DNS Timeouts: Analysis of Root DNS Servers F and G

Author: **Horia-Andrei Botezatu | h.a.botezatu@student.tudelft.nl**
Supervisor & Responsible Professor: **Giovane Moreira Moura**
TU Delft

Background

- The Domain Name System (DNS) is a fundamental part of the Internet's infrastructure, translating human-readable domain names into IP addresses.
- At the top of the DNS hierarchy sit the 13 Root DNS servers (A to M).
- Reliable operation is critical for the reachability of virtually all Internet resources.
- RIPE Atlas operates a global measurement platform with over 14,000 active probes that continuously query these Root DNS servers.
- Data from RIPE Atlas probes reveals unexpected server timeouts that fluctuate periodically rather than randomly.
- Some probes time out repeatedly, while others do so rarely or only towards specific servers.

Main Research Question

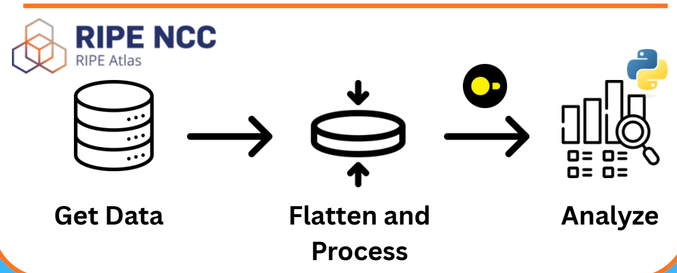
What characterizes and drives the timeout behaviour of RIPE Atlas probes querying Root DNS servers F and G?

Methodology

Dataset

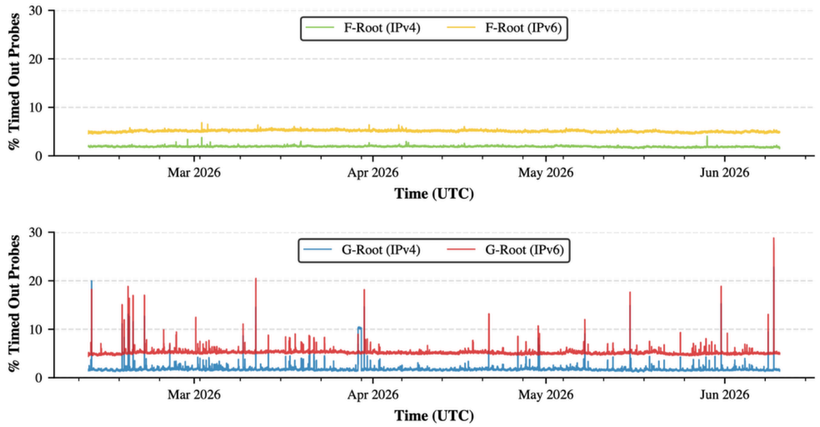
- DNS Measurements & Traceroutes collected from RIPE Atlas, for F & G over both IPv4 & IPv6.
- Period of 4 months (Feb 10th - June 10th 2026).

Data Pipeline



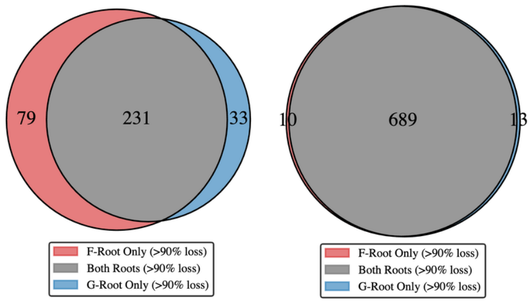
Results & Conclusions

F vs G Contrast



- **F-Root**
  - Operated by Internet Systems Consortium (ISC), American non-profit corporation. Since March 30th 2017 Cloudflare provides additional sites (majority of them).
  - Flat and stable baseline on both protocols.
  - 366 anycast sites, distributed across the world.
- **G-Root**
  - Operated by Defense Information Systems Agency (DISA), under jurisdiction of United States DoD.
  - Low baseline on average, but susceptible to severe spikes.
  - Only 6 sites → increased risk of single points of failure.
  - Severe timeouts happen on both IPv4 and IPv6, and traceroutes show no path issues → issue points to the root server itself.
- **IPv4 vs IPv6**
  - IPv6 runs 2-3x higher than IPv4 on both roots.
  - Same penalty, approximately same size on both roots.
    - Cause is the client-side IPv6 connectivity (the probes), not the servers.

Probe Failure Distribution

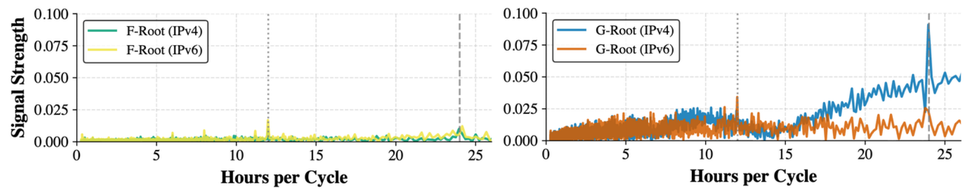


Note: 15225 probes exhibited intermittent or no severe failure (<90% timeouts).

Note: 7830 probes exhibited intermittent or no severe failure (<90% timeouts).

- Probes are isolated into four distinct categories:
  - Intermitent Failures – remain below the 90% failure rate on both protocols
  - Symmetric – fail over 90% towards both roots
  - Asymmetric – fail against one server, while communicating well with the other (< 10% fail rate):
    - F-Root Only
    - G-Root Only
- IPv6 probes are 5x more likely to fail on both roots (8% compared 1.5%) → mostly suffer local, client-side drops.
- IPv4 probes more prone to asymmetric failures (isolated peering disputes, or localised catchment issues).

Temporal Stability



- 12- & 24-hour cycles are real but tiny → the peaks confirm non-random periodicity, but all amplitudes < 0.1 → operationally negligible.
- Severe events are not periodic.

Conclusions

- Timeouts dominate root-server failures (> 95%), but where they come from depens on the protocol and the root.
- Three categories of failures:
  - Client — fails both roots, mostly IPv6 → broken probe connectivity
  - Path — fails one root → routing faults
  - Server — fails both protocols at once → anycast-instance drop (G-Root)
- G-Root's sparse footprint keeps a low median but turns single faults into severe bursts, while F-Root's dense anycast absorbs the same faults as noise.

Limitations

- Results are based on RIPE Atlas probes which are clustered mainly in Europe (and to a lesser extent in North America), introducing a bias mainly towards Europe.
- All case-study attributions rest on external measurements.

Future Work

- Extend analysis window.
- Add return-path data, as traceroutes are only forward-path.
- Add Impact-weighted ranking on the causes to determine the primary one.
- Gather more information from the operators.