The Roots Go Deep: Measuring '.' Under Change

Florian Steurer
Max Planck Institute for Informatics
Saarland University
Saarbruecken, Germany
fsteurer@mpi-inf.mpg.de

Daniel Wagner
DE-CIX
Frankfurt, Germany
daniel.wagner@de-cix.net

Danny Lachos
BENOCS GmbH
Berlin, Germany
dlachos@benocs.com

Anja Feldmann
Max Planck Institute for Informatics
Saarbruecken, Germany
anja@mpi-inf.mpg.de

Tobias Fiebig
Max Planck Institute for Informatics
Saarbruecken, Germany
tfiebig@mpi-inf.mpg.de

Abstract

As the entry point to the DNS hierarchy, the DNS root zone, served by the DNS root server system, is essential for the Internet. It consists of 13 deployments managed by 12 independent root server operators. Due to its importance, the root zone deserves special scrutiny, which it has received from researchers and operators alike.

In this study, we measure all root servers over a period of 174 days from 675 vantage points in 523 networks and 62 countries using IPv4 and IPv6. Using this data, we first investigate the *co-location* between root servers, finding that almost 70% of clients observe co-location of at least two servers. Second, we monitor the *integrity* of zone transfers, finding rare issues like bitflips or stale zone files. Finally, by enriching our data with passive ISP and IXP data, we quantify the *role of IPv6* for performance and behavior under change, finding that even seemingly similar subsets of root servers can differ considerably.

CCS Concepts

• **Networks** → **Network measurement**.

Keywords

DNS, Root Zone, Anycast

ACM Reference Format:
Florian Steurer, Daniel Wagner, Danny Lachos, Anja Feldmann, and Tobias Fiebig. 2024. The Roots Go Deep: Measuring '.' Under Change. In *Proceedings of the 2024 ACM Internet Measurement Conference (IMC '24), November 4–6, 2024, Madrid, Spain.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3646547.3689008

1 Introduction

The root zone is the top of the DNS hierarchy, containing the delegations to the top-level domains. DNS root servers MUST answer queries for the root zone [6], providing a crucial function for DNS and the Internet. RSSAC037 [16] reflects this importance, defining stability, reliability, and resilience goals for root server operations.

IMC '24, November 4–6, 2024, Madrid, Spain

ACM ISBN 979-8-4007-0592-2/24/11
https://doi.org/10.1145/3646547.3689008

To remain fast and reliable in a growing Internet, the scale of the root server system (RSS) steadily grew. As of 2023-12-24, the RSS consists of 1750 instances, operated by 12 independent operators, and serving tens of billions of queries per day [40].

However, such a large deployment may lead to co-location of servers, as it is attractive to deploy instances at locations with good (local) connectivity, such as IXPs. Co-location and the reuse of last hop infrastructure may reduce the redundancy of the system and consequently, negatively affect stability and reliability. Thus, we examine: *How much server co-location exists in the RSS? (RQ1).*

Using active traceroute measurements, we find that co-location is prevalent with almost 70% of clients observing co-location of two or more root servers and some clients being routed to sites with 12 root servers present. While *not* questioning the reliability of the system as a whole, our results indicate that diversifying last-hop infrastructure at certain sites may be worthwhile.

As one of the first systems to deploy IP anycast, and due to the availability of rich data sources [11], the RSS became one of the most popular systems to study the behavior of anycast in practice. Existing studies have investigated performance [20, 38], routing stability [20, 31] or how resolvers react to changes in the RSS [24].

However, existing studies of the root servers' anycast deployment focus on IPv4. To the best of our knowledge, there is no study which comprehensively examines these characteristics for *all* root servers using IPv6. It remains unclear whether results obtained via IPv4 are applicable to IPv6. This work aims to close this gap, answering the question: *What are the differences in the root servers' performance and behavior between IPv4 and IPv6 (RQ2).*

Utilizing data from a large scale active measurement, we show that clients of individual servers are up to 40% (`g.root`) more likely to experience changes of the contacted anycast site when querying via IPv6. While we observe that the overall geographical distance from clients to the contacted anycast sites is comparable to IPv4, we find differences in the experienced RTTs based on the clients location. For example, even though `i.root` and `l.root` have a similar number of replicas deployed in South America, clients experience more than 100% longer RTTs for `i.root` on IPv6 compared to IPv4, whereas clients from `l.root` see 39% lower IPv6 than IPv4 RTTs.

To study the behavior under change, we monitor the change of the `b.root` IP address using passive traffic traces collected at a large European ISP and multiple IXPs. Our findings confirm prior results by Lentz et al. [24] but, again, indicate differences in the behavior of IPv4 and IPv6 clients. We observe that IPv6 clients may be more

eager to adopt the new IP address and see vast differences in traffic shifts at IXPs in Europe, where 61% of traffic switches to the new IPv6 address, and North America, where only 17% of traffic does.

Overall, our findings show that differences between IPv4 and IPv6 manifest in non-obvious ways based on root server deployment and geographical region and are not easily generalizable. Thus, we argue that future studies should carefully assess how their (sub)set of root servers or VPs may impact results.

Finally, we investigate the reliability of zone file distribution mechanisms from a clients' perspective, asking: *Is the integrity of the root zone file distribution sufficiently protected? (RQ3).* In context of the introduction of a new integrity check for zone files (ZONEMD), we analyze zones obtained via zone transfers, CZDS and the IANA website. While we find no issues in CZDS and IANA downloads, we observe cases of bitflips and stale zones in zone transfers. Our results highlight, that ZONEMD is a valuable addition to the DNS ecosystem.

To facilitate future work, we open-source our measurement data, featuring 7B DNS queries, 78M zone transfers and 169M traceroutes.

2 Background

RFC9499 [15] documents current DNS terminology, and RFC9199 [33] best practices for authoritative anycast DNS server operations.

The root servers differ considerably in their deployment strategy. For example, `f.root` is present at a total of 345 unique sites worldwide, whereas `b.root` deploys only 6 sites. As found by Koch et al. [20], larger deployments tend to offer better RTTs even though they are less likely to route a client to the geographically closest replica. Therefore, when analyzing such anycast performance metrics, one has to consider the characteristics of the deployment at hand.

Furthermore, some clients may not even be able to reach their geographically closest site, as some root servers deploy so-called local sites. A local site can be local to an AS (e.g., a large ISP) or a metro area/geographic region (e.g., by using the reachability of an IXP). This is realized by marking the route announcements of the root servers as non-exportable. A global site, on the other hand, is reachable by every host on the Internet if selected.

The exact location and type of their sites are reported by the root server operators via `root-servers.org` [40]. Some servers deploy a large number of global and local sites, namely `e.root` (97 global/147 local), `f.root` (129/216), `j.root` (61/85) and `a.root` (33/23). `b.root` (6/0), `c.root` (12/0), `g.root` (6/0), `h.root` (12/0), `i.root` (81/0) and `l.root` (132/0) use no local sites at all, while `k.root` (105/11) still deploys some local sites. `d.root` (23/186) uses many more local than global sites. `m.root` (7/9) focusses on Asia-Pacific, having only 2 sites outside the region.

3 Related Work

Here, we distinguish between studies of root servers, studies under change and studies of clients.

Studies of Root Servers: Being one of the earliest and most prominent anycast deployments, studies of the root are often used to assess the performance and resiliency of IP anycast. Typically, these studies focus on RTT [3, 10, 12, 14, 20, 23, 26, 28, 30, 38], the distance that requests travel to the selected replicas [2, 20, 26, 31, 41] or how often a clients experience routing changes [2, 3, 20, 31]. Notably, understanding RTT characteristics can also help to detect unauthorized root replicas/caches, as shown by Jones et al. [18].

However, all of these studies are either entirely IPv4-focussed or offer no dedicated comparison between IPv4 and IPv6. Moreover, many studies focus only on a subset of root servers, e.g. the study by Schmidt et al. [38], which is able to *exactly* quantify the additional delay induced by clients not being routed to their optimal replica. However, due to methodological constraints, the study only considers four root servers. A much larger subset of servers (all but `{g,i}.root`) is considered by Koch et al. [20]. They find that route inflation and the corresponding increase in geographic distance is not an inherent property of anycast. They then argue that the root server system may not be representative of anycast in general. However, they also exclude IPv6 data from their analysis.

As previous work has shown that differences between individual root servers can be substantial (e.g. Li et al. [26] for `d.root` vs `c.root`), it is important to include as many root servers as possible in a study. Otherwise, effects unique to specific servers or specific regions may be missed. Thus, our study extends previous work by offering an analysis of all root servers, considering the differences between IPv4 and IPv6. Notably, we find differences in site stability and performance over different regions, deployments and IP families, indicating that individual root deployments do not generalize.

Another recent body of work focusses on understudied regions, e.g., mainland China [8, 25, 27, 45]. Given the regional differences observed in our work, extending these efforts to other regions, such as South America and Africa, would be a worthwhile endeavor.

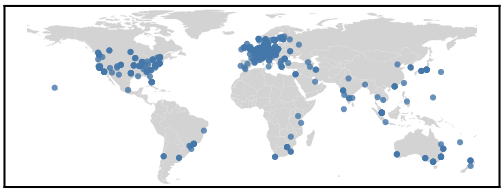
Studies under Change: Researchers also used opportunities to study the behavior of the DNS under change, e.g., Mueller et al. [34] studied the root's first KSK-rollover. They find no major problems in the process and give recommendations for future changes.

Lentz et al. [24] looked at the address change of `d.root` in 2013. They observed an increase in total traffic. At the same time, some resolvers were reluctant to switch to the new IP address. This matches with the long-term perspective from Wessels et al. [44]. They found that even 13 years after an IP change for `j.root`, the old address still received traffic. Similar observations regarding traffic increase were made by Barber et al. [4] (`d.root`) and Manning [32] (`b.root`), who monitored the effects of switching to anycast addresses.

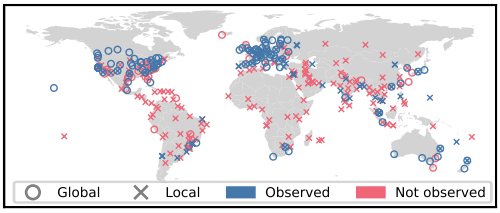
Ten years after the study by Lentz et al. [24], we confirm the reluctancy of clients to switch to a new root server address for `b.root`. Moreover, our results suggest that IPv6 clients may be more eager to switch than IPv4 clients. Our IXP vantage points observe traffic in Europe to be more eager to switch than in North America.

Studies of Clients: DNS queries received by root servers have been frequently used to study clients' query behaviors. One example is the *Day In The Life Of The Internet* (DITL) dataset [11], containing regular traces from participating root servers. Using DITL data, Brownlee et al. [5] and Castro et al. [7] found that the root often receives malformed or repeated queries from the same host. Gao et al. [13] focus on resolvers, finding more than half of all queries fail due to non-existent TLDs, opening a vector for MitM attacks [9].

The fact that most queries to the root are avoidable, motivated Allman [1] to propose the use of local copies of the root zone at recursive resolvers to reduce load on the RSS. However, resolvers must be able to verify the correctness of their local copy as, e.g., enabled by ZONEMD [42]. Our analysis shows that such a verification is in fact needed and that ZONEMD is a valuable addition to the DNS.



(a) VPs–NLNOG clients.



(b) `f.root` instances.

Figure 1: Root server instance coverage.

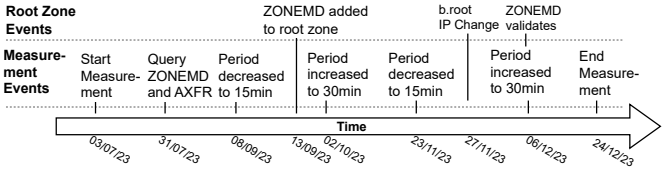


Figure 2: Measurement timeline and root zone events

4 Methodology

To address our research questions, we develop a methodology which allows us to study all root servers using active measurement for IPv4 and IPv6. To better assess the effects of `b.root`'s IP change, we complement our measurement data with passive ISP and IXP traces.

4.1 Datasets

Active Measurement: We used 675 NLNOG RING [37] nodes in 523 ASes and 62 countries as vantage points, see Figure 1a, to run regular active probes between 2023-07-03 and 2023-12-24.

In every measurement, each vantage point (1) conducts a traceroute to each root server via IPv4 and IPv6 and (2) queries the `A`, `AAAA`, and `TXT` records for each of the root servers as well as `NS` for the root and root-servers.net from each root server IP, (3) requests a zone transfer via AXFR from each root server IP and (4) queries `version.bind`, `version.server`, `hostname.bind`, and `id.server` for each root server IP. All queries use `dig @IP +retry=0 +timeout=1`. The full measurement script is in Appendix F. The final dataset includes 7.7 B DNS queries, 78 M zone transfers, and 169 M traceroutes.

In general, our measurement interval per NLNOG RING node is 30 minutes. To closely monitor the rollout of `ZONEMD` and the renumbering of `b.root`, we decreased the interval to 15 minutes from 2023-09-08 to 2023-10-02 and 2023-11-20 to 2023-12-06, see Figure 2 for a timeline. All our measurements were discussed and cleared with the RING administrators in advance. Our script provides contact information and our access to the RING is not sponsored, i.e., we contributed to the infrastructure as normal participants well before this study. Also, see the ethics section in Appendix B.

***IXP-DNS-1*:** We use passive traffic traces from 14 IXPs located in Europe and North America as vantage points. These traces capture traffic in the IXP fabric that is going to or coming from the subnets (/24 for IPv4 and /48 for IPv6) of all root server IPs, including the

Root	Global Site Coverage # Sites	# Cov.	% Cov.	Local Site Coverage # Sites	# Cov.	% Cov.	Total Site Coverage # Sites	# Cov.	% Cov.
a	33	30	90.9	23	20	87.0	56	50	89.3
b	6	6	100.0	0	0	-	6	6	100.0
c	12	12	100.0	0	0	-	12	12	100.0
d	23	23	100.0	186	78	41.9	209	101	48.3
e	97	70	72.2	147	44	29.9	244	114	46.7
f	129	96	74.4	216	60	27.8	345	156	45.2
g	6	6	100.0	0	0	-	6	6	100.0
h	12	12	100.0	0	0	-	12	12	100.0
i	81	61	75.3	0	0	-	81	61	75.3
j	61	47	77.0	85	64	75.3	146	111	76.0
k	105	74	70.4	11	4	36.4	116	78	67.2
l	132	82	62.1	0	0	-	132	82	62.1
m	7	7	100.0	9	7	77.8	16	14	87.5

Table 1: Coverage of root sites (worldwide).

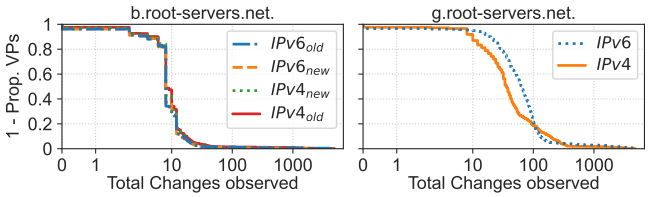


Figure 3: Complementary eCDF of change events for `{b,g}.root`.

subnets of the old and new `b.root` IPs. The IXP traces do not contain any payload, are heavily sampled and aggregated based on their anonymized header information. As a privacy measure, no further header information is stored or processed. This implies that we cannot filter out Internet background radiation, spoofed, or non-DNS traffic. However, we expect the noise to be negligible[1] and, thus, consider the privacy tradeoffs reasonable. The data spans the time from 2023-10-26 to 2023-12-28 and 2024-04-22 to 2024-04-29.

***ISP-DNS-1*:** We analyze passive traces from a large European end-user ISP, spanning from 2024-02-05 to 2024-03-04, 2024-04-22 to 2024-04-29, and one day, 2023-10-08, before the change. The same limitations as with the IXP data hold, as this dataset captures traffic to/from the old/new `b.root` subnets (/24 for IPv4 and /48 for IPv6).

4.2 Dataset Validation

Before starting our main analysis, we check that core aspects of the NLNOG RING measurements are consistent with prior results.

Coverage: To verify that our choice of vantage points does not bias our dataset geographically, we compare the observed root server sites with the ground truth as reported by `root-servers.org` [40]. For this, we match the node names, i.e., answers to `hostname.bind` resp. `id.server`[2] queries. We can map 1,469 out of 1,604 observed server identifiers to root server instances while 135 identifiers (75 from `j.root`) remain unmapped. Figure 1 visualizes the VP locations and our coverage of `f.root` instances, and Figure 11 shows all roots.

Overall, our active measurements have a good coverage for the global sites of all root servers, see Table 1 (worldwide) and Table 4 (per region). Yet, as expected we do not cover all local sites. Thus, for deployments that focus on local sites, e.g., `f.root`, we find good coverage of global sites (96/129) but lower local site (60/216) coverage. Still, we do cover a significant fraction of local sites as well.

[1]For *ISP-DNS-1*, 1.75% of measured UDP and TCP traffic is not from Port 53. While not directly transferable to *IXP-DNS-1*, it provides intuition on expected non-DNS traffic. Additionally, previous work found less than 1.1% of spoofed traffic in similar data [29].
[2]For `{a,c,j,e}.root` we use the IATA airport codes in the nodes' hostnames, as they either do not report identifiers or the identifiers do not map to those published online. This makes nodes in the same metro indistinguishable.

Site Stability: Prior work disagrees on whether the routing/mapping of VP to root server instance is relatively stable. For example, Barber et al. [4] find unexpected churn, while Koch et al. [20] later find that 80% of /24's send all queries to a single site. Analyzing changes, i.e., two subsequent measurements on the same VP reaching different sites, in our dataset, we find *both* behaviors, see Figure 3. The frequency of changes, especially in the long-tail, may depend on the deployment's size, as suggested by Koch et al. [20]

For `b.root`, we find that during our measurement, the median number of changes experienced by a VP is only 8 for both, IPv4 and IPv6. For `g.root` however, VPs experience a median of 36 changes for IPv4 and 64 changes for IPv6. This is surprising, as `g.root` and `b.root` both deploy only 6 anycast sites, yet the routing for `b.root` is considerably more stable. `g.root`, also shows more changes for IPv6, an effect that can be observed for `c.root` and `h.root` as well. Overall, we see differences between root servers, even for seemingly similar deployments, thus, we caution against drawing conclusions about the root server system after studying only a subset of servers.

5 Server Co-Location

In order to handle a growing number of requests, the scale of the RSS has been steadily growing. However, a large number of replicas deployed by different providers may lead to server co-location, as it is attractive to deploy at locations with good (local) connectivity, such as data centers or IXPs. This reuse of the same last-hop infrastructure may reduce the redundancy of an anycast setup.

In principle, this *should* not be an issue. Still, a failure of such a clustered location can, instantaneously, shift traffic to other locations. Moreover, an increase in RTT may cause resolvers to switch to other root server deployments and cause unexpected traffic for servers that are not directly affected by the failure. While unlikely, such an event might lead to unnecessary stress on the system.

To better quantify how much "reduced redundancy" exists due to server co-location in the same facilities and networks, we use the collected traceroutes. Indeed, servers that share the same second-to-last hop are likely to be co-located. Thus, the total number of second-to-last hops minus the unique number is the reduced redundancy. Hops missed by traceroute are treated as unique, so our analysis provides a lower bound on the actual reduced redundancy.

Overall, the reduced redundancy per continent, see Figure 4, is relatively balanced. Still, individual vantage points in North America and Oceania have a reduced redundancy of 8 or more (out of a maximum of 12) for IPv6. For Africa we find that IPv6 has slightly less reduced redundancy if it occurs, while this is the opposite for South America, likely due to out-of-continent routing. There, AS6939 carries significant IPv6 traffic for several root servers, while closer replica with RTTs below 10ms would be available, e.g., for `l.root`. For South America, AS12956 fills this role for IPv4.

Key Takeaway: Root server co-location is prevalent, with ~70% of VPs observing co-location of at least two servers. These results indicate that diversifying last-hop infrastructure at certain sites may improve redundancy, but do *not* question reliability of the RSS.

6 The Role of IPv6

Geographical Distance & RTT: As previous work [20, 26, 38] has shown, clients are not always routed/mapped to the geographically closest anycast instance, negatively impacting RTTs. We now

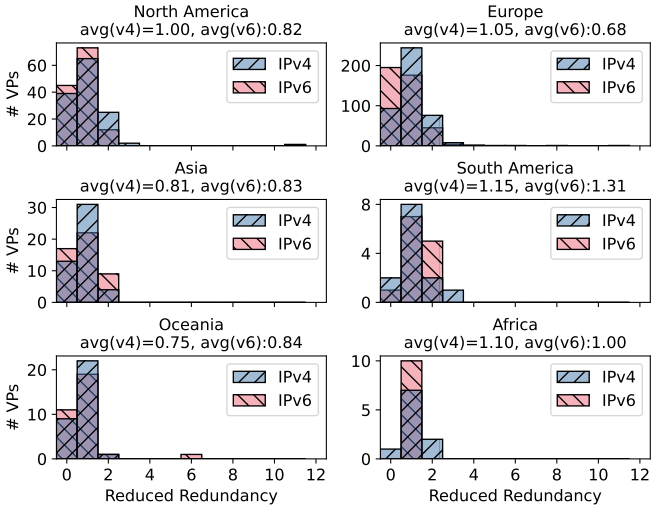


Figure 4: Reduced redundancy due to shared last hop.

study the impact of IPv6 and geographic region on the root servers' performance as well as behavior under change (*RQ2*).

Figure 5 highlights, for each request, the difference in distance between the geographically closest global instance vs. the one that it was routed to. Requests routed to their closest global replica land on the diagonal. Requests routed to a (closer) local replica fall below it, while requests routed to a suboptimal (more distant) instance land above the diagonal. Overall, we see that most requests (78.2%/82.2% for `b.root` v4/v6 and 79.5%/81.0% for `m.root`) are routed to their closest global instance or to an even closer local instance.

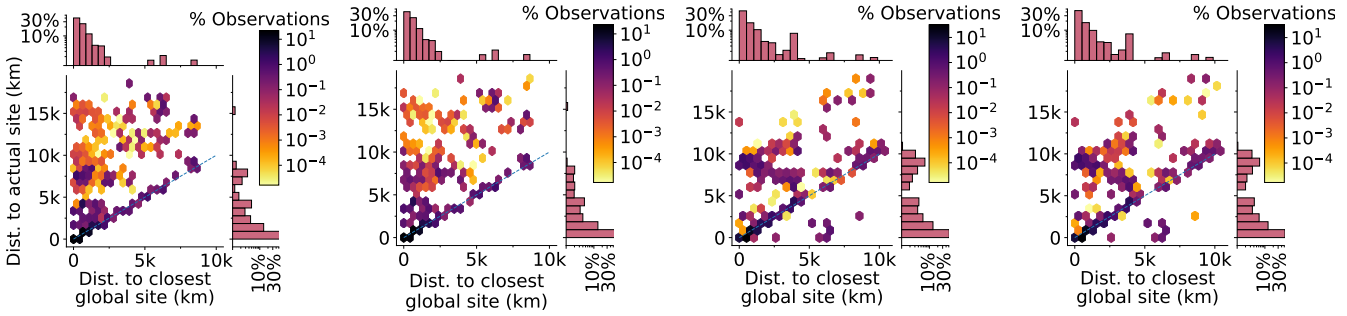
On a per client-basis, we see that 79.5% of `b.root` clients experience an average additional distance of less than 1,000km. However, 21.5% of clients face additional distances of up to 15,000km. Due to the speed of light in fiber every 1,000km induces ~10ms of delay.

For `m.root`, we see only small differences between IPv4 and IPv6, e.g., the local site at distance ~2.5K km but global distance of ~8K km is more prominent for IPv4. To evaluate regional differences in RTT directly, we depict these in a violin plot, Figure 6, of the RTTs from VPs per region per root deployment per IP version.

For example, `a.root` has a higher average latency (168.3ms vs. 140.0ms) and standard deviation (83.2ms vs. 64.8ms) in South America for IPv4 than for IPv6. This is due to two paths being less pronounced (via AS10834 or AS27651, and then AS12956) or absent for IPv6 (via AS60068 and then AS12956). Inversely, for the same region, `h.root` (43.7ms vs. 53.7ms) and `i.root` (23.8ms vs. 50.9ms) show higher IPv6 latency for similar reasons, involving different paths.

These patterns are not specific to regions with a low number of VPs, as, e.g., `i.root` shows a 26.2% lower average latency for IPv6 over IPv4 (46.2ms vs. 62.6ms) in North America. Here, this is due to paths via AS6939 having a lower average latency for IPv6 (23.4ms) than for IPv4 (221.4ms), while AS6939 is also more frequent for IPv6 paths. A possible explanation is AS6939's open peering policy.

We find a similar effect in the African region, albeit increasing RTT, for `l.root`, where IPv4 paths via AS6939 are rare, while for IPv6 a majority of paths traverse AS6939, transporting traffic to a more remote replica with an average RTT of 62.5ms. For additional context, please see the limitations in Appendix E.



(a) `b.root` (new IPv4). (b) `b.root` (new IPv6). (c) `m.root` (IPv4). (d) `m.root` (IPv6).

Figure 5: Distance per request from VPs to root sites.

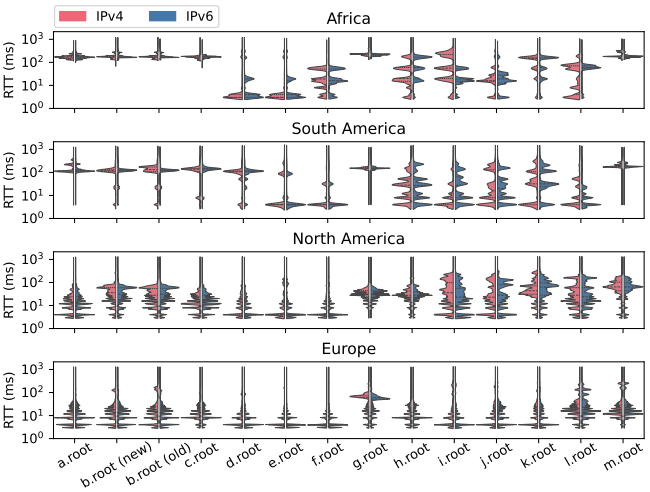


Figure 6: RTTs of requests by continent.

Key Takeaway: Even seemingly similar deployments may exhibit considerable RTT differences per IP version and region. Upstream providers and individual routing policies play a major role. Thus, future work should include routing information when assessing IPv4 and IPv6 RTTs, especially in anycast scenarios

Adaption of new `b.root`: Previous work has investigated the effect of address changes, finding an overall increase in queries [24] and that some resolvers are reluctant to change [4, 24, 32, 44]. We now look at passive traffic traces in order to examine the effects of `b.root`'s address change on these networks, focussing on differences between IPv4 and IPv6-enabled clients.

Figure 7 shows the normalized `b.root` traffic from *ISP-DNS-1* around the change. See Figure 12 for graphs of all roots and datasets.

With regards to the mix of IPv4/v6, we find that on 2023-10-08, the traffic share for the old `b.root` subnets was 10.0%-21.0% for IPv6 and 76.1%-88.9% for IPv4. The new subnets, being already operational but not yet included in the root zone, already receive a small fraction of 0.8% (0.7% IPv4/0.1% IPv6) of the traffic. Subsequently, in the four weeks from 2024-02-05 to 2024-03-04, the new IPv4 subnet receives the majority of traffic (76.2%), while the old IPv4 subnet (11.3%) still receives almost as much traffic as the new IPv6 subnet (12.0%). Looking at the in-address-family shift ratio, we find that only 87.1% IPv4 traffic has shifted, while almost 96.3% of the IPv6 traffic has. This may be due to priming [19] being more likely to be present in newer devices, similar to IPv6 support.

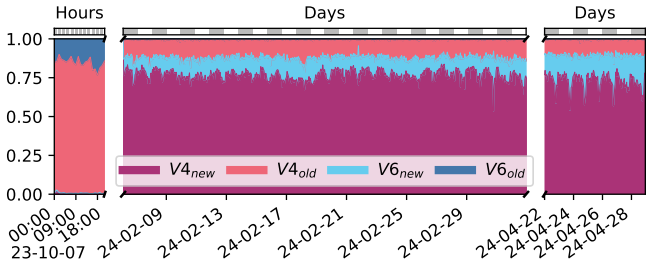


Figure 7: ISP: Traffic to `b.root` before/after change.

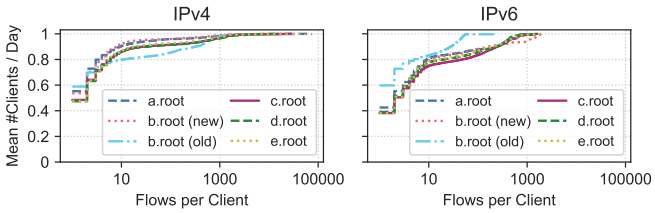


Figure 8: ISP: Mean # of unique client subnets per day.

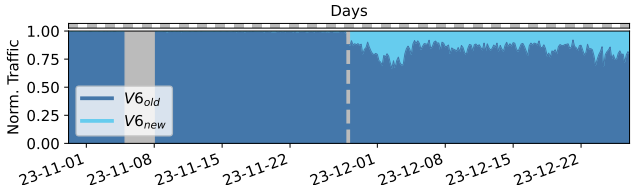
To confirm this conjecture, we check how often clients contact a root server per day after the change, see Figure 8. Indeed, the old `b.root` IPv6 subnets sees more clients contacting it only once per day. This is consistent with priming, where IPv6-enabled clients contact the old `b.root` once and then refrain from using the old subnets.

Figure 9 shows the normalized traffic for `b.root` from *IXP-DNS-1* for North America and Europe around the change. We focus on IPv6 traffic, since the fraction of IPv4 traffic is small. Unlike at the ISP, a large portion of IPv6 traffic is still going to the old subnet, differing per region: In North America, 16.5% of traffic shifts to the new subnet, whereas it is 60.8% in Europe. This could be explained by regional differences in CPEs supporting IPv6, but not priming.

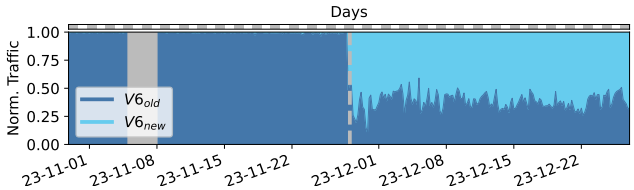
Key Takeaway: Ten years after the study by Lentz et al. [24], some resolvers are still reluctant to switch to a new IP address. We find (IPv6) traffic in Europe more eager to switch than in North America. Finally, our results indicate that IPv6 clients may be more eager to switch to a new IP address than IPv4 clients.

7 `ZONEMD` Roll-Out:

Moving to our third research question *Is the integrity of root zone file distribution sufficiently protected? (RQ3)*, we now present an analysis of the recent `ZONEMD` roll-out. The `ZONEMD` record, contains a message digest for the entire zone–including delegations and glue



(a) North America



(b) Europe

Figure 9: IXP: IPv6 traffic to `b.root`.

Reason	#SOA	First Obs.	Last Obs.	#Obs.	Server	VP_{id}
Sig. not incepted	5	23-12-21 10:35	23-12-23 10:35	5	all	1
	1	23-10-02 22:00	23-10-02 22:00	1	all	2
Bogus Signature	2	23-09-26 21:46	23-10-24 10:00	3	d(v6)	3
	2	23-11-18 07:30	23-11-21 06:16	2	g(v6), b(old v4)	4
	3	23-09-26 10:15	23-10-09 07:00	3	c(v6), g(v4)	5
Signature expired	1	23-08-16 10:00	23-08-16 11:31	12	d(v6)	6-8
	1	23-10-06 10:00	23-10-06 13:31	40	d(v4), d(v6)	9-16

Table 2: ZONEMD validation errors for zones from AXFRS.

```
world. 86400 IN RRSIG NSEC 8 1\
             20231201050000 20231118040000 46780 . ps...MVqw...Hg==
world. 86400 IN RRSIG NSEC 8 1 86400\
             20231201050000 20231118040000 46780 . ps...MICw...Hg==
```

Figure 10: Bitflip in RRSIG in zone from AXFR.

records not covered by DNSSEC [42]. It enables zone verification regardless of how the zone was obtained. This is useful, e.g., when operating a local root server [21, 22] or when using local copies of the root zone for resolution [1].

ZONEMD was rolled out incrementally [43] in the root zone during our measurement period. A non-validating ZONEMD record was added using a private hash algorithm on 2023-09-13. From 2023-12-06, the record uses SHA-384, making it verifiable. The situation will be monitored by the root operators for at least one year [39], before further action is taken, e.g., rejecting non-verifying zones. Currently, no other zones available via CZDS use ZONEMD.

Our study provides an independent temporal perspective on the roll-out. We use `ldnsutils` [36] to fully validate obtained zones, i.e., checking ZONEMD and all RRSIG records against the root DNSKEYS. We verify copies of the root zone file from the following sources:
ICANN CZDS: 194 root zone files from 2023-09-15 to 2024-03-27. Files from 2023-09-21 to 2023-12-07 show ZONEMD records but do not validate, while all later files correctly validate.
IANA Download: 23,823 root zone files downloaded from IANA's website [17] every 15 minutes between 2023-07-11 and 2024-02-14. The first ZONEMD record appears on 2023-09-21T13:30:00 UTC and zones validate from 2023-12-06T20:30:00 UTC on.
NLNOG-DNS-1 dataset: 75,656,924 root zone files, of which 15 distinct zone files from 66 observations do not validate, see Table 2.

Signatures are regularly updated and time-nonced, thus, validation time matters. By validating each zone file using the first and last observation timestamp, we find six cases where time-related validation errors occur on two VPs due to inaccurate VP clocks.

Notably, we encounter eight transfers with `bitflips`, see Figure 10, affecting three VPs and five servers, when comparing non-verifying zones received via AXFR with a version downloaded from ICANN with the same SOA. While the bitflips are most likely due to faulty VP memory, we cannot exclude that it occurred in transit or on the server. In one case, the bitflip affected a top-level domain (`.ruhr` becoming .buèr). Although we did not observe this, an affected name server name is a vector for homograph attacks [35]. Two `d.root` sites, in Tokyo (3 VPs) and Leeds (7 VPs), served a zone file with an expired signature, likely due to a stale local zone file.

Note that even though most observations occurred before the introduction of a validating ZONEMD record, the ZONEMD validation would have allowed to catch these, had it been already in place. ZONEMD will even allow to catch issues in glue/delegation records not covered by DNSSEC. Parties ingesting ZONEMD signed zone files will be able to implement appropriate fallback mechanisms such as rescheduling a zone transfer from a different root server, and avoid rare, yet hard-to-debug problems, such as bitflips or stale versions.
Key Takeaway: While the roll-out of ZONEMD did not encounter unexpected events, we observed rare issues such as bitflips or stale zone files in zone transfers. ZONEMD is an effective way to spot them.

8 Conclusion

By studying all root servers, including IPv4 and IPv6, using 675 vantage points in 62 countries, complemented by passive traces from the *ISP-DNS-1* and *IXP-DNS-1* datasets, our work finds new effects, confirms prior assumptions, and enables future work.
Server Co-Location: Co-location of root servers is prevalent with almost 70% of clients observing a co-location of two or more root servers, with a maximum of 12 co-located servers. Hence, while *not* questioning reliability of the RSS as a whole, diversifying last-hop infrastructure at certain sites may improve redundancy.
IPv4 vs. IPv6: We find varying differences between IPv4 and IPv6 RTTs, rooted in path selection and replicas, manifesting per region in non-obvious ways, see, e.g., `a.root` and `i.root` in Section 6. This aligns with the delay in `b.root` traffic switching to the new IPv6 address per region *IXP-DNS-1*, requiring future research.

Future work assessing IPv4/IPv6 performance in terms of RTT difference should hence include routing information, especially in anycast scenarios. Furthermore, qualitative investigations of, e.g., address family specific and generally transit-free ASes on routing in regions, (remote) peering via IXes, the way operators import routes from them, and intra AS anycast routing are necessary.
Variability of the Root Server System: We find that similar anycast deployments may differ in terms of site stability, route inflation, and performance, i.e., a subset of root servers does not generalize to the RSS or even anycast in general, see also Koch et al. [20]. Hence, future work must even more critically assess how their (sub)set of root servers or VPs may impacts results.
(Hardware) Reliability and ZONEMD: We find a smooth roll-out of ZONEMD, finding individual cases of bitflips and stale zones in the process. Especially bitflips (see Section 6) open interesting opportunities, i.e., pending methodological and ethical questions, it may be possible to measure memory errors via the network.
Limitations: See Appendix E for a list of accepted limitations.
Artifact and Data Availability: The *NLNOG-DNS-1* measurement code is in Appendix F and links to the data in Appendix A.

Acknowledgments

We would like to thank all NLNOG RING operators for building and maintaining the infrastructure for our measurement. We would also like to thank our anonymous reviewers and shepherd for their valuable comments and suggestions to improve our paper.

References

[1] M. Allman. "On Eliminating Root Nameservers from the DNS". In: *Proceedings of the 18th ACM Workshop on Hot Topics in Networks*. 2019.

[2] H. Ballani and P. Francis. "Towards a global IP anycast service". In: *ACM SIGCOMM Computer Communication Review* 35.4 (Aug. 2005).

[3] H. Ballani, P. Francis, and S. Ratnasamy. "A measurement-based deployment proposal for IP anycast". In: *Proceedings of the 6th ACM SIGCOMM conference on Internet measurement*. 2006.

[4] P. Barber, M. Larson, M. Kosters, and P. Toscano. *Life and Times of J-ROOT*. Oct. 2004. URL: https://archive.nanog.org/meetings/nanog32/presentations/kosters.pdf.

[5] N. Brownlee, K. Claffy, and E. Nemeth. "DNS Measurements at a Root Server". In: *GLOBECOM'01. IEEE Global Telecommunications Conference*. 2001.

[6] R. Bush, D. Karrenberg, M. Kosters, and R. Plzak. *Root Name Server Operational Requirements*. RFC 2870. IETF, June 2000. URL: http://tools.ietf.org/rfc/rfc2870.txt.

[7] S. Castro, D. Wessels, M. Fomenkov, and K. Claffy. "A Day at the Root of the Internet". In: *ACM SIGCOMM Computer Communication Review* 38.5 (Sept. 2008).

[8] J. Chen, R. Pan, C. Ma, and Z. Li. "QoS Assessment of Root DNS Servers Based on Fuzzy Comprehensive Evaluation". In: *2023 IEEE 13th International Conference on Electronics Information and Emergency Communication (ICEIEC)*. 2023.

[9] Q. A. Chen, E. Osterweil, M. Thomas, and Z. M. Mao. "MitM Attack by Name Collision: Cause Analysis and Vulnerability Assessment in the New gTLD Era". In: *2016 IEEE Symposium on Security and Privacy (SP)*. 2016.

[10] L. Colitti, E. Romijn, H. Uijterwaal, and A. Robachevsky. "Evaluating the effects of anycast on DNS root name servers". In: *RIPE* (Oct. 2006).

[11] DNS-OARC. *Day In The Life of the Internet*. URL: https://www.dns-oarc.net/index.php/oarc/data/ditl.

[12] K. Fujiwara, S. Sannomiya, A. Sato, and K. Yoshida. "Latency analysis of JP and Root DNS servers from packet capture data". In: *2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC)*. 2023.

[13] H. Gao, V. Yegneswaran, Y. Chen, P. Porras, S. Ghosh, J. Jiang, and H. Duan. "An Empirical Reexamination of Global DNS Behavior". In: *Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM*. 2013.

[14] J. Heidemann, G. C. Moura, and W. Hardaker. "Do You Really Like Me? Anycast Latency and Root DNS Popularity". In: *DINR, Workshop on DNS and Internet Naming Research Directions* (Nov. 2021).

[15] P. Hoffman and K. Fujiwara. *DNS Terminology*. RFC 9499. IETF, Mar. 2024. URL: http://tools.ietf.org/rfc/rfc9499.txt.

[16] ICANN Root Server System Advisory Committee. *A Proposed Governance Model for the DNS Root Server System*. Tech. rep. RSSAC037. June 2018. URL: https://www.icann.org/en/system/files/files/rssac-037-15jun18-en.pdf.

[17] Internet Assigned Numbers Authority. *iana Root Files*. 2023. URL: https://www.iana.org/domains/root/files.

[18] B. Jones, N. Feamster, V. Paxson, N. Weaver, and M. Allman. "Detecting DNS Root Manipulation". In: *Passive and Active Measurement*. 2016.

[19] P. Koch, M. Larson, and P. Hoffman. *Initializing a DNS Resolver with Priming Queries*. RFC 8109. IETF, Mar. 2017. URL: http://tools.ietf.org/rfc/rfc8109.txt.

[20] T. Koch, E. Katz-Basset, J. Heidemann, M. Calder, C. Ardi, and L. Ke. "Anycast in Context: A Tale of Two Systems". In: *Proceedings of the 2021 ACM SIGCOMM 2021 Conference*. 2021.

[21] W. Kumari and P. Hoffman. *Decreasing Access Time to Root Servers by Running One on Loopback*. RFC 7706. IETF, Nov. 2015. URL: http://tools.ietf.org/rfc/rfc7706.txt.

[22] W. Kumari and P. Hoffman. *Running a Root Server Local to a Resolver*. RFC 8806. IETF, June 2020. URL: http://tools.ietf.org/rfc/rfc8806.txt.

[23] B.-S. Lee, Y. S. Tan, Y. Sekiya, A. Narishige, and S. Date. "Availability and effectiveness of root DNS servers: A long term study". In: *2010 IEEE Network Operations and Management Symposium - NOMS 2010*. 2010.

[24] M. Lentz, D. Levin, J. Castonguay, N. Spring, and B. Bhattacharjee. "D-mystifying the D-root address change". In: *Proceedings of the 2013 conference on Internet measurement conference*. 2013.

[25] C. Li, J. Chen, Z. Zhang, Y. Cheng, Z. Li, and Z. Li. "Evaluating the Quality of Service of the DNS Root Server From the Service Scope". In: *2023 International Conference on Mobile Internet, Cloud Computing and Information Security (MICCIS)*. 2023.

[26] Z. Li, D. Levin, N. Spring, and B. Bhattacharjee. "Internet anycast: performance, problems, & potential". In: *Proceedings of the 2018 Conference of the ACM Special Interest Group on Data Communication*. 2018.

[27] Z. Li, C. Li, G. Sun, Z. Zhang, Y. Cheng, and M. Weng. "Research on Optimal Selection Measurement of DNS Root Instance". In: *IEEE Access* 11 (2023).

[28] J. Liang, J. Jiang, H. Duan, K. Li, and J. Wu. "Measuring Query Latency of Top Level DNS Servers". In: *Passive and Active Measurement*. 2013.

[29] F. Lichtblau, F. Streibelt, T. Krüger, P. Richter, and A. Feldmann. "Detection, classification, and analysis of inter-domain traffic with spoofed source IP addresses". In: *Proceedings of the 2017 Internet Measurement Conference*. 2017.

[30] R. Liston, S. Srinivasan, and E. Zegura. "Diversity in DNS Performance Measures". In: *Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment*. 2002.

[31] Z. Liu, B. Huffaker, M. Fomenkov, N. Brownlee, and K. Claffy. "Two Days in the Life of the DNS Anycast Root Servers". In: *Passive and Active Network Measurement*. 2007.

[32] B. Manning. *Persistent Queries and Phantom Nameservers*. Nov. 2006. URL: https://www.caida.org/workshops/wide/0611/slides/manning-wide0611.pdf.

[33] G. Moura, W. Hardaker, J. Heidemann, and M. Davids. *Considerations for Large Authoritative DNS Server Operators*. RFC 9199. IETF, Mar. 2022. URL: http://tools.ietf.org/rfc/rfc9199.txt.

[34] M. Müller, M. Thomas, D. Wessels, W. Hardaker, T. Chung, W. Toorop, and R. v. Rijswijk-Deij. "Roll, Roll, Roll your Root: A Comprehensive Analysis of the First Ever DNSSEC Root KSK Rollover". In: *Proceedings of the Internet Measurement Conference*. 2019.

[35] N. Nikiforakis, S. Van Acker, W. Meert, L. Desmet, F. Piessens, and W. Joosen. "Bitsquatting: exploiting bit-flips for fun, or profit?" In: *Proceedings of the 22nd International Conference on World Wide Web*. 2013.

[36] NLnetLabs. *ldnsutils*. URL: https://packages.debian.org/ldnsutils.

[37] NLNOG RING. *NLNOG Ring*. URL: https://ring.nlnog.net/introduction/.

[38] R. de Oliveira Schmidt, J. Heidemann, and J. H. Kuipers. "Anycast Latency: How Many Sites Are Enough?" In: *Passive and Active Measurement*. 2017.

[39] R. S. Operators. *Statement on ZONEMD*. Aug. 2022. URL: https://root-servers.org/media/news/2022-08-Statement_on_ZONEMD.pdf.

[40] *Root Server Technical Operations Association*. URL: https://root-servers.org/.

[41] S. Sarat, V. Pappas, and A. Terzis. "On the use of anycast in DNS". In: *ACM SIGMETRICS Performance Evaluation Review* 33.1 (June 2005).

[42] D. Wessels, P. Barber, M. Weinberg, W. Kumari, and W. Hardaker. *Message Digest for DNS Zones*. RFC 8976. IETF, Feb. 2021. URL: http://tools.ietf.org/rfc/rfc8976.txt.

[43] D. Wessels. *Adding ZONEMD Protections to the Root Zone*. Apr. 2023. URL: https://blog.verisign.com/security/root-zone-zonemd/.

[44] D. Wessels, J. Castonguay, and P. Barber. "Thirteen Years of "Old J-Root"". In: *DNS-OARC Fall 2015 Workshop, Montreal* (Oct. 2015).

[45] F. Zhang, C. Lu, B. Liu, H. Duan, and Y. Liu. "Measuring the Practical Effect of DNS Root Server Instances: A China-Wide Case Study". In: *Passive and Active Measurement*. 2022.

	Africa	Asia	Europe	N. America	S. America	Oceania
#Vantage Points	10	52	435	133	13	32
Unique Countries	4	19	29	3	3	4
Unique Networks	9	31	386	94	12	22

Table 3: Distribution of vantage points per region.

A Dataset Availability

Our active measurement dataset is available at https://edmond.mpg.de/dataset.xhtml?persistentId=doi:10.17617/3.1OAUEP.

B Ethics

For collecting our *NLNOG-DNS-1* dataset, we send out 47 queries to each root-server IP in each measurement interval (15, resp. 30 minutes). While this amounts to a total of 888,300 queries per measurement, we do *not* parallelize the queries at each vantage point, so that at most 675 queries are inflight globally. Given the enormous scale of the root server system (serving over 50,000,000,000 queries daily), our measurement should not account for more than 0.1%. Furthermore, we provide information about us and how to contact us in the deployed scripts, see Appendix F, in addition to using an NLNOG RING account registered to us.

Additionally, we also monitored the NLNOG RING mailing-list. There, one operator sought contact, not to stop the measurements, but out of curiosity, and to learn more about what we were doing.

For our *ISP-DNS-1* and *IXP-DNS-1* datasets, all data processing occurs on-premises at the data collection infrastructure. In order to avoid exposing personally identifiable information, all IPs are normalized to their covering prefix, i.e., /24 for IPv4 and /48 for IPv6. For both data providers, the use of aggregate data for research and development activities is covered by their TOS. The data consists of highly sampled packet header data that is aggregated to flows.

C Coverage

For analyzing the coverage of our dataset (see Section 4), we match the node names, i.e., answers to `hostname.bind` and `id.server` to the corresponding root site as reported by `root-servers.org` [40]. Table 4 contains the distinct sites observed during our measurement per region, whereas Figure 11 contains the corresponding locations on a map. Sites that we have observed are marked as blue, whereas unobserved sites are marked as red. Note that `{a,c,j,e}.root` report no identifiers that are mappable to the sites, so we refer to using the IATA airport codes in the nodes' hostnames. This implies that we cannot distinguish multiple nodes (i.e. local and global)

For the distribution of our VPs per region, we refer to Table 3.

D Traffic to all roots

ISP-DNS-1: Figure 12 shows the traffic share of all root servers for the selected time intervals in the ISP network. `b.root` has a traffic share of 4.90% before the change and 4.46% after the change. In comparison to other root servers, we find that `b.root`'s total traffic share hardly changes despite the address change. `a.root` sees a traffic dip on 2024-02-26, which should be investigated in future work.
IXP-DNS-1: Looking at the traffic shares of the root servers at all 14 IXPs, see Figure 13, we find that traffic is dominated by few root servers, especially `k.root` and `d.root`.

E Limitations

Like all empirical work, our measurements of the root server system have limitations, and there is always room for improvement. Here, we verbosely discuss accepted limitations to aid the reader in contextualizing our results for specific findings.

While these limitations may appear extensive, we simply decided to explicitly spell out common assumptions, scope decisions, and practical requirements in network measurements for our work. We believe that this practice greatly improves the interpretability of studies and contributes positively to the scientific community.

Not using RIPE Atlas: One of the standard measurement platforms for distributed active measurements is RIPE Atlas, see also Section 3. It provides over 20,000 vantage points around the globe and already includes several build-in measurements related to the root server system. Using RIPE Atlas for our measurements could increase our coverage.

However, given the scale of RIPE Atlas, and to remain conservative in its storage requirements, the build in tests do not include, e.g., full AXFRs from all root servers, and queries for the root's IP addresses (A/AAAA). Similarly, no detailed distinction between the old and new IPs for `b.root` are implemented. Instead, only queries with different frequencies for SOA (1800s), version.bind (43200s), hostname.bind (240s), id.server (1800s), and version.server (43200s) are executed, see https://atlas.ripe.net/docs/built-in-measurements/. Furthermore, it is not clear whether local middle boxes interfere with DNS measurements, especially given the high prevalence of end-user ISP located probes.

Nevertheless, it would have been possible to add the measurements necessary for our work to RIPE Atlas. We reached out to the RIPE Atlas team prior to our study. However, in the discussion, it became clear that the additional load put on storage and compute for RIPE Atlas due to these additions would not be feasible.

For reference, our current active measurement dataset includes 7.7B DNS queries, 78M zone transfers, and 169M traceroutes. Using a custom dictionary-based compression approach leveraging deduplication in conjunction with ZSTD, we can reduce this dataset to roughly 0.5TB of data with a compression ratio of over 99.5% for eventual sharing with other researchers and the community. Given that the RIPE Atlas backend uses a Hadoop cluster with limited deduplication, this amount of additional data would not have been feasible to add on top of the existing data flows.

Low Number of VPs in Specific Regions: Several regions, most notably Africa and South America, are heavily underrepresented in the *NLNOG-DNS-1* dataset, see also Table 3, while Europe and North America are overrepresented.

This may induce artifacts in our results. For example, our observations on the comparatively discrete distribution of RTTs in Africa and South America seen in Section 6 may be related to the low number of vantage points in those regions. As such, especially the observed RTT shifts per address family and based on specific paths may not be representative for the region as a whole. Similarly, the observed effects in relation to specific selected paths, e.g., via AS6939 or AS12956, may be related to routing policy interactions between these specific ASes and the ASes in which our vantage points are located. However, given that we found a comparable effect in a region with more vantage points, i.e., North America, we are confident that this effect is robust. Nevertheless, further work

	Root		a	b	c	d	e	f	g	h	i	j	k	l	m
Worldwide	Global Sites	#	33	6	12	23	97	129	6	12	81	61	105	132	7
		# Covered	30	6	12	23	70	96	6	12	61	47	74	82	7
		% Covered	90.9	100.0	100.0	100.0	72.2	74.4	100.0	100.0	75.3	77.0	70.4	62.1	100.0
	Local Sites	#	23	0	0	186	147	216	0	0	0	85	11	0	9
		# Covered	20	0	0	78	44	60	0	0	0	64	4	0	7
		% Covered	87.0	-	-	41.9	29.9	27.8	-	-	-	75.3	36.4	-	77.8
	Total Sites	#	56	6	12	209	244	345	6	12	81	146	116	132	16
		# Covered	50	6	12	101	114	156	6	12	61	111	78	82	14
		% Covered	89.3	100.0	100.0	48.3	46.7	45.2	100.0	100.0	75.3	76.0	67.2	62.1	87.5
Africa	Global Sites	#	0	0	0	0	0	3	0	1	3	0	2	11	0
		# Covered	0	0	0	0	0	3	0	1	2	0	2	7	0
		% Covered	-	-	-	-	-	100.0	-	100.0	66.7	-	100.0	63.6	-
	Local Sites	#	0	0	0	42	43	25	0	0	0	8	0	0	0
		# Covered	0	0	0	7	6	1	0	0	0	4	0	0	0
		% Covered	-	-	-	16.7	14.0	4.0	-	-	-	50.0	-	-	-
	Total Sites	#	0	0	0	42	43	28	0	1	3	8	2	11	0
		# Covered	0	0	0	7	6	4	0	1	2	4	2	7	0
		% Covered	-	-	-	16.7	14.0	14.29	-	100.0	66.7	50.0	100.0	63.7	-
Asia	Global Sites	#	6	1	2	2	8	13	1	3	24	16	34	25	5
		# Covered	5	1	2	2	6	9	1	3	15	13	16	10	5
		% Covered	83.3	100.0	100.0	100.0	75.0	69.2	100.0	100.0	62.5	81.3	47.1	40.0	100.0
	Local Sites	#	2	0	0	39	34	84	0	0	0	11	9	0	7
		# Covered	2	0	0	15	14	20	0	0	0	6	3	0	5
		% Covered	100.0	-	-	38.5	41.2	23.8	-	-	-	54.5	33.3	-	71.4
	Total Sites	#	8	1	2	41	42	97	1	3	24	27	43	25	12
		# Covered	7	1	2	17	20	29	1	3	15	19	19	10	10
		% Covered	87.5	100.0	100.0	41.5	47.6	29.9	100.0	100.0	62.5	70.4	44.2	40.0	83.3
Europe	Global Sites	#	12	1	4	9	33	46	2	2	25	18	44	33	1
		# Covered	12	1	4	9	28	42	2	2	22	17	37	31	1
		% Covered	100.0	100.0	100.0	100.0	84.8	91.3	100.0	100.0	88.0	94.4	84.1	93.9	100.0
	Local Sites	#	7	0	0	39	22	26	0	0	0	34	2	0	0
		# Covered	7	0	0	30	14	17	0	0	0	29	1	0	0
		% Covered	100.0	-	-	76.9	63.6	65.4	-	-	-	85.3	50.0	-	-
	Total Sites	#	19	1	4	48	55	72	2	2	25	52	46	33	1
		# Covered	19	1	4	39	42	59	2	2	22	46	38	31	1
		% Covered	100.0	100.0	100.0	81.3	76.4	81.9	100.0	100.0	88.0	88.5	82.6	93.9	100.0
North America	Global Sites	#	13	3	5	12	45	54	3	4	16	20	17	22	1
		# Covered	13	3	5	12	26	33	3	4	14	14	12	16	1
		% Covered	100.0	100.0	100.0	100.0	57.8	61.1	100.0	100.0	87.5	70.0	70.6	72.7	100.0
	Local Sites	#	14	0	0	49	30	34	0	0	0	24	0	0	0
		# Covered	11	0	0	19	7	11	0	0	0	19	0	0	0
		% Covered	78.6	-	-	38.8	23.3	32.4	-	-	-	79.2	-	-	-
	Total Sites	#	27	3	5	61	75	88	3	4	16	44	17	22	1
		# Covered	24	3	5	31	33	44	3	4	14	33	12	16	1
		% Covered	88.9	100.0	100.0	50.8	44.0	50.0	100.0	100.0	87.5	75.0	70.6	72.7	100.0
South America	Global Sites	#	0	1	1	0	5	4	0	1	10	4	6	23	0
		# Covered	0	1	1	0	4	2	0	1	6	0	5	10	0
		% Covered	-	100.0	100.0	-	80.0	50.0	-	100.0	60.0	0.0	83.3	43.5	-
	Local Sites	#	0	0	0	12	13	40	0	0	0	6	0	0	0
		# Covered	0	0	0	3	2	7	0	0	0	4	0	0	0
		% Covered	-	-	-	25.0	15.4	17.5	-	-	-	66.7	-	-	-
	Total Sites	#	0	1	1	12	18	44	0	1	10	10	6	23	0
		# Covered	0	1	1	3	6	9	0	1	6	4	5	10	0
		% Covered	-	100.0	100.0	25.0	33.3	20.5	-	100.0	60.0	40.0	83.3	43.5	-
Oceania	Global Sites	#	0	0	0	0	6	9	0	1	3	3	2	18	0
		# Covered	0	0	0	0	6	7	0	1	2	3	2	8	0
		% Covered	-	-	-	-	100.0	77.8	-	100.0	66.7	100.0	100.0	44.4	-
	Local Sites	#	0	0	0	4	4	7	0	0	0	2	0	0	2
		# Covered	0	0	0	4	1	4	0	0	0	2	0	0	2
		% Covered	-	-	-	100.0	25.0	57.1	-	-	-	100.0	-	-	100.0
	Total Sites	#	0	0	0	0	10	16	0	1	3	5	2	18	2
		# Covered	0	0	0	0	7	11	0	1	2	5	2	8	2
		% Covered	-	-	-	100.0	70.0	68.8	-	100.0	66.7	100.0	100.0	44.4	100.0

Table 4: Coverage of root sites per region.

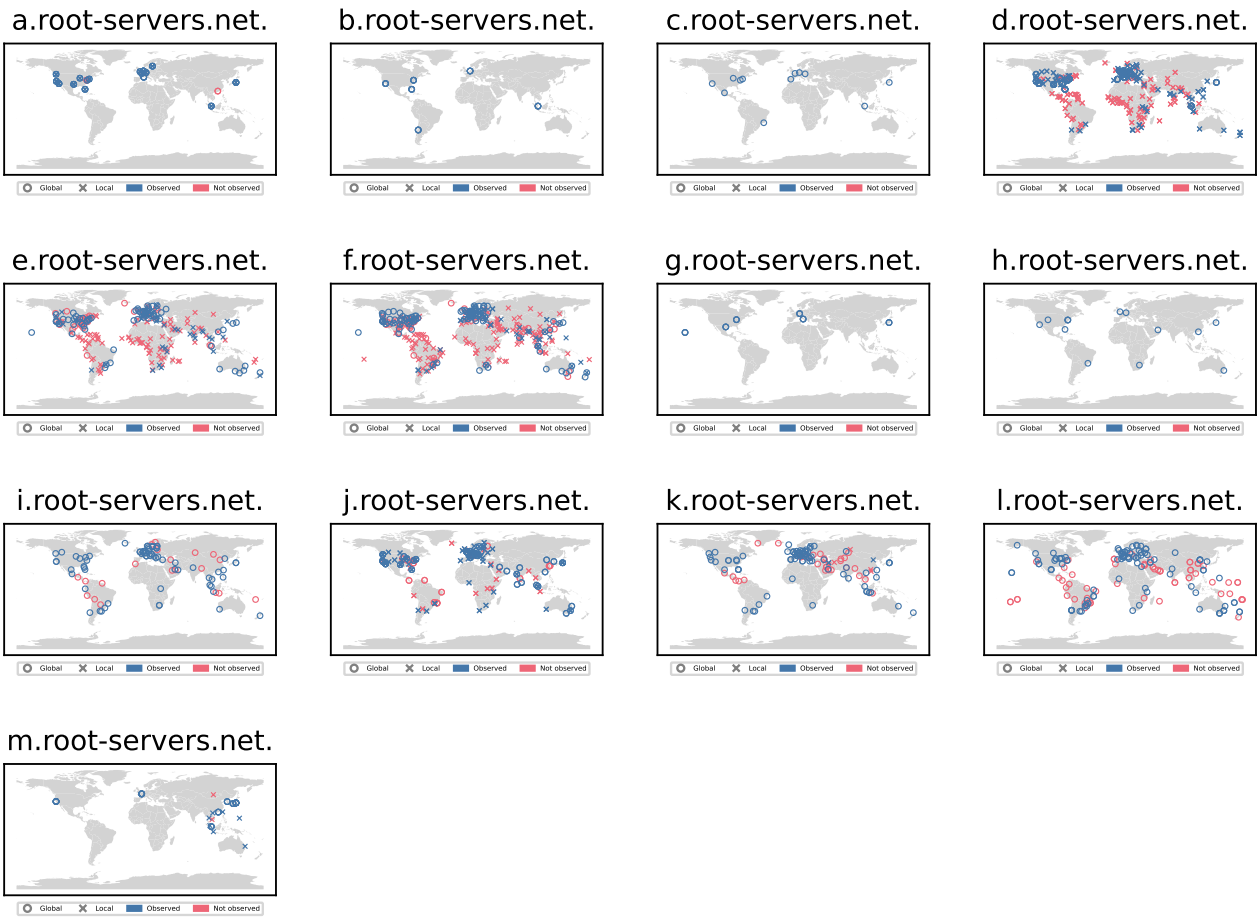


Figure 11: Coverage of root server locations

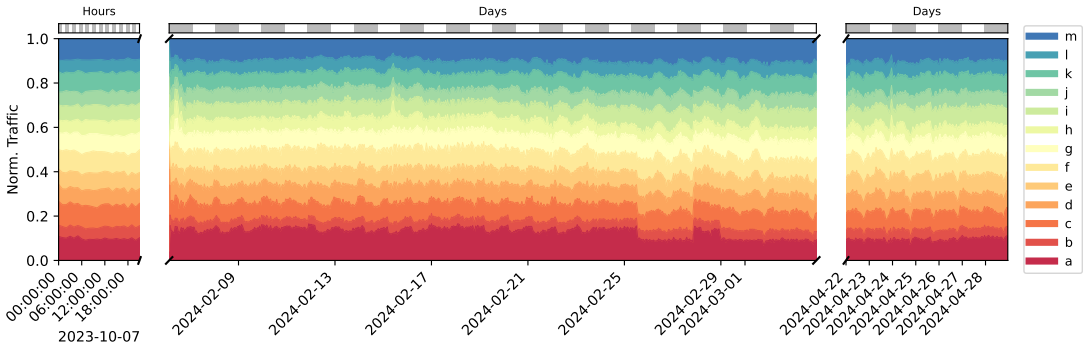


Figure 12: ISP: Traffic to all roots.

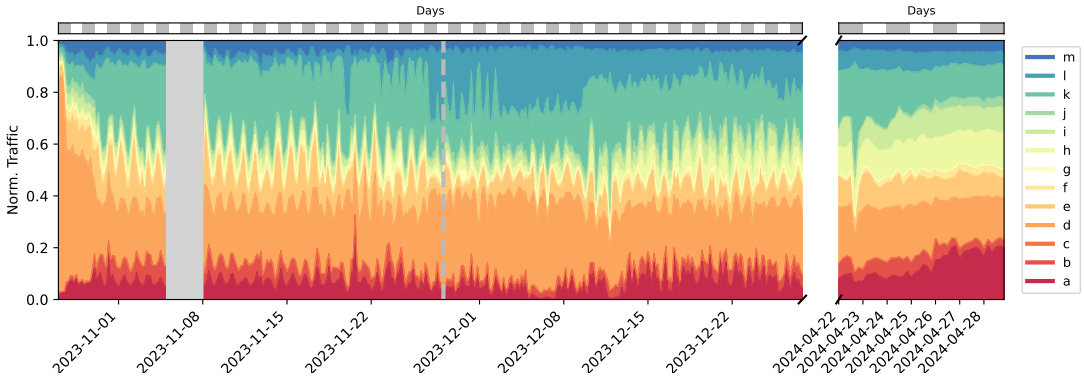


Figure 13: IXP: Traffic to all roots.

will be necessary to better understand the role of specific neighbor relationships on the observed RTTs of anycast setups.

Absence of a Control Group: Our measurements target the root server system. As noted in Section 3, earlier work noted that the root server system may not be fully representative of anycast setups. This also aligns with our findings.

Hence, the reliability of our method would have been increased by introducing an additional control group, i.e., adding an additional anycast setup under our control to the measurements. However, to limit the scope of this paper, this was not done.

Missing Evaluation of Control Plane Data (BGP): The measurements only collected unidirectional control plane data (traceroutes). However, in addition to that, control plane data, i.e., information on the selected routes in BGP could have been collected for each vantage point for the root server prefixes. Furthermore, return-path data, i.e., visibility of the vantage point's prefixes from the anycast locations should have been included.

Given the complexity of collecting this data, requiring coordination with all root server operators (to receive routes of the VP locations) as well as all NLNOG RING node contributors, this was not done. We argue that the collected traceroutes provide a sufficient perspective for the observations we make.

Nevertheless, observations in Section 6 on the impact of individual paths could be sharpened using this data. We hence recommend revisiting such a more extensive research design in future work, especially to better study path selection in less interconnected and vantage point heavy regions, as well as the impact of IXPs on RTT due to imported routes from (remote) peers.

Limited Temporal Resolution: Our *NLNOG-DNS-1* measurements run every 30 minutes, with an increased resolution of every 15 minutes during expected change periods. While this provides an actionable trade-off between frequency, insight, and load on the NLNOG RING and root server system, see Appendix B, it also limits the insight into change events. Especially the synchronization behavior of root servers cannot be captured with this resolution.

There, it would be preferable to issue higher frequency measurements, ideally up to a per-second resolution. To lessen load on VPs and root servers, this should be limited to, e.g., SOA records.

Nevertheless, as the exact timings of synchronization below average DNS zone TTLs was not the core objective of our work, we accepted this trade off. Future work should consider such a measurement setup, or the use of passive traces from root servers to investigate this specific issue.

Limited Exploration of Individual Effects: Individual effects in the dataset are not explored to their maximum depth. For example, see the investigation of the routing impact of individual ASes.

This limitation is rooted in scope choices related to data collection, see above, as well as in the objective to focus on overarching effects. Nevertheless, we acknowledge that the deeper exploration of individual effects might produce interesting and relevant results. Hence, we recommend it to be the subject of future work.

Use of Proprietary Datasets: Being committed to open science, we share the full artifact used for collecting the *NLNOG-DNS-1*, along with the compressed raw data with the community for future work, analysis, and validation of our results. However, we also leverage proprietary *ISP-DNS-1* and *IXP-DNS-1* to attain additional perspectives within the scope of our work.

Due to privacy concerns, see Section B, this data cannot be freely shared, potentially impacting reproducibility. However, access to comparable datasets is available to various groups in the community, still allowing for independent reproduction. Furthermore, aforementioned privacy requirements mean that our perspective is, e.g., limited to *relative* traffic shares. While, naturally, exact numbers would provide a more complete picture, the reported aggregates are still sufficient for the research questions at hand.

F Active Measurement Script

You can find the measurement script which we used on the NLNOG Ring nodes below. Even though we took utmost care to ensure that it can be copy-pasted and run, you may have to apply some manual adjustments, mostly related to missing or misplaced ` and #.

Furthermore, the script currently assumes GNU date and hostname utilities, i.e., needs adjustments to work under UNIX.

```
#!/bin/bash
# DESCRIPTION:
#
# This script collects data on the (locally reachable) anycast nodes of the root servers.
# It is executed every 30 minutes.
#
# The purpose of this measurement is tracking the IP address changeover of b.root expected
# in Q4/2023.
#
# In case of issues, please contact noc@as59645.net / +49 5424 2 119 722
#
# This script is licensed under a 3c BSDL; If you can read this, you may use it.
#
# Copyright (c) 2023 Tobias Fiebig <contact@as59645.net>. All rights reserved.
#
# Redistribution and use in source and binary forms, with or without modification, are
# permitted provided that the following conditions are met:
```

```
#
# 1. Redistributions of source code must retain the above copyright notice, this list of
#    conditions and the following disclaimer.
# 2. Redistributions in binary form must reproduce the above copyright notice, this list
#    of conditions and the following disclaimer in the documentation and/or other
#    materials provided with the distribution.
# 3. Neither the name of the copyright holder nor the names of its contributors may be used to
#    endorse or promote products derived from this software without specific prior
#    written permission.
#
# THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY
# EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
# MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL
# THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
# SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT
# OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
# INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
# LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE
# OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
set -u
DATE=`date --iso-8601=seconds`
DAY=`date --iso-8601`

RSERVERS="
a.root-servers.net.
b.root-servers.net.
c.root-servers.net.
d.root-servers.net.
e.root-servers.net.
f.root-servers.net.
g.root-servers.net.
h.root-servers.net.
i.root-servers.net.
j.root-servers.net.
k.root-servers.net.
l.root-servers.net.
m.root-servers.net.
"

RSERVERSv4="
198.41.0.4
199.9.14.201
170.247.170.2
192.33.4.12
199.7.91.13
192.203.230.10
192.5.5.241
192.112.36.4
198.97.190.53
192.36.148.17
192.58.128.30
193.0.14.129
199.7.83.42
202.12.27.33
"

RSERVERSv6="
2001:503:ba3e::2:30
2001:500:200::b
2801:1b8:10::b
2001:500:2::c
2001:500:2d::d
2001:500:a8::e
2001:500:2f::f
2001:500:12::d0d
2001:500:1::53
2001:7fe::53
2001:503:c27::2:30
2001:7fd::1
2001:500:9f::42
2001:dc3::35
"

mkdir -p ./data/$DATE/
echo "Starting at: `date --iso-8601=seconds`" > ./data/$DATE/run_log.log
echo "Cleaning old data: " >> ./data/$DATE/run_log.log
find ./data -type d -cmin +90 -exec rm -rvf {} \; >> ./data/$DATE/run_log.log

# For each rootserver;
# Get a/aaaa for each rootserver, ns ., chaos, traceroute
for rsv4 in $RSERVERSv4;
do
 echo "`date --iso-8601=seconds`: Garthering data for $rsv4" >> \
   ./data/$DATE/run_log.log
 mtr -c 1 -n -j $rsv4 > ./data/$DATE/$rsv4-mtr-pre.json 2>&1 &
 dig @$rsv4 +retry=0 +timeout=1 AXFR . > ./data/$DATE/$rsv4-root-AXFR.dig 2>&1
 dig @$rsv4 +retry=0 +timeout=1 +dnssec ZONEMD . > \
   ./data/$DATE/$rsv4-root-ZONEMD.dig 2>&1
 dig @$rsv4 +retry=0 +timeout=1 +dnssec NS . > \
   ./data/$DATE/$rsv4-root-NS.dig 2>&1
 dig @$rsv4 +retry=0 +timeout=1 +dnssec NS root-servers.net > \
   ./data/$DATE/$rsv4-root-servers.net-NS.dig 2>&1
 dig @$rsv4 +retry=0 +timeout=1 CH TXT hostname.bind > \
   ./data/$DATE/$rsv4-CH-TXT-hostname.bind.dig 2>&1
 dig @$rsv4 +retry=0 +timeout=1 CH TXT id.server > \
   ./data/$DATE/$rsv4-CH-TXT-id.server.dig 2>&1
 dig @$rsv4 +retry=0 +timeout=1 CH TXT version.bind > \
   ./data/$DATE/$rsv4-CH-TXT-version.bind.dig 2>&1
 dig @$rsv4 +retry=0 +timeout=1 CH TXT version.server > \
   ./data/$DATE/$rsv4-CH-TXT-version.server.dig 2>&1
 for rsname in $RSERVERS;
 do
  echo "`date --iso-8601=seconds`: Garthering data for $rsv4, $rsname" >> \
    ./data/$DATE/run_log.log
  dig @$rsv4 +retry=0 +timeout=1 +dnssec A $rsname > \
    ./data/$DATE/$rsv4-$rsname-A.dig 2>&1
  dig @$rsv4 +retry=0 +timeout=1 +dnssec AAAA $rsname > \
    ./data/$DATE/$rsv4-$rsname-AAAA.dig 2>&1
  dig @$rsv4 +retry=0 +timeout=1 +dnssec TXT $rsname > \
    ./data/$DATE/$rsv4-$rsname-TXT.dig 2>&1
 done;
 echo "`date --iso-8601=seconds`: Finished garthering data for $rsv4" >> \
   ./data/$DATE/run_log.log
done;

for rsv6 in $RSERVERSv6;
do
 echo "`date --iso-8601=seconds`: Garthering data for $rsv6" >> \
   ./data/$DATE/run_log.log
 mtr -c 1 -n -j $rsv6 > ./data/$DATE/$rsv6-mtr-pre.json 2>&1 &
 dig @$rsv6 +retry=0 +timeout=1 AXFR . > ./data/$DATE/$rsv6-root-AXFR.dig 2>&1
 dig @$rsv6 +retry=0 +timeout=1 +dnssec ZONEMD . > \
   ./data/$DATE/$rsv6-root-ZONEMD.dig 2>&1
 dig @$rsv6 +retry=0 +timeout=1 +dnssec NS . > \
   ./data/$DATE/$rsv6-root-NS.dig 2>&1
 dig @$rsv6 +retry=0 +timeout=1 +dnssec NS root-servers.net > \
   ./data/$DATE/$rsv6-root-servers.net-NS.dig 2>&1
 dig @$rsv6 +retry=0 +timeout=1 CH TXT hostname.bind > \
   ./data/$DATE/$rsv6-CH-TXT-hostname.bind.dig 2>&1
 dig @$rsv6 +retry=0 +timeout=1 CH TXT id.server > \
   ./data/$DATE/$rsv6-CH-TXT-id.server.dig 2>&1
 dig @$rsv6 +retry=0 +timeout=1 CH TXT version.bind > \
   ./data/$DATE/$rsv6-CH-TXT-version.bind.dig 2>&1
 dig @$rsv6 +retry=0 +timeout=1 CH TXT version.server > \
   ./data/$DATE/$rsv6-CH-TXT-version.server.dig 2>&1
 for rsname in $RSERVERS;
 do
  echo "`date --iso-8601=seconds`: Garthering data for $rsv6, $rsname" >> \
    ./data/$DATE/run_log.log
  dig @$rsv6 +retry=0 +timeout=1 +dnssec A $rsname > \
    ./data/$DATE/$rsv6-$rsname-A.dig 2>&1
  dig @$rsv6 +retry=0 +timeout=1 +dnssec AAAA $rsname > \
    ./data/$DATE/$rsv6-$rsname-AAAA.dig 2>&1
  dig @$rsv6 +retry=0 +timeout=1 +dnssec TXT $rsname > \
    ./data/$DATE/$rsv6-$rsname-TXT.dig 2>&1
 done;
 echo "`date --iso-8601=seconds`: Finished garthering data for $rsv6" >> \
   ./data/$DATE/run_log.log
done;

echo "Finished run at: `date --iso-8601=seconds`" >> ./data/$DATE/run_log.log
sleep 3
mkdir -p ./data/archive/$DAY
tar cfz ./data/archive/$DAY/`hostname -f`-$DATE.tar.gz ./data/$DATE
rm -rf ./data/$DATE
```

G Geographical Differences in RTT

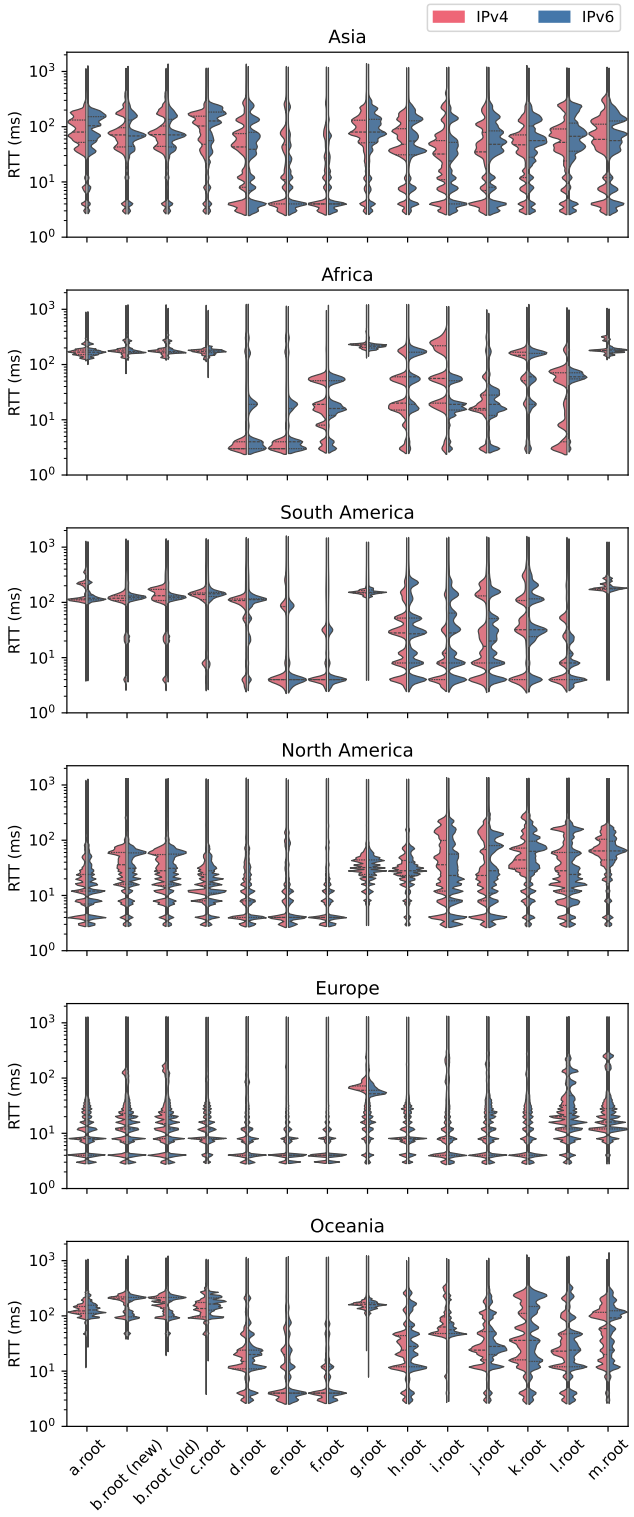


Figure 14: Violin plots of RTTs of requests by continent, address family, and root-server.

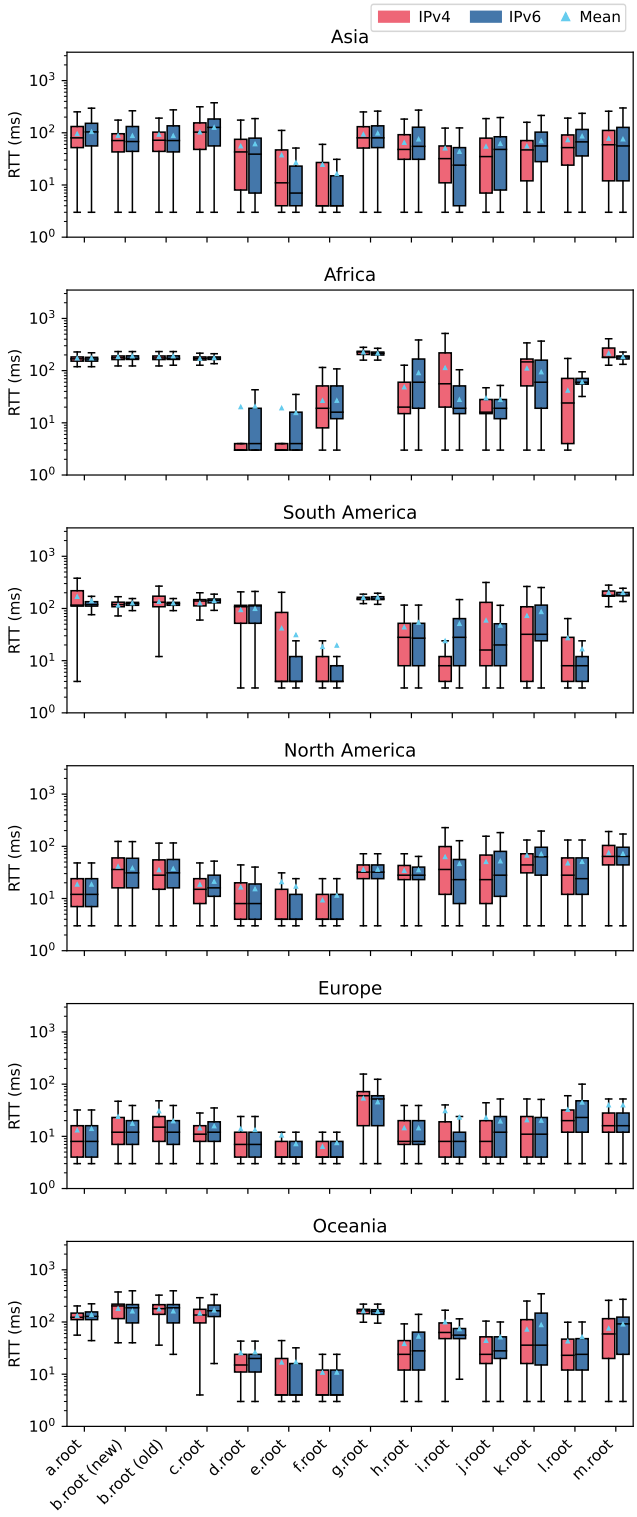


Figure 15: Boxplots of RTTs of requests by continent, address family, and root-server.