

Dude, where's my DNS?

Sara Dickinson sara@sinodun.com

DNS is evolving

DOT: [DNS-over-TLS](#)

DOH: [DNS-over-HTTPS](#) (WIP)

- **DOT** [RFC7858](#) standard May 2016
- **DOH** draft [draft-ietf-doh-dns-over-https](#) is in WGLC
 - Deals with protocol, not detailed use cases or discovery
- Both are happening, both will change stub to recursor
DNS in many ways.... focus on end user here

Implementation

	Client	Recursive Resolver
DOT	<ul style="list-style-type: none">• getdns library• Stubby (smart proxy)• Unbound/Knot resolver (fwd)• Android system config (dev)• systemd (PR)• Tenta browser	<ul style="list-style-type: none">• Unbound, Knot Resolver, dnsmdist, CoreDNS, Tenta• BIND on the way
DOH*	<ul style="list-style-type: none">• Android 'Intra' App• Firefox config option + "experiment"• Stubby (next release)• Various experimental	<ul style="list-style-type: none">• Various experimental

* 10+ implementations (see DOH mailing list and IETF 101 Hackathon)

Recursive Resolver Deployment

	Standalone	Large Scale
DOT	<ul style="list-style-type: none">• <u>19 test servers</u>	<ul style="list-style-type: none">• Quad9 (9.9.9.9)• Cloudflare (1.1.1.1)
DOH*	<ul style="list-style-type: none">• Google https://dns.google.com/experimental• Few other test servers	<ul style="list-style-type: none">• Cloudflare https://cloudflare-dns.com/dns-query

* Experimental, some support JSON as well as wireformat

System or App?



- **Always been technically possible** for apps to do their own DNS, has just been the exception and not encrypted.
- **getdns** was designed as a modern, async DNS API with applications in mind (but also as a system wide component)
- **DOH** use case “allowing web applications to access DNS information via existing browser APIs”
 - Fully expect all browsers to offer DOH soon as **browser wide option** (will it ever be the default?)
 - Proposals about **discovery** of DOH server for a domain...

SYSTEM RESOLVER

**YOU KEEP USING THAT WORD. I DO NOT
THINK IT MEANS WHAT YOU THINK IT MEANS**

Dude, where's my DNS?

- In a 'cloud' based world, most queries go through the browser
- Other apps likely to follow and system component will use DOT/DOH
- But what does this practically mean for users?
 - Most won't notice...
 - Increased privacy (yeah!)
 - But.. complicates DNS management

Dude, where's my DNS?

- In a 'cloud' based world, most queries go through the browser
- Other apps likely to follow and system component will use DOT/DOH
- But what does this practically mean for users?
 - Most won't notice...
 - Increased privacy (yeah!)
 - But.. complicates DNS management



Dude, where's my DNS?

- Multiple config points (transport, authentication)
 - Importantly DNSSEC ✗
- Multiple recursive resolvers
 - Scatter queries/reduce leakage ✓
 - What if some fail, get blocking or attacked ?
- Multiple points for monitoring/debugging?
 - Will all apps expose DNS queries to users? ?
- Co-ordination of end device DNS is not obvious
 - System API to advertise user preferences?

Dude, where's my DNS?

- Multiple config points (transport, authentication)
 - Importantly DNSSEC ✗
- Multiple recursive resolvers
 - Scatter queries/reduce leakage ✓
 - What if some fail, get blocking or attacked ?
- Multiple points for monitoring/debugging?
 - Will all apps expose DNS queries to users? ?
- Co-ordination of end device DNS is not obvious
 - System API to advertise user preferences?

DNS no longer
part of the
infrastructure?

Dude, where's my DNS?

I'm not judging...
I'm just saying...

Dude, where's my DNS?

I'm not judging...
I'm just saying...



It's DNS Jim,
but not as we know it

Thank you!