DNS Not Over UDP/TCP, mid-2017 Update

Paul Hoffman

ICANN

DNS-OARC 26, Madrid

DNS over **TLS** and **DTLS**

- The DPRIVE WG finished the base spec for DNS over TLS, RFC 7858, a year ago
- Authentication profiles (draft-ietf-dprive-dtls-and-tls-profiles) should be ready very soon
- Stub-to-recursive only
- Some implementations, but very little deployment so far
- DNS over DTLS, RFC 8094, published a few months ago

DNS over **HTTP**

- Generic DNS over HTTP proposed last year
  - Focus on HTTP/1 caused too many options
- Recent draft-hoffman-dns-over-https on DNS over HTTP/2 over TLS
  - Getting much more traction with browser vendors
  - Still stub to recursive, but for applications like browsers and even JavaScript apps in browsers
  - Can easily be turned into DNS over HTTP/2 over QUIC
- Also draft-ietf-dnsop-dns-wireformat-http
  - Different use case: proxying DNS queries

DNS over **QUIC**

- draft-huitema-quic-dnsoquic
- Very recent
- Being used as a test case for "something other than HTTP/2 over QUIC"
- Advantages over DNS over TLS
- Might exist in parallel with "DNS over HTTP/2 over QUIC"

Later this year

- More activity on DNS over HTTP/2 and probably DNS over QUIC
- Maybe start of discussion of DNS-over-foo for recursive-to-authoritative connection?
- More deployment of DNS over TLS?