AT THE ROOT OF TIMEOUTS

Causality of timeouts for Root DNS Requests: A deep dive into timeout behaviour of root DNS operators B and D.

Joshua Gort | jgort@student.tudelft.nl
Supervisor: Giovane Moura
Faculty EEMCS, Delft University of Technology, The Netherlands

1. Background

- Root DNS → gTLD → Domain resolve (Root B → .nl → tudelft.nl)
- DNS root consists of 13 root letters, served via IP anycast
- Focus on letters B and D
  - B (USC-ISI): small, 6 sites
  - D (UMD/PCH): large, ~231 sites
- RIPE Atlas probes measure timeouts
- **Timeouts still happen often at different times for different root servers, why?**
- Possible causes:
  - **Client-side**: Router/ISP issues
  - **Routing-based**: Somewhere along the path to/from the DNS root server
  - **Server-side**: At the DNS root server

2. Research Question

How do timeout rates of root operators B and D behave over time, and to what extent can individual timeout events be attributed to client-, server-, or route-based causes?

3. Dataset

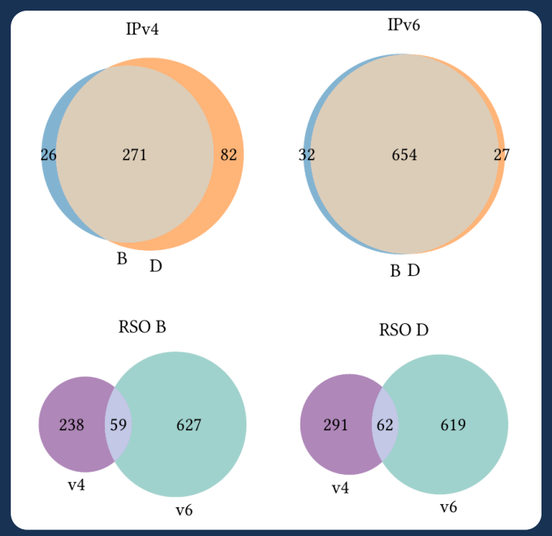
- Study window of 6 months (Dec 2025 - Jun 2025)
- DNS Root server operators B and D
- RIPE Atlas measurements:
  - DNS
  - Traceroute

4. An overview of timeouts over the last six months

Observations:

- Timeout rate consists of two parts: Timeout **floor** and **events**
- Less events occurred in last 2 months
- Events IPv4 vs IPv6:
  D: simultaneous
  B: seperate

5. Timeout floor



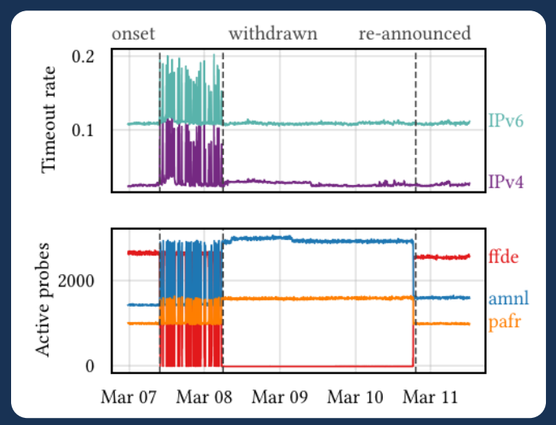
Probes that persistently fail

- Mostly same probes between operators across IPv4 and IPv6
- Difference between probes failing IPv4 vs IPv6
- Larger number of failing IPv6 probes consistent with related work [1]
- **Root cause seems to be (near) client: Probe/router/ISP misconfiguration**

[1] T. Saluja, J. Heidemann, and Y. Pradkin, "Differences in Monitoring the DNS Root Over IPv4 and IPv6," in 2022 IEEE/ACM International Conference on Big Data Computing, Applications and Technologies (BDCAT), Vancouver, WA, USA: IEEE, Dec. 2022, pp. 194–203. doi: 10.1109/BDCAT56447.2022.00036.

6. Case studies

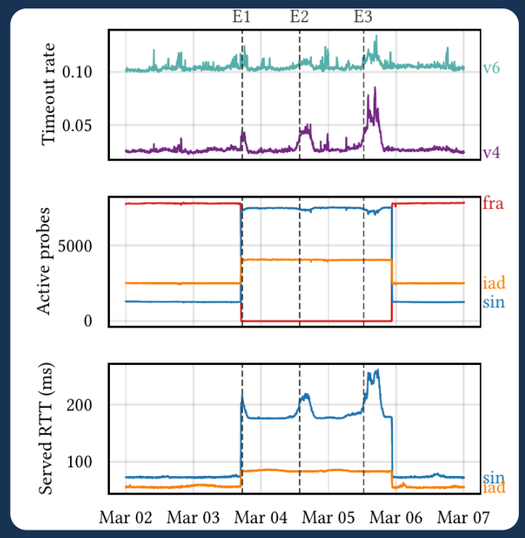
Case 1



1. Frankfurt site seems to fail, but does not withdraw
2. Traffic flow constantly switches between Frankfurt and other sites → Timeout rate increases
3. Once Frankfurt withdraws → Timeout rate back to normal
4. Timeout rate stays normal after re-announcement on March 11

Recommendation: Withdraw a site that stops serving, not just one that goes down.

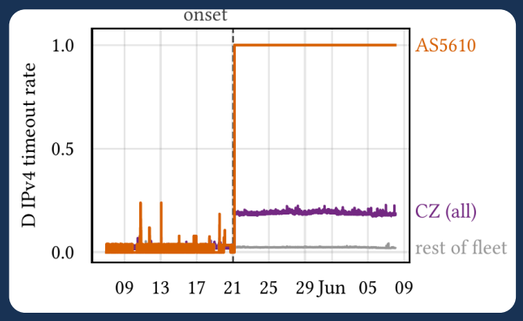
Case 2



1. Frankfurt site fails
2. Sites in Singapore and Washington receive traffic which normally goes to Frankfurt
3. The Singapore site seems to get overloaded on busy parts of the day → Timeout rate increases
4. Once Frankfurt site comes back → Timeout rate back to normal

Recommendation: Provision failover targets for the load they inherit.

Case 3



Observation: Floor of RSO D over IPv4 increased since May 21

- Caused by routing change near AS5610 (Czech ISP, O2 Czech Rep.)
- All probes from AS5610 fail to reach Root DNS operators D and J over IPv4
- Contacted ISP

7. Other recommendations and future work

Recommendation: Monitor reachability from client vantages, and improve return-path observability

Future work: Analyze return-path, other measurement platforms, automated detection and root-cause monitor