EDSR

Encrypted DNS Server Redirection

Corey Mosher – Quad9
John Todd – Quad9
Tommy Jensen – Microsoft

Changes from IETF 115

Changed name used from the resolver.arpa SUDN to the name of the resolver

Provided guidance for self-redirections, redirection chains, and multiple redirects

Defined how the effective TTL of a redirection is determined

Added TLS minimum version as a compat requirement of destination server

Clarified adding requirements to which TLS cert chains to trust is out of scope

Reviewing IETF 115 Feedback

“Use of resolver.arpa is problematic”

Two arguments provided: conflation with DDR configuration and risk of EDSR queries being blindly passed along to upstream resolvers

Text changed to use the name of the resolver instead of an SUDN

Reviewing IETF 115 Feedback

“What guidance for self-redirecting / looping / long chains of redirections?”

Not generally a good idea (but avoiding a specific number, left up to clients to decide how much “too many” is and server cautioned to minimize use of chains)

Added text to define self-redirecting as name-based, not IP-based

Added text to specify that self-redirecting may allow client discovery of other configurations it could use to reconnect

Added considerations for avoiding loops, long chains, and multiple redirects

Reviewing IETF 115 Feedback

“Why not use HTTP 3xx / comparison with alt-svc related work”

This approach ensures we have a general solution across all TLS-based encrypted DNS protocols (HTTP mechanisms would be DoH-specific)

We believe this is sufficiently different from the Alt-SvcB scenario to warrant separate work

We believe HTTP alt services show a precedent for trusting redirections without DDR-like shared control verification

Reviewing IETF 115 Feedback

“This poses geo-based policy concerns / why not client configuration?”

We believe EDSR can be used to address geo-based policy concerns

- It is more transparent to the client than anycast about destination
- Lost clients can be guided to the right geolocation

This does not replace client configuration; it replaces the need for anycast, while also allowing traffic shedding and geolocation optimizations

Next Steps

Seeking WG adoption

Any blocking issues?