

DNS over HTTP

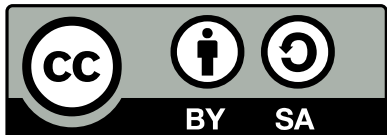
draft-shane-review-dns-over-http

draft-song-dns-wireformat-http

Davey Song, Shane Kerr, Runxia Wan / BII Labs

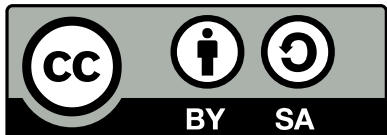
Paul Vixie / Paul Vixie

2016-04-08 / dnsop @IETF 95



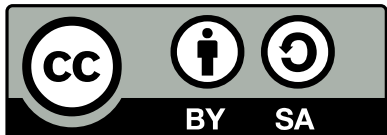
DNS over HTTP: two drafts

- “survey” document
 - Covers many models of DNS over HTTP
 - Informational
- “wire format” document
 - Covers one specific production protocol
 - Standards-track?



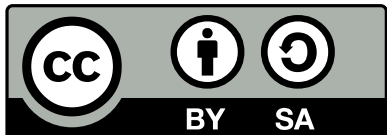
DNS over HTTP survey

- High-level abstraction of approaches
- From most like DNS to most like the web
- Thanks to Jinmei and Stéphane Bortyrmeyer for feedback!
- One more draft likely with minor updates.



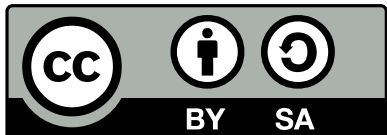
DNS over HTTP wire format

- Documents two implementations
- As simple as possible... but not simpler
- Normal HTTP POST message
- Wire-format DNS message
- Headers
 - Content-Type: application/octet-stream
 - Proxy-DNS-Transport: udp (*or tcp*)



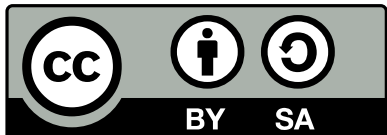
Wire format scenarios

- Proxy mode
 - Either client or server can run as a proxy
 - "drop-in" support
- Direct mode
 - Support in server
 - none yet... is it useful?
 - Support in applications
 - via API
 - Better in truncation case



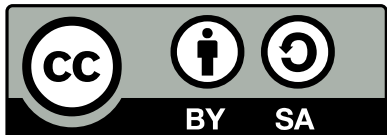
Wire format latest discussion

- POST vs. GET for HTTP message
- *Could* be used by web developers
- TCP/UDP flag required
- Clarification of 2-byte length field in TCP
- Expanded security section
 - A bit vague, since all DNS, HTTP, and TLS vulnerabilities may be applicable....
- `/.well-known/dns-over-http`
- Thanks to Bob Harold and Paul Hoffman for review!



Performance Tests

- Latency tests:
 - <http://www.dnsv6lab.net/...protocol/>
- UDP
- TCP
- HTTP(S) (w & w/o keepalive)
- HTTP/2
- TLS
 - TLS performance was surprisingly poor



Adoption?

- Survey
 - Informational
 - Independent Submission?
- Wire format
 - We present one solution
 - Could be informational or standards-track
 - We think it should be a dnsop document

