DNS-Error Reporting draft (IETF109 recap)
draft-arends-dns-error-reporting-00

- DNS Resolvers often encounter errors with domain name configurations in authoritative servers.
- The DNS-Error Reporting draft describes a method to allow resolvers to signal the error back to the owner of that domain.
- The intent is to help domain owners and authoritative server operators detect misconfigurations earlier.
- This draft was first communicated to several DNS software development teams to get early feedback, which was overall positive.
- IETF109 hackathon resulted in one server-side implementation. The resolver-side depends on Extended DNS Errors implementation.
- The current draft will see some additional edits, but the idea seems stable.

DNS-Error Reporting draft (IETF110-111)
draft-arends-dns-error-reporting-00

- Recent errors and warnings are a good example of the issues that can be reported
  - Failures due to DS records at zone apex.
  - NSEC3 iterations higher than RFC5155 recommended CAP
  - DNSSEC configuration issues:
    - .beauty, .llp, .unicom, .firestone, etc etc
    - cdc.gov, caltech.edu, time.nist.gov, etc etc
- Recent work in the DPRIVE Working Group has proposed using DNS records for discovery of whether an authoritative server offers DNS over encrypted transport.
- In such an environment, it would be useful for a resolver to be able to report to an authoritative server if such discovery records are in error.
- Our proposed method can deliver that error.
- We have asked the IETF DNSOP WG chairs to assess consensus to adopt this as a DNS WG item.