Improving DNS Service Availability by Using Long TTLs

draft-pappas-dnsop-long-ttl-02

V. Pappas, B. Zhang, E. Osterweil,
D. Massey, L. Zhang

Whose TTL We Are Talking About

- Everything in DNS is an RR and has a TTL value
- This talk: the TTL setting for NS RRs and associated A/AAAA RRs
  - *Infrastructure records*

Existing Recommendations for TTL Settings

- RFC 1034:
  - Some examples for host records
- RFC 1912:
  - TTL value for SOA records
- RFC 2308:
  - TTL values for negative answers

So far we have not seen a specific recommendation for setting TTL values for *infrastructure RRs*

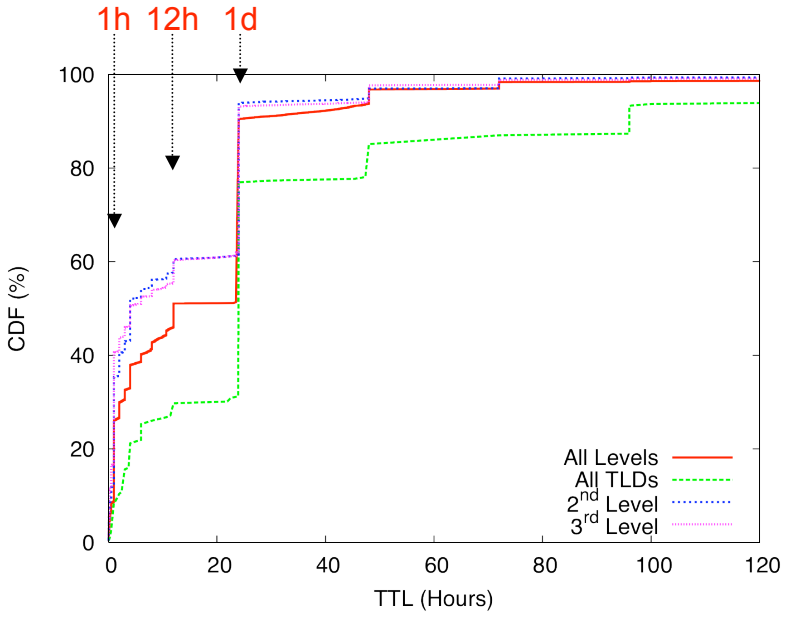
How Long Are the NS TTLs Used In Reality?

Data collected from actual queries (to about 1M zones)

1/3 of NS TTLs less than 1 hour

Even worse for 2nd and 3rd level domains

0.3% have TTL value of 0!



Sample zones with 0 TTL for NS RRs

- spcsdns.net.
- 0845pages.com.
- 800ideas.com.
- fasthousing.de.
- aacconsulting.com.
- usno.navy.mil.
- abcom.com.
- vmi.edu.
- academy21.com.
- acadia.net.
- acay.com.au.
- addictionggames.com.
- adoption.com.
- adoptionshop.com.
- in2home.co.uk.
- penisplus.com.br.
- cruisingforsex.com.
- ipowerweb.com.
- softure.com.
- adultlounge.com.
- skinnygirlies.com.
- aipm.co.il.
- airi.co.kr.
- avalon.nf.ca.
- baruel.com.br.
- yzu.edu.tw
- ran.es.
- ej-gv.es.
- fidal.fr.
- psu.ac.th.
- ghirada.it.
- momsdiary.co.kr.

- TTL values for some ccTLD NS RRs:
  - bb: 0 sec
  - ve: 10 minutes
  - cl: 20 minutes
  - ma: 30 minutes
  - cf,es,fm: 1 hour

- Fortunately:
  - the root lists 1 day for all TLDs
  - Resolvers usually learn the TTL for TLDs from the root zone

Our Recommendation

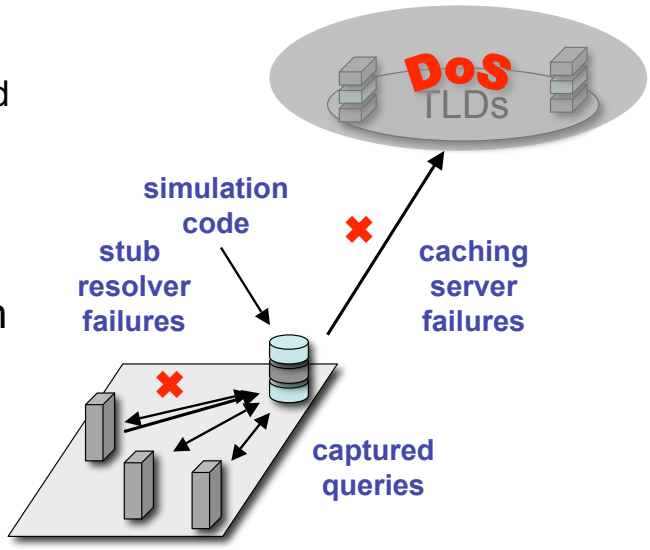
- Recommend that the TTL values for infrastructure RRs to be set longer
  - At least 1-3 days
  - Preferably 3-7 days?
- The benefits:
  - Adding resiliency to DNS service in face of DDoS attacks
    - Also improving performance
  - No protocol modifications, simple to deploy
  - Effective

Development of the Domain Name System (Mockapetris, 1987)

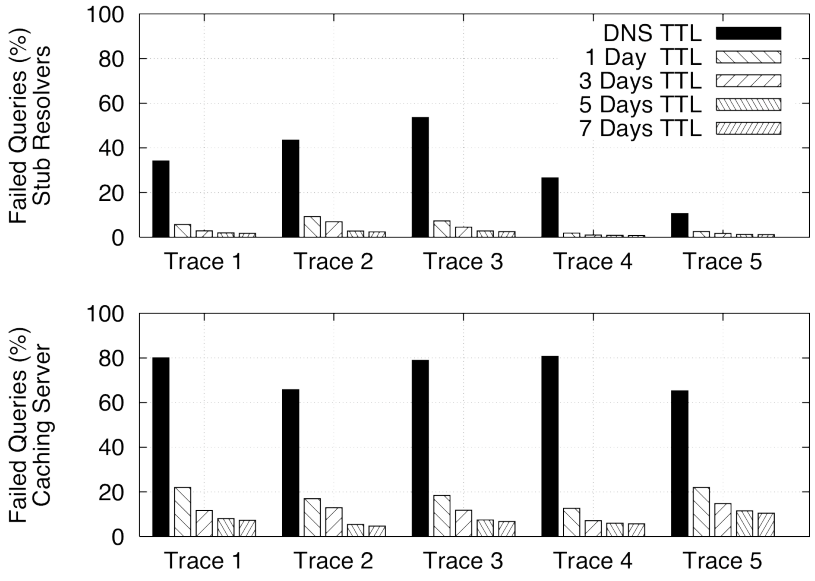
- The administrator defines TTL values for each RR as part of the zone definition; a low TTL is desirable in that it minimizes periods of transient inconsistency, while a high TTL minimizes traffic and allows caching ***to mask periods of server unavailability due to either network or host problems.***

Evaluation

- Experiment:
  - 5 DNS traces
  - 7 days long each
  - Simulate DNS cache
  - Assuming all TLDs wiped out by attacks on the 7th day
- Question: How many queries failed on the 7th day?



Service Resilience by Long TTL



Issues with longer infrastructure TTLs (1)?

- Dynamic DNS: no impact
- All your load balancing games can still work!
- We propose changes only to infrastructure TTLs
  - One can still set TTL of host RR's to 0 as one wishes

Issues with longer infrastructure TTLs (2)?

- Potential inconsistencies between authoritative NS/A RRs and the caches
- Our measurement shows that NS/A RRs do not change frequently
  - (only 5% changed in a month)
- In case servers changed during cache lifetime: inconsistency can be resolved (by paying a cost of query delay):
  - At the zones authoritative servers
  - Or, at the parent

Issues with longer infrastructure TTLs (3)?

- Would DNSSEC be affected?
  - We hope/believe not (much)
  - DNSSEC signature lifetime needs to be a small multiple of the TTL value

Questions to the WG

- Are there any other issues we missed?
- Would the WG be interested in taking on this topic of infrastructure RR TTL considerations as a working item?
  - Document the tradeoffs