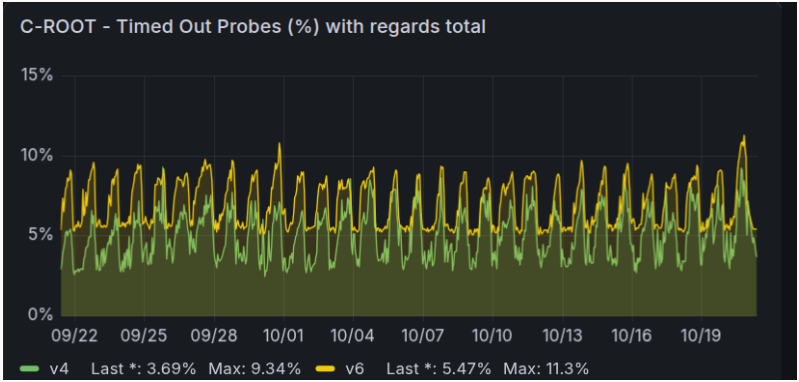
Finding 3: Where Are the Affected Probes?

- **96** of the 684 probes are in **AS3320**
  (Deutsche Telekom, Tier 1)
- **20** more are in **AS2119**, which uses AS3320 as upstream
- Others may as well use AS3320 (see Jesse's report)



AS3320 ATLAS probes geolocation that timeout at 16:00 but not at 06:00

Why AS3320 are timing out in diurnal pattern?



The Main Suspect: The Management Layer



cogent

FOR IMMEDIATE RELEASE

Cogent Contacts:

For Public Relations:
Eric Schweizer
+ 1 (202) 295-4313
eschweizer@cogentco.com

For Investor Relations:
+ 1 (202) 295-4212
investor.relations@cogentco.com

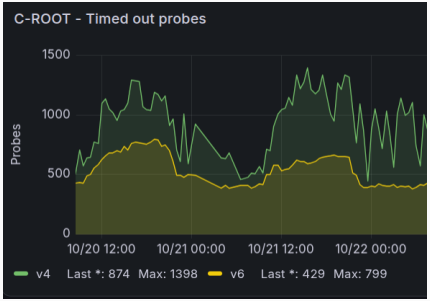
Cogent Communications Sues

Deutsche Telekom for Congesting Internet Connections

https://www.cogentco.com/en/news/press-releases/967-cogent-communications-sues-deutsche-telekom-for-congesting-internet-connections

The Main Suspect: The Management Layer

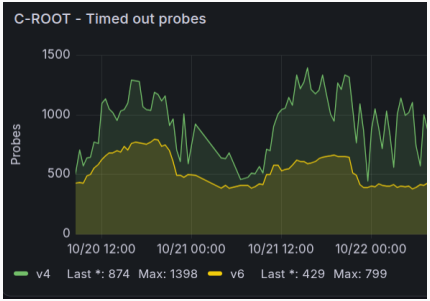
- C-Root is operated by **Cogent**
- DTAG and Cogent have a long-running **peering dispute** over payment
  - Meta also stopped peering with DTAG
- Observed pattern: once traffic reaches peak hours (diurnal), it is **dropped**
- DNS traffic is very small; may be collateral damage
- We contacted DTAG; they are **investigating**



We take no side in the dispute; we only report what we measure.

The Main Suspect: The Management Layer

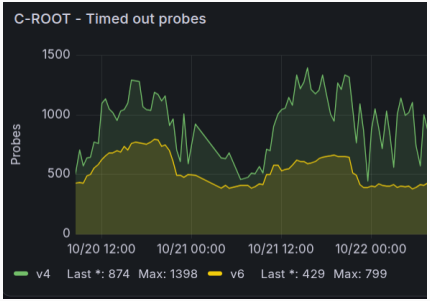
- C-Root is operated by **Cogent**
- DTAG and Cogent have a long-running **peering dispute** over payment
  - Meta also stopped peering with DTAG
- Observed pattern: once traffic reaches peak hours (diurnal), it is **dropped**
- DNS traffic is very small; may be collateral damage
- We contacted DTAG; they are **investigating**



We take no side in the dispute; we only report what we measure.

The Main Suspect: The Management Layer

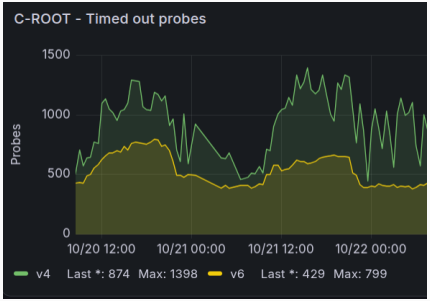
- C-Root is operated by **Cogent**
- DTAG and Cogent have a long-running **peering dispute** over payment
  - Meta also stopped peering with DTAG
- Observed pattern: once traffic reaches peak hours (diurnal), it is **dropped**
- DNS traffic is very small; may be collateral damage
- We contacted DTAG; they are **investigating**



We take no side in the dispute; we only report what we measure.

The Main Suspect: The Management Layer

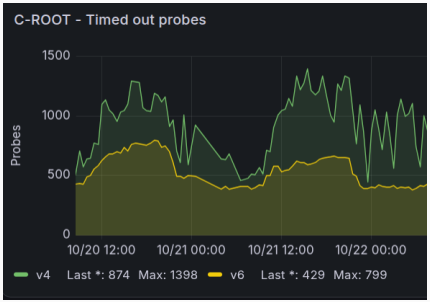
- C-Root is operated by **Cogent**
- DTAG and Cogent have a long-running **peering dispute** over payment
  - Meta also stopped peering with DTAG
- Observed pattern: once traffic reaches peak hours (diurnal), it is **dropped**
- DNS traffic is very small; may be collateral damage
- We contacted DTAG; they are **investigating**



We take no side in the dispute; we only report what we measure.

The Main Suspect: The Management Layer

- C-Root is operated by **Cogent**
- DTAG and Cogent have a long-running **peering dispute** over payment
  - Meta also stopped peering with DTAG
- Observed pattern: once traffic reaches peak hours (diurnal), it is **dropped**
- DNS traffic is very small; may be collateral damage
- We contacted DTAG; they are **investigating**



We take no side in the dispute; we only report what we measure.

Outline

Introduction

RootViz Pipeline

Root Server Operators Main Goal

Dashboards

Findings

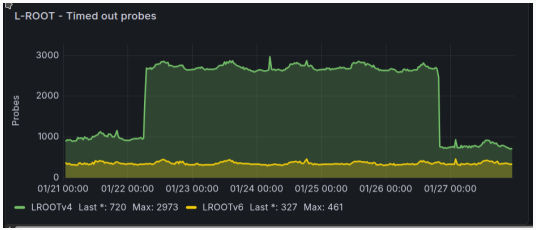
Case study: L-ROOT Jan 2026 event

Deep Dive

RootViz **flags** when something is off — but **not why**.
Once an event is detected, you can drill down:

- Which **probes** timed out?
- Which **anycast site** were they catching before?
- Which **ASNs** / **countries** are affected?

RootViz is the **smoke detector** — the investigation comes next.



LROOT Jan 2026 event

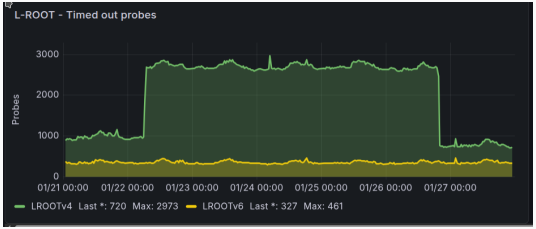
Case study: L-Root, January 2026

2026-01-22, ∼06:00 UTC

lasted until 01-26 20:00 UTC

- **∼2,000 Atlas probes** suddenly time out
- Reaching **L-Root over IPv4**
- IPv6 **unaffected**
- Other RSIs **unaffected**

Sharp spike, then back — not noise.

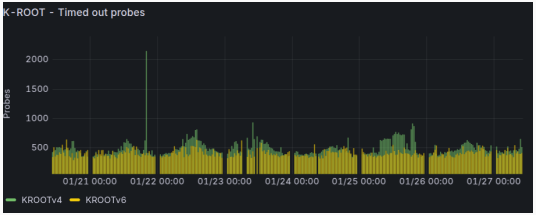


L-Root, IPv4 timeouts, Jan 21–27

“But probes are noisy — nothing to see here”

If it were just probe noise, *all* RSIs would spike together.
They didn’t.

- Same probes, same time window
- K-Root: **stable**
- Other RSIs: **stable**
- Probes weren’t offline — **timeouts only**
- IPv6 worked fine

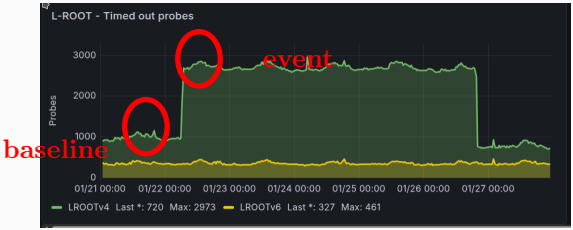


K-Root, same time window — flat

Drill down: who are the timing-out probes?

Compare two 10-min windows of the same measurement (https://atlas.ripe.net/measurements/10308):

- **Baseline**: Jan 22nd, 2026: 04:00–04:10 UTC (10min)
- **Event**: Jan 22nd, 2026: 13:00–13:10 UTC (10min)

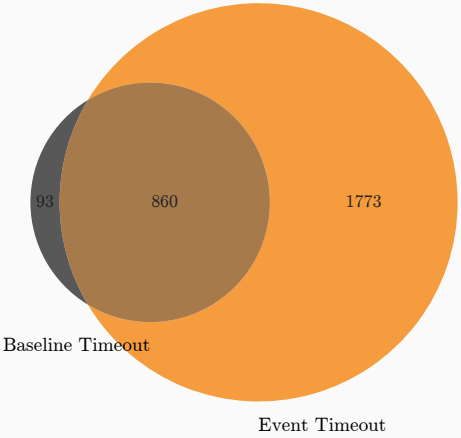


L-Root, IPv4 timeouts, Jan 21–27

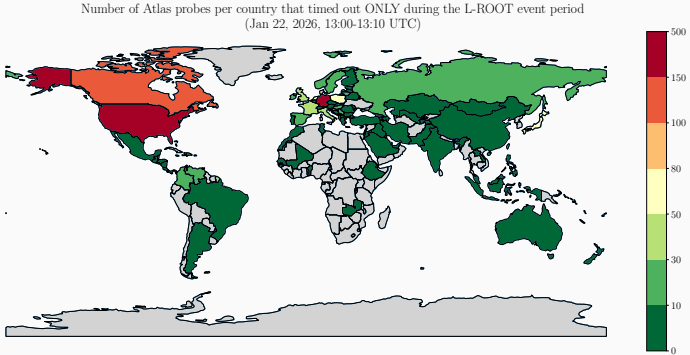
Drill down: event window

Same measurement, 9 hours later:

- 1,773 probes timed out only during the event



Where are these probes? (countries)



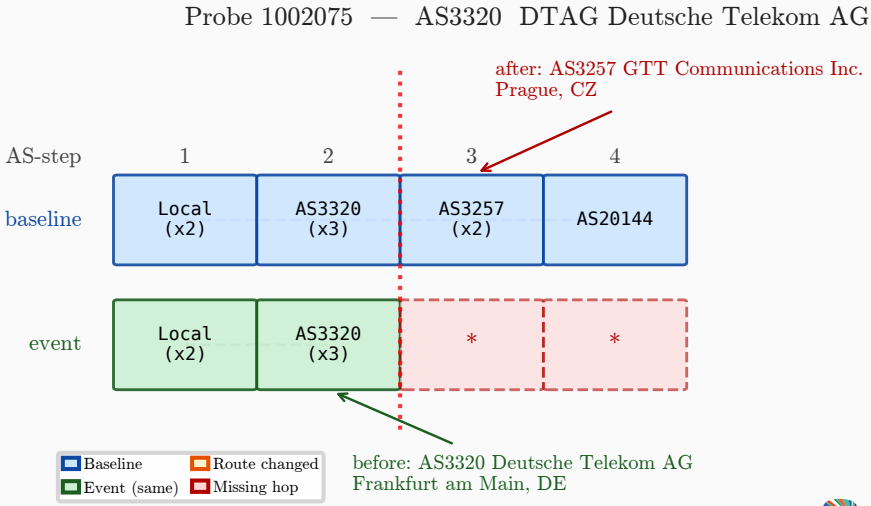
Country	Probes
Germany	464
United States	348
Canada	119
Japan	75

Spread across **97 countries** — not a localized issue.

Which networks? (top 10 ASNs)

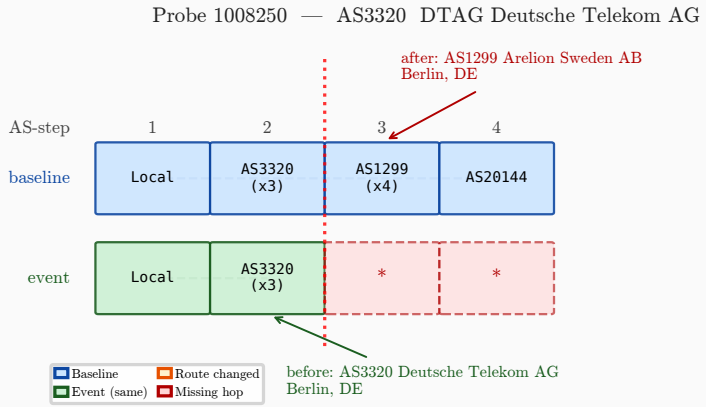
ASN	Network	Timed out	Reached OK	Ratio OK
3320	Deutsche Telekom (DTAG)	353	3	0.8%
33915	Vodafone Libertel (NL)	53	15	22.1%
396982	Google Cloud Platform	40	39	49.4%
16509	Amazon AWS	37	35	48.6%
36352	ColoCrossing	37	5	11.9%
14593	SpaceX Starlink	35	63	64.3%
3292	TDC (DK)	23	0	0.0%
5617	Orange Polska	23	0	0.0%
31898	Oracle Cloud	22	159	87.8%

DTAG AS Path (from traceroutes)



Atlas measurement: https://atlas.ripe.net/measurements/5008/

DTAG AS Path (from traceroutes)



- No route or path changes seen on BGP (RIPE RIS)
- Private peering (PNI) to blame?

Atlas measurement: https://atlas.ripe.net/measurements/5008/

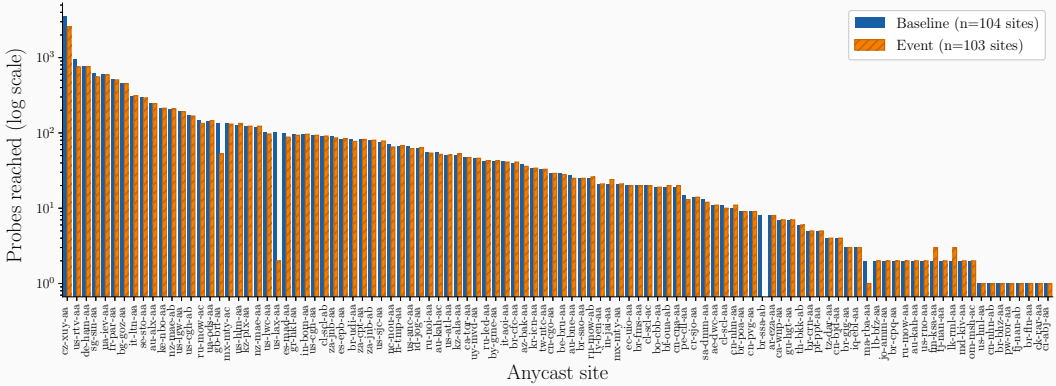
L-ROOT side: which anycast sites were they hitting?

Before the event, the affected probes' **anycast catchments** were:

L-Root site	**Probes**
`cz-xuy-aa` (Czechia)	962
`us-rtv-aa` (US)	390
`sg-sin-aa` (Singapore)	127
`us-lax-aa` (US)	94
`gb-brf-aa` (UK)	80

⇒ probes that *later* timed out used to reach **Czechia** or **US** sites.

Were these sites down? (Atlas sees 103 of 140)

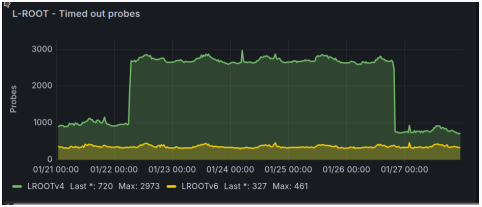


No. Many probes of other ASes reached them

L-Root event: conclusion

- RootViz timeouts $\neq$ **root server fault**
- Issue lived **in the network**, not at L-Root

Takeaway: a root server looking "down" from a Atlas/Rootviz can also mean that the **path is broken**, not the **server**.



L-Root, IPv4 timeouts, Jan 21–27

Lessons Learned

1. **Dashboards help a lot**
2. **Root operators are responsive and open**, and often take the blame for network problems outside their control
3. **Reachability issues: root causes are hard to pinpoint**
4. **The management layer** also plays a role



Tip for students: make the data visible. Dashboards make it easy to eyeball the data and spot patterns.

Recap

RootViz works for eyeballing.

- Real-time view across **all** RIPE Atlas probes
- Already **confirmed events** with Root operators
- Points to **where** to look: country, ASN, anycast site, v4/v6

Step	Done by
Spike detected	RootViz
IPv4 only?	RootViz
Which probes?	Manual
Which anycast sites?	Manual
BGP state check	Manual
Transit AS scan	Manual
Data plane failure	Manual

But the L-Root case shows the limit:

Detection was easy. Root cause took **hours of manual work**.

Students working @ TU Delft

Group 1: software
Event detection & reports

Group 2: research
Per-RSI deep dive

MSc thesis
Automating the analysis

- Open-source; Codeberg link
- Anomaly detection proved **very hard**

5 students, **2 letters** each:

Student	Letters	Report
Joshua Gort	B, D	PDF
Horia Botezatu	F, G	PDF
Jesse Prins	C, K	PDF
Radu Burchel	E, M	PDF
Serban Orza	I, L	PDF
TEMP Link	Download	

- Look into **automating** root-cause analysis

Thank You, TU Delft Students!

Group 1: Software Project

Event detection & reporting

Anuvrat Patil

Halid Çırak

Esin Elibol

Sevda Tozkoparan

Dylan Schotvanger

Starting: MSc Thesis

Joaquin Vaquero*

* Presented before at RIPE meetings

Group 2: BSc Theses

Per-RSI deep dives

Joshua Gort	**B** & **D**-Root (PDF)
Horia Botezatu*	**F** & **G**-Root (PDF)
Jesse Prins	**C** & **K**-Root (PDF)
Radu Burchel	**E** & **M**-Root (PDF)
Serban Orza*	**I** & **L**-Root (PDF)

The reports do deep divers per RSI: methods, data and per-letter findings.

Roadmap: RootViz v2

- **Full automation** of event detection
- **Event labeling** & classification
- **Public datasets** for the community
- **Open-source**

From dashboard to a measurement service.

Try it

https://rootviz.sidnlabs.nl

Questions?

giovane.moura@sidn.nl