

Local root: the traffic trade-off between root queries & root zone distribution

Ilyas Rahimi
Willem Toorop

University of Amsterdam
NLnet Labs

Thursday, 29 October 2026 at the RIPE 93, Sofia, Bulgaria

Motivation

- **draft-wkumari-dnsop-localroot-bcp**
 - Populating resolvers with the root zone
 - for privacy, security and robustness benefits
- **How would it affect traffic when applied at scale?**
 - More or less traffic?
 - How much?

 UNIVERSITY OF AMSTERDAM

RESEARCH PROJECT TWO

Local Root Serving by Default: Quantifying the Traffic Trade-off Between Root Queries and Root Zone Distribution

[illegible]

January, 2026

Student:
Ilyas Rahimi
12330337

Supervisor:
dr. Marios Avgeris
Assistant Professor, University of
Amsterdam
m.avgeris@uva.nl

CoSupervisor:
Willem Toorop
Senior Research Engineer, NLnet Labs
willem@nlnetlabs.nl

Methodology

- **Two Perspectives:**
 - **Root-side:** RSSAC002 aggregate statistics.
 - **Resolver-side:** Direct measurement in a controlled testbed.
- **Unit of Measure:** Bytes per resolver per day.
- **Approach:** Derived baseline vs. measured reality.

Methodology – RSSAC002 & Baseline

- **RSSAC002:** Standard reporting framework for Root Servers.
- **Metric 1:** Total query/response counts.
- **Metric 2:** Packet size distributions (bucketed).
- **Metric 3:** Unique source IP counts.
- **Calculation:** $(\text{Total Bytes}) / (\text{Unique Source IPs}) = \text{Baseline traffic per resolver.}$

I. [RSSAC 002v5: Advisory on Measurements of the Root Server System](#)

Experimental Setup

- **Environment:** Proxmox virtualization platform.
- **Isolation:** Components communicated over a local virtual network.
- **Software:** Recent Linux distribution; open-source resolver software.
- **Observation:** 4 consecutive days of production root zone evolution.

Resolver Roles & Update Mechanisms

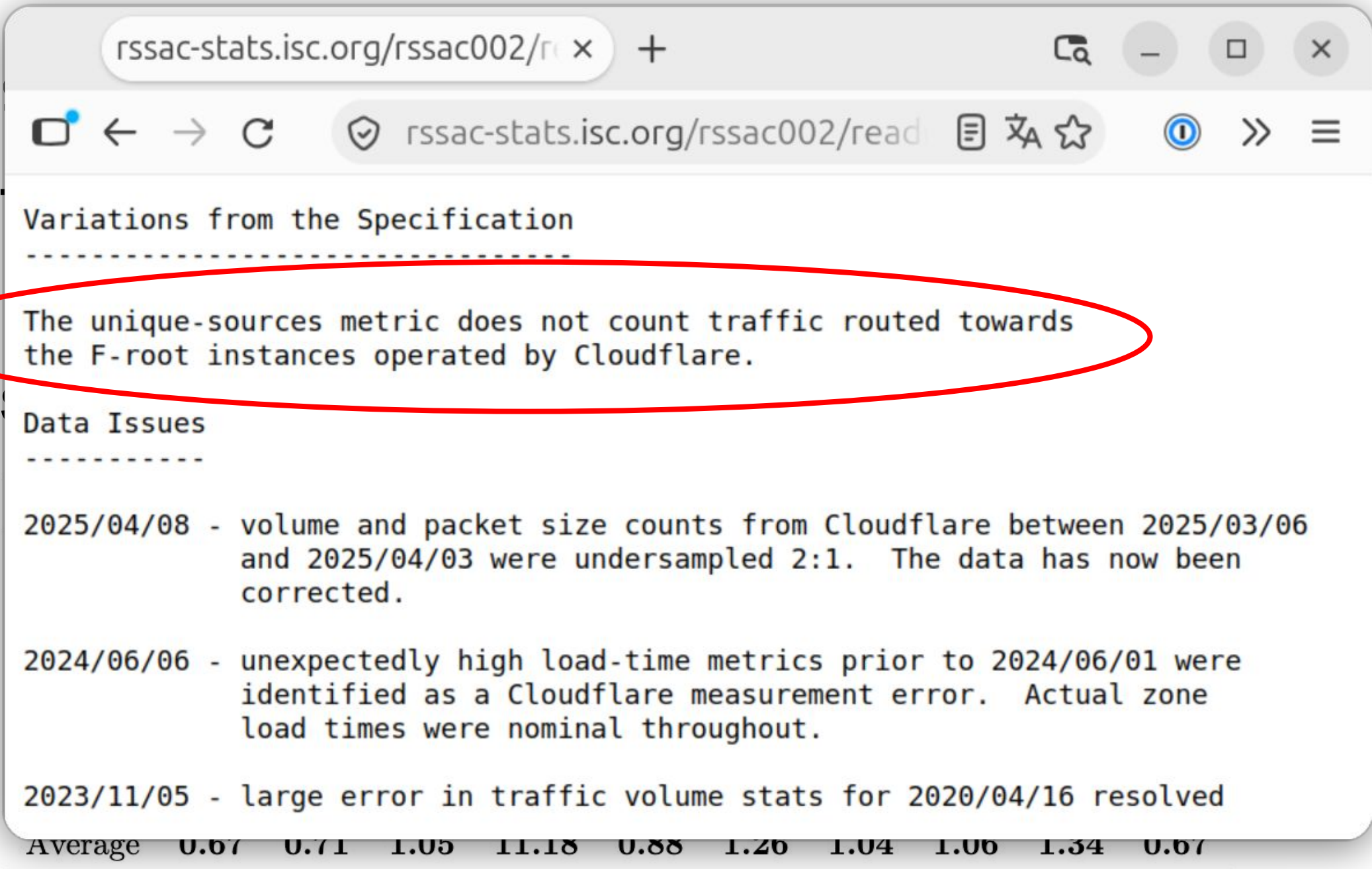
- **BIND:** DNS-based IXFR (Incremental transfers).
- **Unbound (Role A):** DNS-based IXFR.
- **Unbound (Role B):** HTTPS-based retrieval.
- **Knot Resolver:** Native HTTPS-based local root functionality.
- **Traffic Captured:** DNS/HTTPS payloads + TCP/TLS/Control overhead.

Results Conventional (Baseline) Traffic

- **Table 1 Summary:**
 - Most roots: **0.67 to 1.34 MB/day.**
 - F-root outlier: **11.18 MB/day.**
- **System-wide Average: Approximately 2 MB/day.**

Day	b	c	d	f	h	i	j	k	l	m
1	0.69	0.71	1.04	11.40	0.88	1.30	1.11	1.06	1.35	0.70
2	0.69	0.72	1.08	11.26	0.90	1.27	1.08	1.04	1.35	0.68
3	0.66	0.70	1.03	10.92	0.86	1.25	1.07	1.02	1.32	0.62
4	0.66	0.70	1.04	10.91	0.85	1.30	1.05	1.07	1.34	0.69
5	0.66	0.70	1.06	11.13	0.88	1.25	1.01	1.07	1.31	0.63
6	0.68	0.71	1.06	11.35	0.89	1.22	0.97	1.06	1.33	0.67
7	0.68	0.72	1.06	11.28	0.90	1.25	0.99	1.10	1.36	0.70
Average	0.67	0.71	1.05	11.18	0.88	1.26	1.04	1.06	1.34	0.67

Re



rssac-stats.isc.org/rssac002/read

- Variations from the Specification

The unique-sources metric does not count traffic routed towards the F-root instances operated by Cloudflare.
- Data Issues

2025/04/08 - volume and packet size counts from Cloudflare between 2025/03/06 and 2025/04/03 were undersampled 2:1. The data has now been corrected.

2024/06/06 - unexpectedly high load-time metrics prior to 2024/06/01 were identified as a Cloudflare measurement error. Actual zone load times were nominal throughout.

2023/11/05 - large error in traffic volume stats for 2020/04/16 resolved

Average	0.67	0.71	1.05	11.18	0.88	1.26	1.04	1.06	1.34	0.67
---------	------	------	------	-------	------	------	------	------	------	------

Results BIND (DNS-based IXFR)

- **Mechanism:** Triggered by SOA serial changes.
- **Data Size:** ~1.45 MB per incremental update.
- **Daily Average: 4.35 MB/day.**
- **Pattern:** Traffic scales with the number of updates (2–4 per day).

Date (2026)	Updates	MB per update	Total MB/day
Jan 20	2	1.45	2.90
Jan 21	3	1.45	4.35
Jan 22	4	1.45	5.80
Jan 23	3	1.45	4.35
Average	—	—	4.35

Results Unbound (DNS-based IXFR)

- **Mechanism:** Identical update logic to BIND.
- **Data Size:** ~1.31 MB per incremental update.
- **Daily Average:** **3.93 MB/day.**
- **Comparison:** Slightly smaller per-update transfer size than BIND.

Date (2026)	Updates	MB per update	Total MB/day
Jan 20	2	1.31	2.62
Jan 21	3	1.31	3.93
Jan 22	4	1.31	5.24
Jan 23	3	1.31	3.93
Average	—	—	3.93

Results Unbound (HTTPS-based)

- **Mechanism:** Polling every SOA refresh time (30 min.)
- **Data Size:** 2.19 MB per update (Full Zone in presentation format).
- **The Anomaly: 105.12 MB/day.**
- **Analysis:** 48 full downloads/day ([fixed with current Unbound](#))

Date (2026)	Updates/day	MB per update	Total MB/day
Jan 20	48	2.19	105.12
Jan 21	48	2.19	105.12
Jan 22	48	2.19	105.12
Jan 23	48	2.19	105.12
Average	—	—	105.12

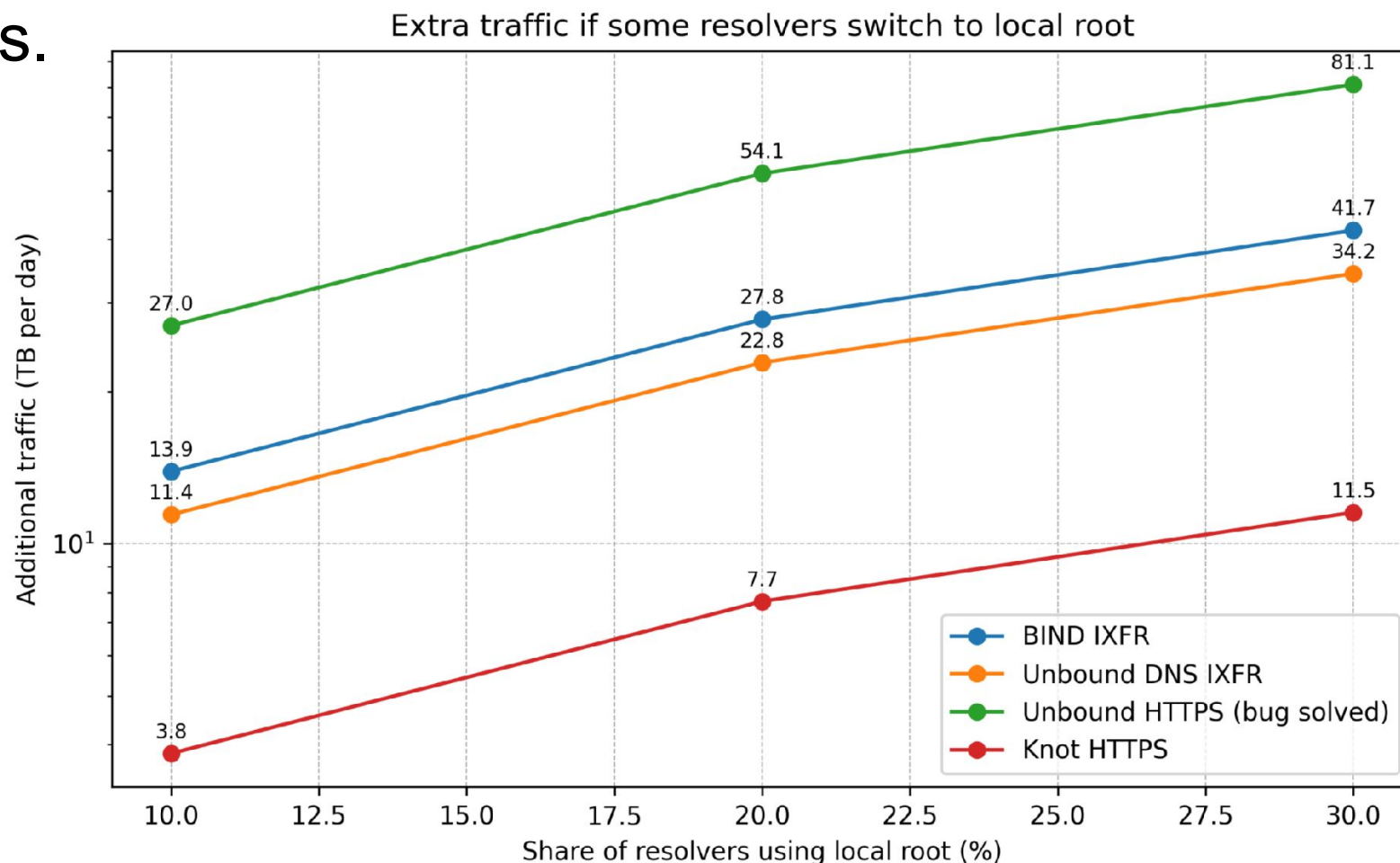
Results Knot Resolver (HTTPS-based)

- **Mechanism:** Cache fill
- **Frequency:** One full update per day (the lowest TTL in the root)
- **Daily Average: 2.65 MB/day.**
- **Finding:** Most efficient local root configuration evaluated.

Date (2026)	Time (CET)	Data transferred (MB)
Jan 20	12:06	2.69
Jan 21	12:06	2.61
Jan 22	12:06	2.67
Jan 23	12:06	2.65
Average	—	2.65

Results – Impact on overall traffic

- Global adoption levels (10%, 20%, 30%).
- ~59.1 million resolvers.
- Additional daily traffic in **Terabytes (TB)**.
- **Result (Knot 10%):**
 - +3.8 TB/day.
 - Twice current traffic



Discussion

- Currently the root is **fully** signed ~2.5 times a day
 - At 4am and 4pm UTC and when changes happen

	XFR size	Daily traffic	Factor
Baseline(without F)		0.96 MB	1
DNS XFR	1.31 MB	3.28 MB	3.4
HTTPS XFR	2.19 MB	105.12 MB	109.5
HTTPS XFR (bug fixed)	2.19 MB	5.48 MB	5.7
HTTPS cache pre-fill	2.19 MB	2.19 MB	2.3

Discussion

- Currently the root is **fully** signed ~2.5 times a day
 - At 4am and 4pm UTC and when changes happen
- Fully signed means full transfer always, because $2 * \text{sizeoff}(\text{all RRsigns}) > \text{sizeoff}(\text{whole zone})$
- **What if...** it would have been incrementally signed
 - Portion of (oldest) RRsigns is renewed twice a day
 - Only the changes resigned when changes happen

What if... the root is signed incrementally

- RRSIG lifetime must be longer than SOA expire
 - see [\[Section 4.3.4 of RFC 6781 \]](#)
- All RRSIGs have a 13 days and 1 hour lifetime
 - *except for the KSK RRSIG which lives for 21 days*

```
. 86400 IN SOA a.root-servers.net. nstld.verisign-grs.com. (  
    2026102300 ; serial  
    1800       ; refresh (30 minutes)  
    900        ; retry (15 minutes)  
    604800     ; expire (1 week)  
    86400      ; minimum (1 day)  
    )
```

- Fresh RRSIG at least every $13 - 7 = 6$ days

What if... the root is signed incrementally

- Resign 1/12th of the oldest RRSIGs twice a day
- Resign the changes when they happen
- <https://codeberg.org/wtoorop/incremental-root>
 - Shadow, incrementally signed, version of the root zone
 - All versions since 22nd of December 2025
 - IXFRs from version to version in presentation format with wire format size in comment

What if...

- Resign 1/12
- Resign the
- [https://code](https://codeberg.org/wtoorop/incremental-root)
 - Shadow, i
 - All version
 - IXFRs from
with wire f

The screenshot shows the Codeberg repository page for `wtoorop/incremental-root`. The repository is described as "An incrementally signed (IXFR friendly) version of the root zone, since Dec 21 21:29 UTC (SOA serial 2025122101)". It has 13 commits, 1 branch, 0 tags, and a size of 517 MiB. The commit history shows a recent commit by Willem Toorop updating incremental zones. The file list includes a `keys` directory and several zone files and IXFRs, such as `2025122101.zone`, `2025122200.zone`, `2025122200.zone.ixfr`, `2025122201.zone`, `2025122201.zone.ixfr`, `2025122202.zone`, `2025122202.zone.ixfr`, `2025122300.zone`, `2025122300.zone.ixfr`, `2025122301.zone`, `2025122301.zone.ixfr`, and `2025122400.zone`.

File	Description	Time
keys	updated incremental zones	22 minuten geleden
2025122101.zone	First batch of incrementally signed versions of the root	8 maanden geleden
2025122200.zone	First batch of incrementally signed versions of the root	8 maanden geleden
2025122200.zone.ixfr	Updated incremental transfers	7 maanden geleden
2025122201.zone	First batch of incrementally signed versions of the root	8 maanden geleden
2025122201.zone.ixfr	First batch of incrementally signed versions of the root	8 maanden geleden
2025122202.zone	First batch of incrementally signed versions of the root	8 maanden geleden
2025122202.zone.ixfr	First batch of incrementally signed versions of the root	8 maanden geleden
2025122300.zone	First batch of incrementally signed versions of the root	8 maanden geleden
2025122300.zone.ixfr	First batch of incrementally signed versions of the root	8 maanden geleden
2025122301.zone	First batch of incrementally signed versions of the root	8 maanden geleden
2025122301.zone.ixfr	First batch of incrementally signed versions of the root	8 maanden geleden
2025122400.zone	First batch of incrementally signed versions of the root	8 maanden geleden

Wh

- R
- R
- h

incremental-root/202610 x +

codeberg.org/wtoorop/incremental-root/src/commit/400a067081cd4d70369f96 130%

 Verkennen About FAQ Help

Donate

Registreren Aanmelden

 wtoorop / incremental-root

 Volgen 1  Ster 0  Afsplitsing 0

<> Code

Issues

Pull requests

Activiteit

400a067081

incremental-root / 2026102600.zone.ixfr

 Willem Toorop

400a067081 updated incremental zones

1 uur geleden

480 regels | 192 KiB | Text

Ruw Blame Geschiedenis

```
1 ; IXFR data file
2 ; zone .
3 ; from_serial 2026102501
4 ; to_serial 2026102600
5 ; data_size 137238
6 ; IXFR created by NSD 4.8.0 for . 2026102501 to 2026102600 of 137238 bytes at time Mon Oct 26 06:10:59 2026
7 . 86400 IN SOA a.root-servers.net. nstld.verisign-grs.com. 2026102600 1800 900 604800 86400
8 . 86400 IN SOA a.root-servers.net. nstld.verisign-grs.com. 2026102501 1800 900 604800 86400
9 . 86400 IN RRSIG SOA 8 0 86400 20261107170000 20261025160000 22735 . KaOklrCq+eISmgqCUEYeZHE9EQx3bEJY
LvWZUrma8zjh1LLai/6RhaZAYXOqGW9TT6++wtPQ8tMQd9zaqliXIqf5gz9ZFp7h2KMDmwGDE4HERwXYvrkX1TogLMIyjdDiADU9wOl/OawTx
```

Wh

-
-
-

```
willem@orangutan: ~/incremental-root
willem@orangutan:~/incremental-root$ grep '^; data_size ' *.ixfr
2025122200.zone.ixfr:; data_size 137274
2025122201.zone.ixfr:; data_size 137134
2025122202.zone.ixfr:; data_size 2027
2025122300.zone.ixfr:; data_size 137314
2025122301.zone.ixfr:; data_size 137256
2025122400.zone.ixfr:; data_size 137178
2025122401.zone.ixfr:; data_size 137040
2025122500.zone.ixfr:; data_size 136890
2025122501.zone.ixfr:; data_size 137226
2025122600.zone.ixfr:; data_size 137126
2025122601.zone.ixfr:; data_size 137106
2025122602.zone.ixfr:; data_size 1976
2025122700.zone.ixfr:; data_size 138504
2025122701.zone.ixfr:; data_size 139872
2025122800.zone.ixfr:; data_size 137272
2025122801.zone.ixfr:; data_size 137138
2025122900.zone.ixfr:; data_size 137318
2025122901.zone.ixfr:; data_size 137252
2025123000.zone.ixfr:; data_size 137176
2025123001.zone.ixfr:; data_size 137042
```

What if... the root is signed incrementally

	XFR size	Daily traffic	Factor
Baseline(without F)		0.96 MB	1
DNS XFR	1.31 MB	3.28 MB	3.4
HTTPS XFR (bug fixed)	2.19 MB	5.48 MB	5.7
HTTPS cache pre-fill	2.19 MB	2.19 MB	2.3
Incremental DNS XFR	0.10 MB	0.26 MB	0.27

What if... resolvers rely on ZONEMD only

What if... resolvers rely on ZONEMD only

- When resolvers verify and validate ZONEMD, then
 - they can assume all DSes are correct
 - they don't need to validate those RRSIGs anymore
- Need only the DNSKEY and ZONEMD signatures
- Special (A/I)XFRs without RRSIGs *except for DNSKEY and ZONEMD*
- Two hash values for ZONEMD
 - 1 for the full root zone with all RRSIGs
 - 1 for the full zone without RRSIGs *except for DNSKEY and ZONEMD*

What

- What

-

-

- New

- Sp

- Tw

-

-

```
willem@orangutan: ~/incremental-root
willem@orangutan:~/incremental-root$ grep '^; data_size ' *.rixfr
2025122200.zone.rixfr;; data_size 1024
2025122201.zone.rixfr;; data_size 1024
2025122202.zone.rixfr;; data_size 1253
2025122300.zone.rixfr;; data_size 1024
2025122301.zone.rixfr;; data_size 1024
2025122400.zone.rixfr;; data_size 1024
2025122401.zone.rixfr;; data_size 1024
2025122500.zone.rixfr;; data_size 1024
2025122501.zone.rixfr;; data_size 1024
2025122600.zone.rixfr;; data_size 1024
2025122601.zone.rixfr;; data_size 1024
2025122602.zone.rixfr;; data_size 1232
2025122700.zone.rixfr;; data_size 1024
2025122701.zone.rixfr;; data_size 1024
2025122800.zone.rixfr;; data_size 1024
2025122801.zone.rixfr;; data_size 1024
2025122900.zone.rixfr;; data_size 1024
2025122901.zone.rixfr;; data_size 1024
2025123000.zone.rixfr;; data_size 1024
2025123001.zone.rixfr;; data_size 1024
```

DNEMD

What if... resolvers rely on ZONEMD

- ZONEMD validation full (AXFR) transfer size: 0.52 MB, factor: 0.4

	XFR size	Daily traffic	Factor
Baseline(without F)		0.96 MB	1
DNS XFR	1.31 MB	3.28 MB	3.4
HTTPS XFR (bug fixed)	2.19 MB	5.48 MB	5.7
HTTPS cache pre-fill	2.19 MB	2.19 MB	2.3
Incremental DNS XFR	0.10 MB	0.26 MB	0.27
ZONEMD validation IXFR	1112 bytes	2808 bytes	0.0027

- 89% of IXFR messages < 1232 bytes

Local root: the traffic trade-off between root queries & root zone distribution

- Populating resolvers with the root zone will currently **increase** traffic (*per resolver on average*) with a **factor** of **2.3** at the very least
- **Acceptable?**
- **Decrease to one third** of the current average traffic per resolver is possible when the **root zone** would be **incrementally signed** and resolvers would XFR over DNS (with IXFR)
- **Radical decrease** to negligible amounts of traffic is possible (by relying on ZOMEMD to vouch for the DSes in the root zone), but **requires radical protocol changes**