

ANAME update

IETF 105, Montreal

Motivation

- We want a standardized way to do “www” referral from the zone apex
- Should work for CDNs
 - ECS, DNSSEC online signing, short TTLs, ...
 - But should not be required for simple use cases
- DNS providers have their own proprietary solutions
 - Makes it hard to switch providers, or support multiple provider model

History

- 7 Apr 2017: draft-hunt-dnsop-aname
- 27 May 2017: Adopted by the wg
- 11 Jan 2018: -01 version
 - Required resolver support
 - Issues with ANAME aware/unaware secondaries
- 19 Oct 2018: -02 version (Tony Finch rewrite)
- 15 Apr 2019: -03 version (Editorial)
- 8 Jul 2019: -04 version (Resolving GitHub issues)

-02

- Much cleaner version
- Resolver support is optional
 - Allows for gradual deployment
- Target lookup is optional
 - Sibling address records can be used as a default
 - Both authoritative and resolver may do the lookup
 - No exceptions for zone transfers
 - Lots of flexibility to adapt to your use case

-03

- Mostly style, structure, grammar, clarifications
- Split up Implications section
 - Clarify text on zone transfers (there are really no special exceptions for ANAME)
 - Dynamic updates (was just an example in -02, not a requirement for ANAME)
- Appendix on alternative setups
 - Targets the CDN use case
 - Add text on XFR scaling concerns and GeoIP

-04

- ANAME precedence
 - Sibling addresses as a default (not an override)
- TTL considerations
 - Address records in response is the minimum of all encountered TTLs during target lookup
 - TTL stretching considerations
- Revised query processing rules
 - QTYPE=A(AAA): ANAME in Answer section
 - QTYPE=ANAME: Sibling address records in Additional Section

-04

- #30: Maximum TTL
- #32: split additional section processing
- #34: Revisit TTL considerations
- #38: Relax requirements about sibling address records
- #43: Clarify ANAME processing requirements
- #53: “address record” should not be limited to A(AAA)
- #58: ANAME precedence
- #62: Answer vs Additional sections
- #68: Considerations related to ANAME behavior

Open issue: loop detection

- #45: ANAME loop detection
 - QTYPE=ANAME means don't chase targets
 - Target lookup queries MUST use QTYPE=ANAME
 - Will browsers in the future query for ANAME?
 - EDNS option "don't chase targets"
 - Target lookup queries MUST set this option
 - Resolver signals support for ANAME lookups
 - But authoritative may still want to chase targets to give a better response
 - How will browsers signal support?

Open issue: target lookup failure

- #66: ANAME target lookup fails, what now?
 - How to treat an erroneous response
 - What is the expected behavior? Return SERVFAIL?
Return currently known sibling address records?

Next steps

- Solve ANAME loop detection
- Define behavior when ANAME target lookup fails
- Publish -05
- WGLC?