CLOUDFLARE®

Revisiting TTL values

Ólafur Guðmundsson

Why talk about TTL´s

- There is no good guidance on what the values should be
- There are no ``Performance`` goals for changes to propagate to edges
- What is are the appropriate tradeoff’s ?
- Two cases:
  - Regular Records: A, AAAA, SRV, MX ….
  - Delegation Records: NS, SOA, DS

History matters

	Then	Now
Links	slow and unreliable	Fast and reliable connectivity
Computers	slow	Fast
Services	provided at single source	replicated/distributed/anycast
Delay tolerance	understanding	not acceptable
DNS changes	Move slowly through	fast changes, dynamic answers

Problem area

- When DNS change is migrating thought the system resolvers are inconsistent with each other, makes testing harder as some resolver have OLD data and some NEW.
- NS set exists on both sides of delegation + we have no “control” over which set is used by resolvers ==> we need to assume worst case
  - Changing DNS provider takes long time and child can not do anything about this !!!
- DS points to DNSKEY set.
  - During rollover child NEED’s to wait for parent DS set to propagate before taking next step(s)

How about goals

- How long should DNS be out-of-sync during change ?
  - Guidance both for delegation records and regular records.
- Should children expect of parents not getting in their way?
- Should one be able to expect that DNS operator (NS set replacement) take less than X hours ?
    - in .com it now takes over 2 days
- How can one roll DNSSEC keys in one working day ?
  - now it takes at least 3-5 days for most TLD’s

Opinions