From: Mark Andrews
Sent: Tuesday, 26 February 2019 11:23:41 AM
To: auDA Policy Review
Subject: Basic DNS server RFC compliance.

The implicit assumption that when someone registers a DNS server is that theserver being registered behave as documented in the various DNS RFCs. This however is clearly not the case[1] and causes current and future operational problems, so much so that DNS resolver vendors banded together to say “Enough is enough” and collectively removed work arounds for some of the misbehaviours[2].

Every time the DNS has extended resolver vendors come across non-compliant behaviour.

* Adding new record types (e.g. AAAA and TLSA record) you have servers that return invalid answers like NXDOMAIN or NOTIMP for names that return A record or just don’t return a response at all. RFC 1034/RFC 1035 behaviour would be to return NOERROR without any records at the name. DNS vendors should not assume that only specific query types will be sent to a DNS server. All types are to be expected. Testing for whether a service exist at a name is often done by querying for specific types at that name.

* Adding flag bits to requests. Queries get block or flag bits get blindly copied to responses. The AD bit suffers from this as there are servers that blindly copy this bit to responses making its presence in the response unreliable. RFC 1034/RFC 1035 specifies that servers ignore unknown bits in the request and to set them to zero when sending. Adding the EDNS DO flag bit also cause problem in that there were firewall that blocked the query despite explicit instructions that unknown (at the time) EDNS flag should be ignored.

* Add the OPT record to DNS requests for EDNS resulted in queries being blocked rather than FORMERR being returned.

* Adding DNS COOKIE EDNS option to DNS requests resulted in request being blocked rather than the unknown option being ignored.

This misbehaviour has mostly been the result of DNS vendors taking short cuts and firewall vendors not understanding DNS properly (Checkpoint and Juniper have removed overly strict checks recently in the default firewall configuration of the products they ship).

Either a new policy need to be written of a existing policy expanded to say that listed DNS servers need to comply with the existing RFCs, in particular RFC 1034 and RFC 1035. If EDNS is implemented, RFC 6891. If DNSSEC is implemented, RFC 4034 and RFC 4035.

There needs to be discussion about how to test for compliance. What tests should be made. There is test software available that can perform checks. Testing how servers handle the “unknown” is critical to the ability to deploy future changes. The listed RFC above all contain rules about how to handle the “unknown”. Change was expected. Unfortunately this is often not tested for and as a result interoperability problems arise.

There needs to be discussion about what steps should be taken when non compliance is detected / reported.

There is a lot of technical debt out there. Most of it can be addressed by just upgrading to recent versions of the product causing the issue.

Mark

[1] EDNS Compliance, <https://ednscomp.isc.org/>.

[2] DNS Flag Day, <https://dnsflagday.net>.