

DNS over DTLS (DNSoD)

draft-ietf-dprive-dnsodtls-02

November 2015

IETF 94

Authors: T. Reddy, D. Wing and P. Patil

Presenter : Dan Wing

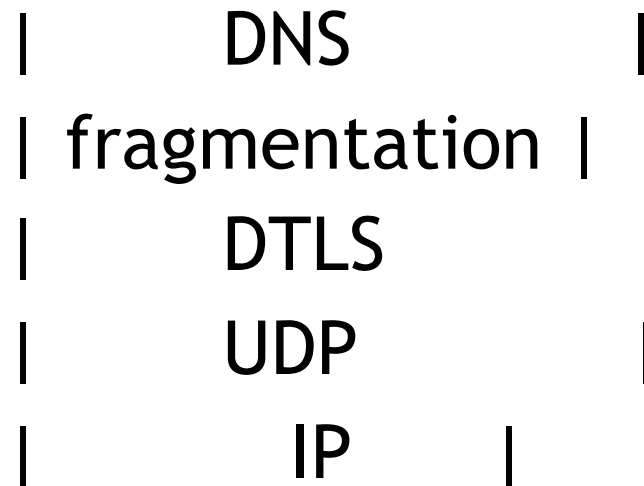
Major changes from 01 to 02

- Now using IANA-registered port 853
- Added Fragmentation and Reassembly

Fragmentation and Reassembly

- Problem: “Big responses cause fallback to DNS-over-TLS, so why bother with DNS-over-DTLS?”
- Solution 1: abandon DNS over DTLS
- Solution 2: add fragmentation and reassembly
- Negotiated during DTLS connection
- Overhead only when fragmenting

Layering



Fragmentation Design

- Client and server negotiate # of fragments
- No additional server state
- Works with RR change between re-xmited requests
 - Changing RR is obscure, but robustness important

WG Feedback

- Fragmentation: Necessary? Design?

draft-ietf-dprive-dnsodtls-02