DNS TTL's - some observations from the wild

John Ronan[12] Dr. David Malone[2] Naga Lakshmi Anipeddi[1]

[1]Walton Insitute
South East Technological University

[2]Hamilton Institute
Maynooth University

WALTON Institute for Information and Communication Systems Science

Outline

Background

- Would it be interesting to.....
  - Create some DNS records with long-ish expiry TTL's and see how long it takes for them to expire
  - Look up DNS records from various locations
  - Pull/Drop the records in various ways
  - Continue to look up DNS records and see how availability changes over time

Motivation: What happens if DNS infrastructure goes away (in-addr.arpa) and monitoring at the same time

Background

- What happens if we create an A record, wait for it to be visible and...
  - Scenario 1 - Remove the A record (NXDOMAIN), How long for it to actually disappear?

Background

- What happens if we create an A record, wait for it to be visible and...
  - Scenario 1 - Remove the A record (NXDOMAIN), How long for it to actually disappear?
  - Scenario 2 - Stop Named (SERVFAIL)

Background

- What happens if we create an A record, wait for it to be visible and...
  - Scenario 1 - Remove the A record (NXDOMAIN), How long for it to actually disappear?
  - Scenario 2 - Stop Named (SERVFAIL)
  - Scenario 3 - Shut down Server (SERVFAIL/REFUSED?)

Background

- What happens if we create an A record, wait for it to be visible and...
  - Scenario 1 - Remove the A record (NXDOMAIN), How long for it to actually disappear?
  - Scenario 2 - Stop Named (SERVFAIL)
  - Scenario 3 - Shut down Server (SERVFAIL/REFUSED?)
  - Scenario 4 - Firewall DNS port/Port unreachable (SERVFAIL/REFUSED?)

Experimental Setup

- Single Ubuntu 22.04 VM Sitting on Proxmox VE in HEAnet's Data Center
- BIND 9.18.28-ubuntu0.22.04.2
- Glue Records from master zone point to test server

Measurement

- Running/Hosting RIPE Atlas in HEAnet's Data Center
- Set up https://atlas.ripe.net/measurements/68036870/Measurement 68036870
- 50 Probes, once per hour, spread of 600 seconds

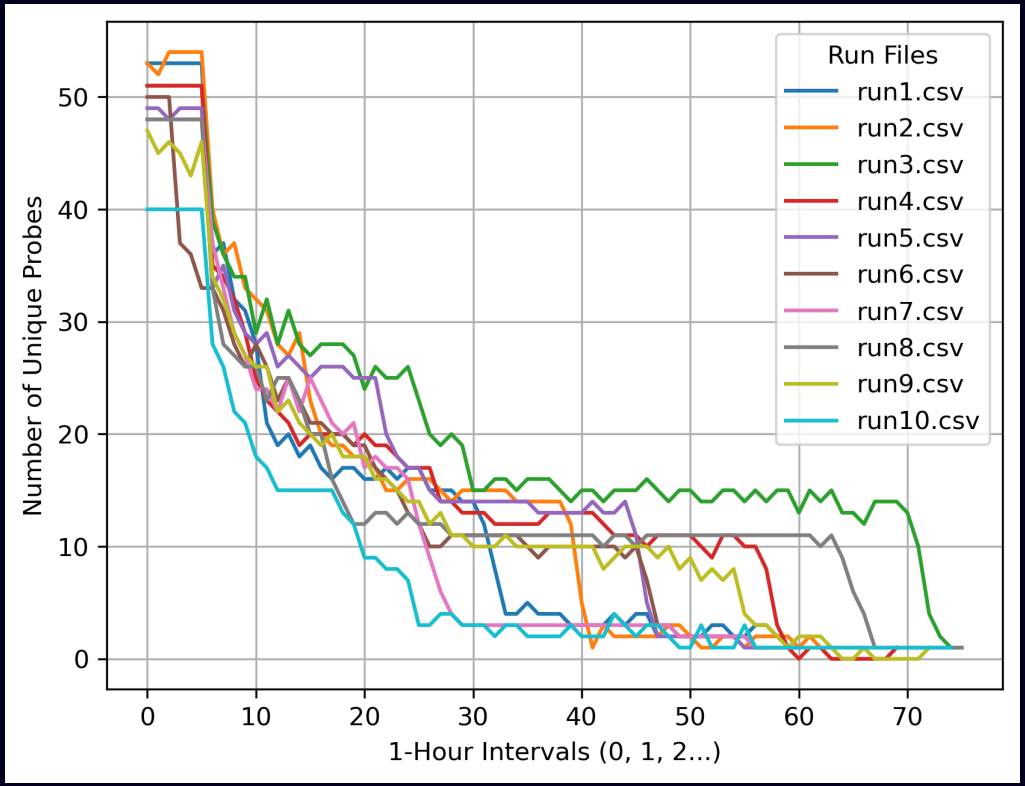
SOA Record

- Refresh 3 hours (10800)
- Retry 15 minutes (900)
- Expire 1 Week (604,800s)
- Min/Neg Caching 1 hour (3600s)

Methodology

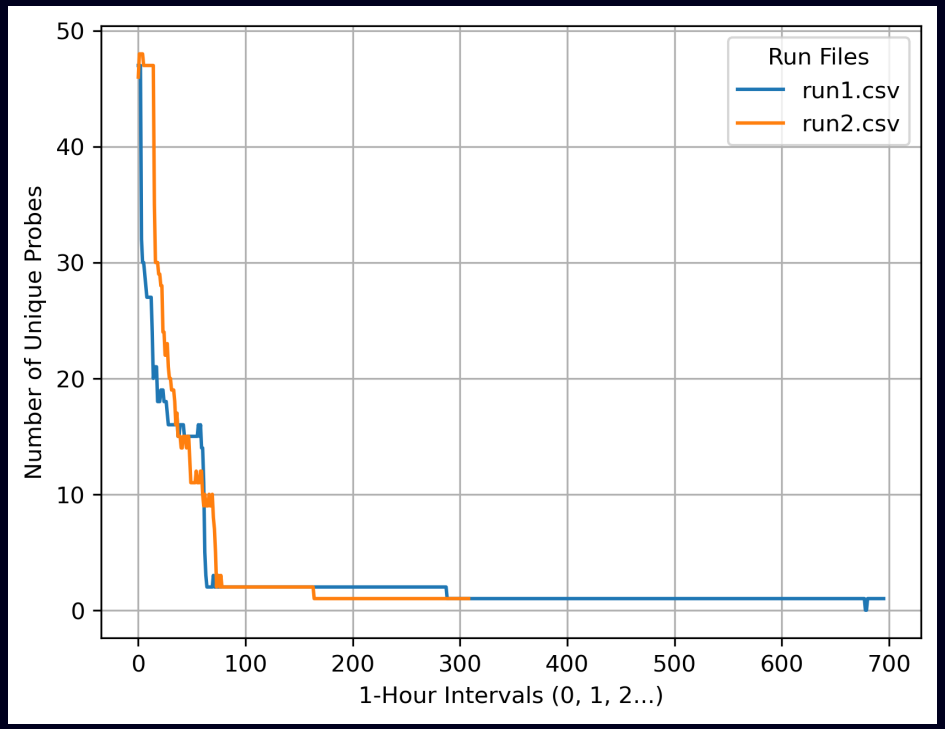
- NXDOMAIN
  - Create entry in Zone file
  - Monitor responses until the number of probes responding with 'success' becomes fairly constant
  - Remove entry, roll serial number forward, reload zone file
- SERVFAIL
  - Create entry in Zone file
  - Monitor responses until the number of probes responding with 'success' becomes fairly constant
  - Shutdown bind daemon

Results so far - NXDOMAIN



- Runs were started at different times of the day
- No apparent correlation between decay rate and time of day

Results so far - SERVFAIL



- Expire is set to 1 Week 168hours
- Stopped second run after 12 days
- Connections to Authoritative server are seeing 'connection refused'

Open Questions

- Are the same servers dropping off at the same rate each 'run'
- Is there detectable caching of stale results (looks likely, needs more work)
- What errors are we seeing, NoError or NXDomain should clean cache, Refused or ServError should continue to cache

Questions for audience

- Have we missed some literature here?
- We know about RFC8767, but haven't seen any measurements relating to it.

Thank You!
Any questions?