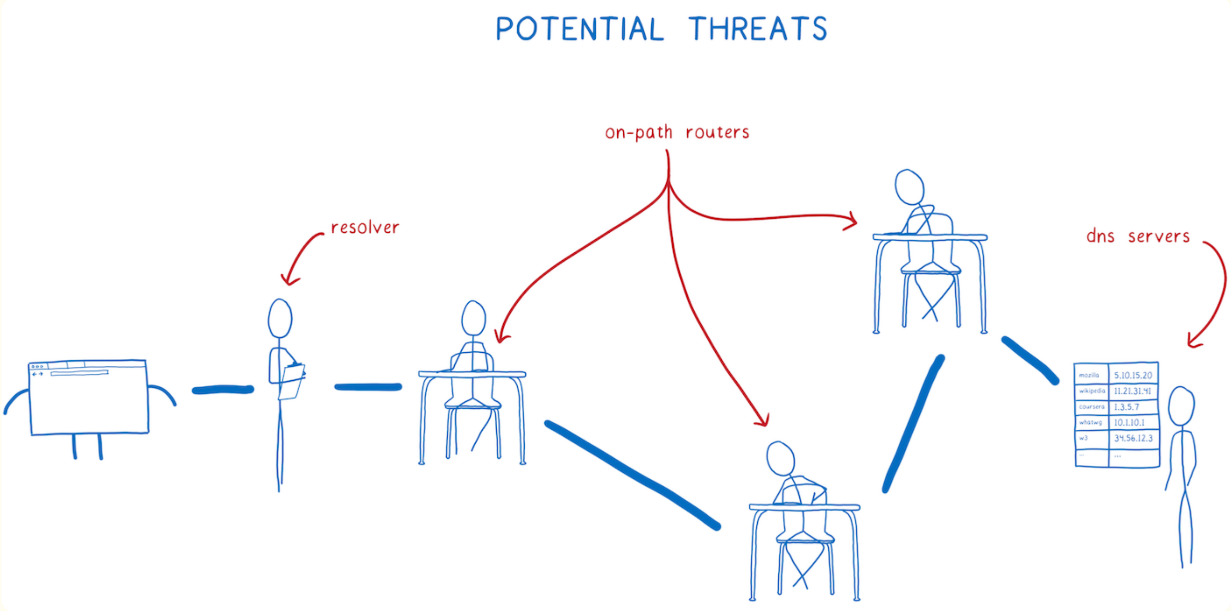
iOS 14, Big Sur and DNS over HTTPS

17 Sep 20

iOS 14 & MacOS Big Sur have finally added support for DNS over HTTPS↗ and DNS over TLS↗ standards — also known as encrypted DNS.

What is DOH / DOT?



mozilla	5.10.15.20
wikipedia	11.21.31.41
coursera	1.3.5.7
whatwg	10.1.10.1
w3	34.56.12.3
...	...

↗

Imagine you're at a conference. You're using its public Wi-Fi.

How many entities will know what websites you've been visiting out there?

1. Conference organizer aka Wi-Fi admin
2. Internet service provider (ISP) of the organizer
3. All ISPs / companies that route traffic of this ISP

Prior to 2013, most traffic was sent via HTTP without any encryption. So, everyone saw exactly which wikipedia page you've been at.

Today, most traffic is encrypted, thanks to HTTPS and Let's Encrypt↗. All these entities can still see that you've been visiting wikipedia.org↗ — but it's hard for them to deduce which exact article it was. This happens because your device sends DNS queries, which associate some website with some IP address.

With Encrypted DNS, the middlemen will only see `91.198.174.192` — which is an IP of `wikipedia.org`. Hold on, there's a nice detail. Ipinfo.org tells us there are at least 19 domain names associated with this IP! In fact, you could be visiting `invoker.com` — which has the same IP today. The ISP would not know the difference.

This is particularly useful in our age of cloud computing, when one Amazon IP is reused by five different customers.

Note: Even with encrypted DNS, TLS connections contain **unencrypted domain name -** it's called SNI. This can be, however, handled by using TLS 1.3 & encrypted SNI↗.

HTTPS or TLS?

There are many articles that compare DoH to DoT, but it all comes back to these points:

1. It's harder for middlemen to monitor and censor DNS queries if it's DNS over HTTPS. It looks like ordinary HTTPS traffic, while DNS over TLS requires separate port 853.
2. DNS over TLS may be faster since it's one level lower, but judging from benchmarks, that's not the case.

So, my recommendation here is to just use DoH.

Dangers of encrypted dns

If your ISP is no longer resolving DNS addresses, someone else must be doing it?

Today, it's probably cloudflare with its 1.1.1.1 public DNS, or google (8.8.8.8). So, instead of letting your ISP monitoring your DNS traffic, Cloudflare or Google will do it.

Of course, they can sell collected data, or use it to create a dossier on someone.

Ideally, there would be thousands of fast public eDNS servers.

Of course, there is no need to use public DNS servers. If you want a higher level of privacy, set up your own eDNS server.

Using DOH / DOT

If you've been using Firefox, enabling DOH is as simple as entering DNS server

IPs in Network Settings.

To make those work natively for all apps in iOS & MacOS, you’ll need to install configuration profile. This profile would tell operating system to use DOH / DOT. Note: it’s not enough to simply set cloudflare (etc) server IPs in System Preferences — you need to install a profile.

- Cloudflare↗
- Google↗
- OpenDNS↗
- Quad9↗
- Other 10+ profiles↗

On iOS, after installation, go to system **Settings => General => Profile**, select downloaded profile and click “Install” button.

All profiles are located at github.com/paulmillr/encrypted-dns↗, you’re welcome to review the source code & adjust it to your needs.