Internet Periodic Timeouts: Why Do They Occur?

Analysis of root servers E and M

Radu Burchel | rburchel@student.tudelft.nl | Supervisor: Giovane Moura | Faculty EEMCS, Delft University of Technology

1.Introduction

DNS

The Domain Name System (DNS) is a critical component of Internet infrastructure, resolving domain names into their corresponding IP addresses.

RIPE Atlas

Large-scale measurement platform that enables observation of real-world Internet behavior through over 12,000 globally distributed probes.

Initial findings

Surface level analysis of data gathered by RIPE Atlas probes shows periodic patterns in timeouts and latency of root DNS servers.

Goal

Why do RIPE Atlas probes experience temporary and apparently periodic timeouts when querying Root DNS root servers E and M?

2.Methodology

Steps

1. RIPE Atlas probes
2. DNS Measurement
3. Removed Hijacked Responses
4. Baseline Analysis
5. Rolling Averages & Fourier Analysis
6. Per Site Analysis of Anomalies

3.Root Servers E and M

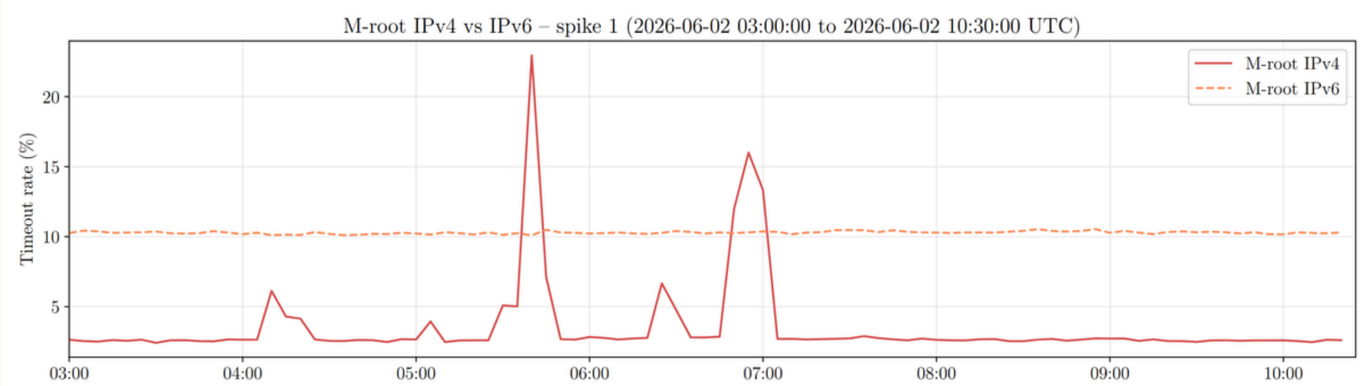
Root-E

- Infrastructure by PCH and Cloudflare, with one server ran by NASA.
- Large globally distributed anycast deployment.
- Sites: 328
- Strong worldwide presence across multiple regions.

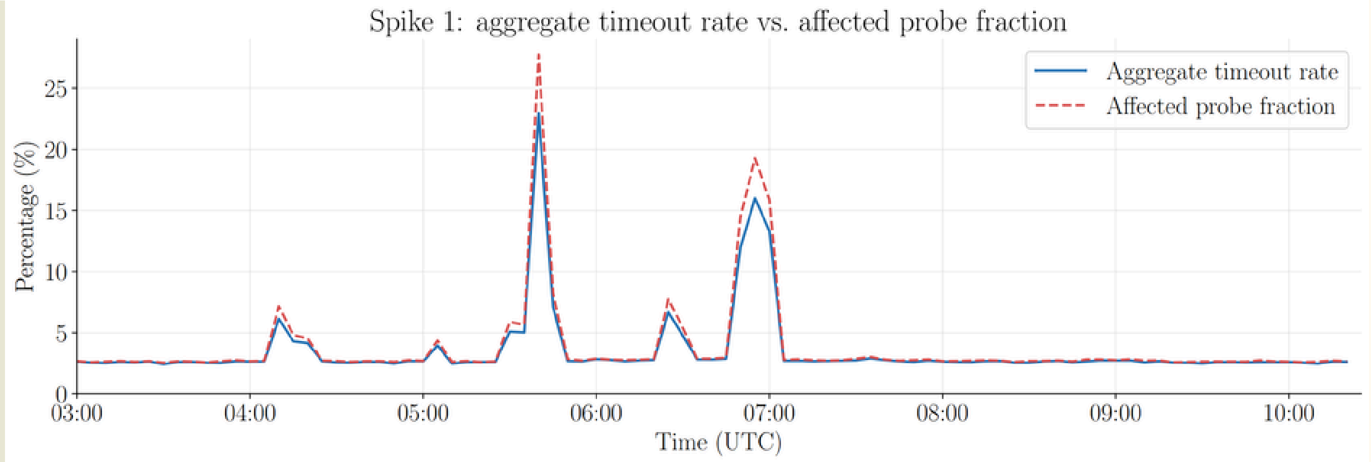
Root-M

- Operated by the WIDE Project, a Japanese academic and research organization.
- Primarily community/research operated.
- Sites: 29
- Deployment is more concentrated in Asia compared to E-root.

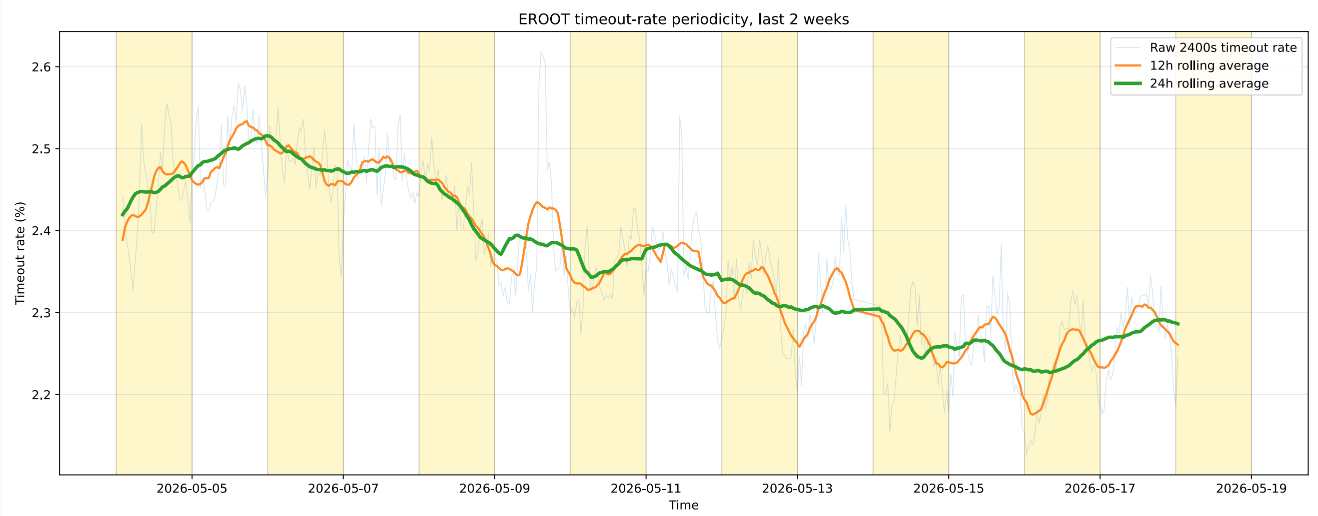
4.Timeout Occurrence and Issues



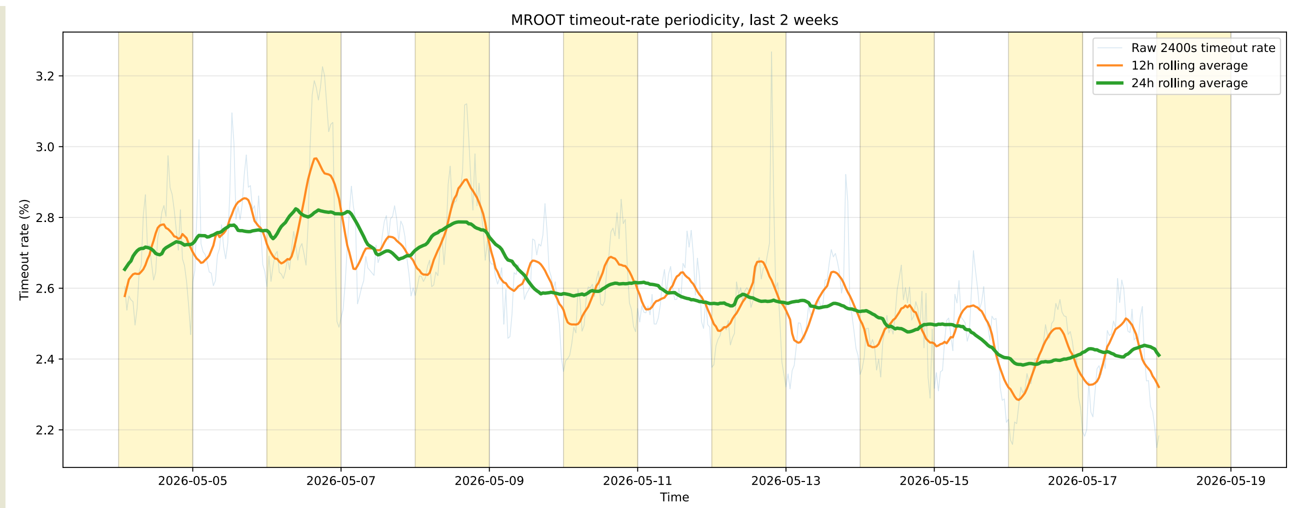
- IPv4-only spikes observed June 2-3, 2026, peaking at 22.95%.
- IPv6 remains stable.



- Spike is directly proportional to percentage of affected probes.
- Failure is not global.



- E-root displays weaker periodic timeout oscillations.
- Timeout behaviour appears smoother across time.



- M-root exhibits stronger recurring timeout oscillations.
- 12-hour periodic patterns are more visible.

5.Data Filtering

Timeouts

- Some probes consistently timeout and this can affect the data.

DNS Hijacking

- Some probes receive responses from DNS servers other than the intended root server.
- This behavior is often caused by enterprise firewalls or DNS interception mechanisms.

6.Discussion

Limitations

- Timeouts do not return a site ID, so the heuristics used to determine it might be wrong.
- The timeouts can happen in the network layer before reaching the server, not being the DNS server's fault (and this likely happens often).
- Probes are mostly localised in Europe and North America, other regions not being as dense.

Lessons Learned

- Internet measurements are inherently very noisy.
- External data is often not enough to achieve certain conclusions.
- Aggregate timeout rates can be misleading when dominated by a small number of persistently broken probes.

7.Conclusion

- M-root exhibits stronger periodic timeout behaviour than E-root. This could be due to worse load balancing resulting from the lower site count.
- Peaks are especially visible around 12-hour timescales.
- The vast majority of probes have correlated timeout behaviour across both roots.
- Timeouts can happen in more ways than server errors or server downtime.