



DNS over HTTPS

The Current State of DNS is Disastrous

Privacy, security, efficiency

Regular DNS data is sent over UDP in “clear text”

Users just magically “get” a DNS server to use

Easily spied upon

Most resolvers “snitch” on you by telling the world *you* asked for `www.s`

DOH is HTTPS - no snooping!

DOH let's you select a server using
Qname minimization, EDNS client subnet

Privacy, security, efficiency

DHCP is insecure, easy to force clients to use specific servers

DNSSEC is typically used by resolvers only

UDP DNS is easily *modified* by third parties and is - in 1.5% of traffic

DOH is HTTPS - no modifying

Verified server

Privacy, security, efficiency

HTTPS with HTTP/2 means

- ✓ Multiplexing
- ✓ connection re-use
- ✓ proxy friendly
- ✓ hard to block

DOH in IETF

Not standardized yet (DOH working group)

<https://tools.ietf.org/html/draft-ietf-doh-dns-over-https-07>

Limited server availability still

DOH in Firefox 61

Configured separately (about:config, “network.trr.*”)

Can be used as “try this first, fallback to native if necessary”

I wrote it

<https://daniel.haxx.se/trr>

DOH in curl (1/2)

Not started yet

Custom DNS code, small and easy enough (?)

Bootstrap DOH server with `-resolve` (?)

Basically a request before the actual request

Let's use the "real" TTL for caching

Do test cases with the "regular" HTTP server

Fallback modes?

DOH in curl (2/2)

Who's in?!

