Improving DNS Service Availability by Using Long TTL Values

draft-pappas-dnsop-long-ttl-04.txt

Vasileious Pappas + Eric Osterweil +
Danny McPherson + Duane Wessels +
Matt Larson + Dan Massey + Lixia Zhang

What do TTLs have to do with availability?

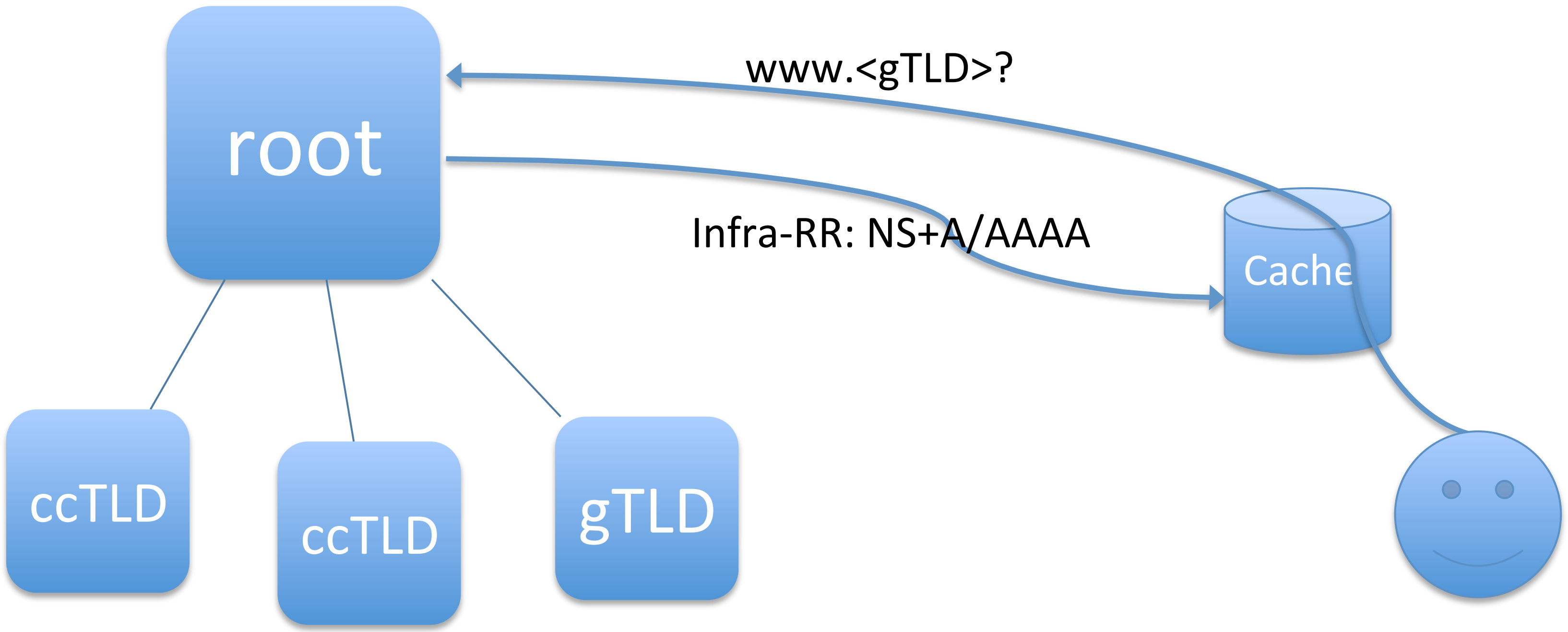
- Their role in caching can be used to speed up response time
- But, they can also reduce impacts of *total* zone outages, like from DDoS attacks
  - Redundant name servers help overcome local outages: if one NS is reachable it can serve they zone
  - But if they are all unreachable, only remotely cached data for a zone is available
- Long TTLs on *certain* RRsets mean that outages (from DDoS, for Ex) can be overcome by careful operational provisioning

Where does this really matter

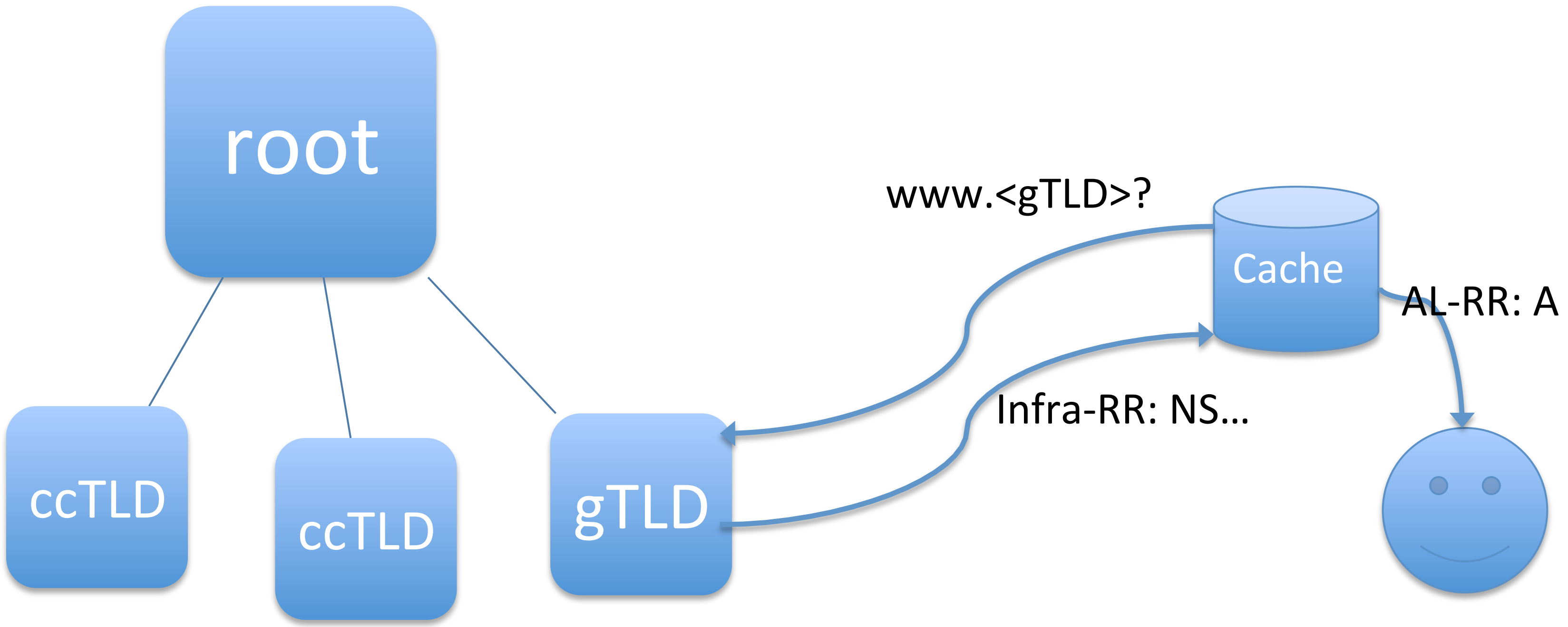
- We propose to distinguish between *Infrastructure RRs* and *Application Level RRs*
  - Infra-RRs: NS+A/AAAA,DNSKEY, DS, etc.
  - AL-RRs: <everything else>

- While content may need to change at varying rates, measurements have indicated Infra-RRs often don't
- In such cases, zones delegated from an unavailable zone may still be available during a parent zone's outage

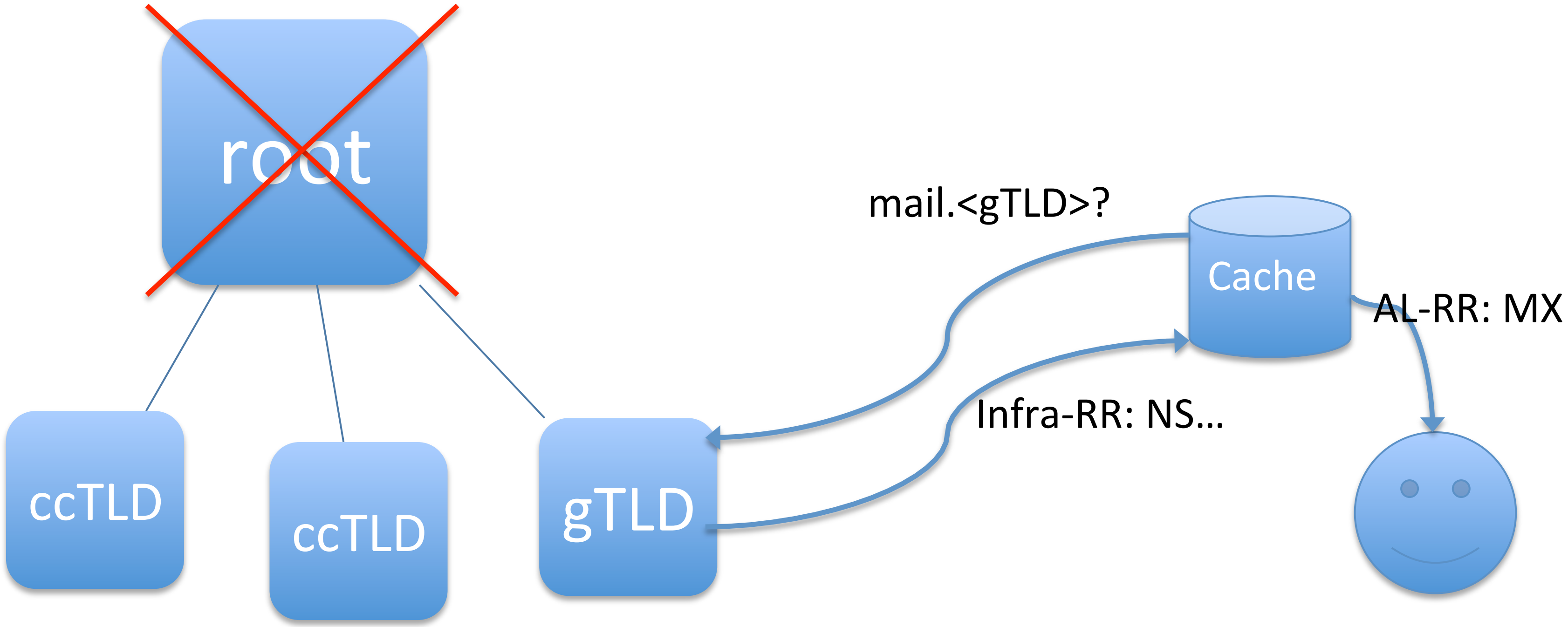
Example: t0



Example t1



Example t2



Who would this help, and how much?

- Helps Infra-RRs, higher up in the hierarchy
  - Long TTL delegations from root aid TLD subtrees
- Likely helps if there popular zones below a fan out (TLDs are an example)
  - Long TTL delegations from TLDs aid popular sites (who are likely to be cached)

Measurements

- Performed measurements and idealized simulations
  - Randomly selected 100,000 zones out of 15 million
  - During 4 months, 75% did not change NS+A/AAAA values
  - More #s in the draft

Simulations

- Simulated an outage at the root (all NS unreachable) using DNS resolver traces from UCLA

TTL (days)	3 hour attack	6 hour attack	12 hour attack	24 hour attack
-	28.6%	27.7%	28.8%	31.8%
3	14.5%	13.6%	13.6%	13.4%
5	11.7%	11.0%	10.8%	11.0%
7	9.8%	9.1%	8.8%	8.8%
9	9.1%	8.4%	8.0%	7.7%

Take away

- Longer TTL values *can* increase the overall system availability under denial of service attacks
  - Note: idealized cache (no TTL caps, etc)
- Simulations suggest that with a 7 day TTL, effects of DDoS-related outage can be mitigated by roughly 70%
- Note: just simulations, real tests show resolver/ cache-specific results
  - See Duane Wessels' OARC talk

Thanks

Questions?