Domain Name Basics
DNS: DoT, DoH, and DoQ

Tobias Sattler
tobiassattler.com

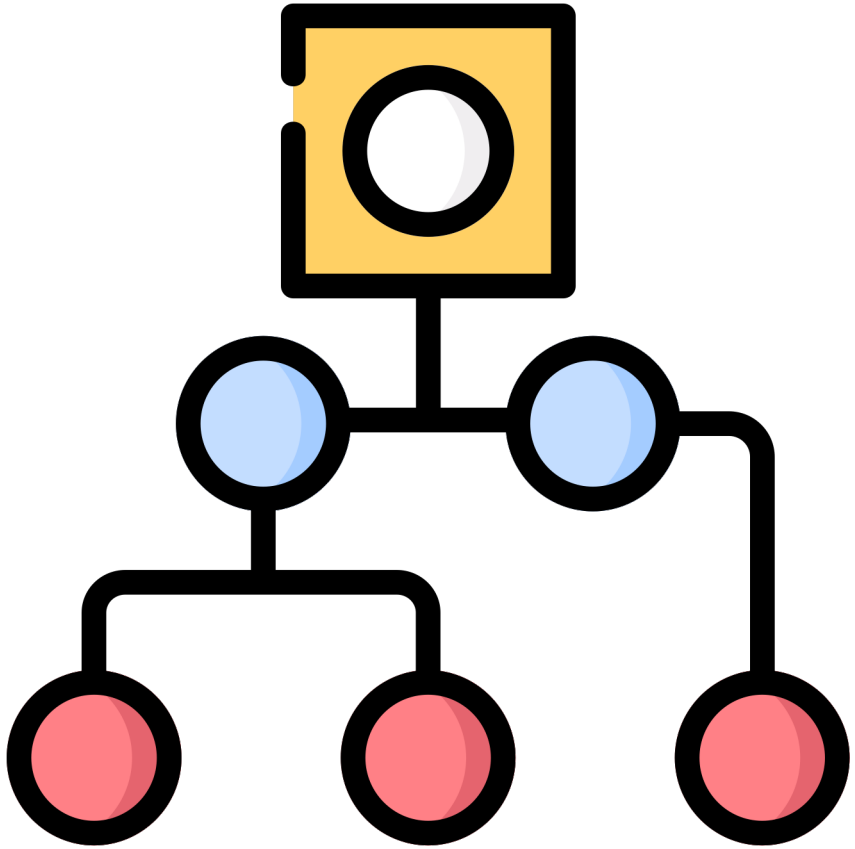
Domain Name System (DNS)

DNS is a hierarchical distributed naming system to **translate domain names** into **IP addresses**, which makes websites easier to remember, such as

- tobiassattler.com instead of 78.46.19.133

The domain namespace is a tree, and its root is a dot.

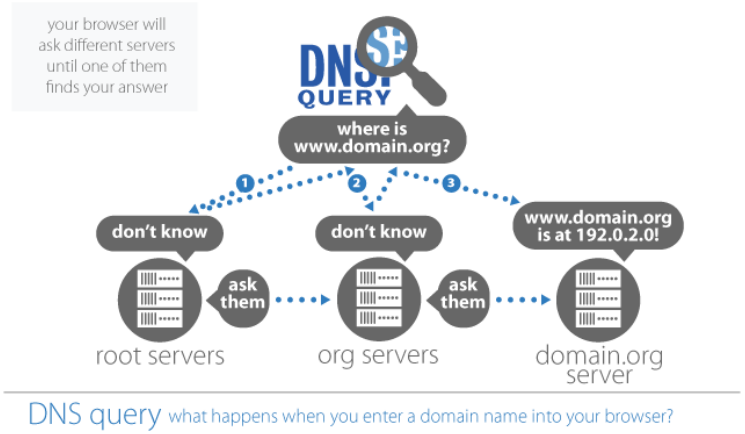
- www.tobiassattler.com.



What is a DNS query?

A **DNS query** is the **process** to inquire about the **IP address** for a **name**, such as tobiassattler.com into 78.46.19.133.

Domain name resolvers determine the domain name server responsible for the domain name in question by a sequence of queries starting with the right-most (top-level) domain label.



Picture Source: https://whois.icann.org/en/dns-and-whois-how-it-works - Effective 10/2020

Flaws of the system

DNS is **unencrypted**. That means that everyone between your device and the DNS resolver can see and even modify your queries and responses.

That frequently happens in public WiFi networks but can also occur with your Internet Service Provider (ISP) or the transit providers.

In short, it **affects your privacy** by revealing the domain names that you are visiting.

DNSSEC #1

The original design of the Domain Name System (DNS) did not include security and allowed false DNS data to be returned.

This required trust that the DNS answers were authentic and not modified.

Domain Name System Security Extensions (DNSSEC) is a set of extensions to DNS that provide DNS clients via a **digital signature** (resolvers) **origin authentication** of DNS data.

DNSSEC #2

By validating the digital signature, a DNS resolver can check if the information is identical to the data published by the zone owner and served on an authoritative DNS server and thereby mitigate, such as ‘man-in-the-middle attacks’ (see also https://en.wikipedia.org/wiki/Man-in-the-middle_attack).

DNSSEC doesn’t provide confidentiality of data, and the responses are **authenticated** but not **encrypted**.

Authenticity without Privacy

DNSSEC allows clients to verify the returned DNS answer's integrity, but it does **not encrypt** the DNS transport.

With that, you can make sure that the DNS resolver is providing the "true" answer.

However, if you want to be sure that your client receives the DNS resolver's untampered answer, you need additional encryption.

DNS over TLS

DNS over TLS (DoT) was published in the RFC 7858 in May of 2016.

With DoT, the original DNS communication is embedded into a secure and encrypted TLS channel between the requesting device and provider. That protects the privacy of the request and ensures it is not modified.

DoT uses a different port to communicate (port 853) instead of DNS port 53.
Because this introduces a new port, existing firewalls may require updating to allow it to function correctly.

DNS over HTTPS

DNS over HTTPS (DoH) was published in the RFC 8484 in May 2018.

DoH is using the same port as all encrypted web traffic: 443.

It was designed to support two primary use cases:

- Prevent the DoT problem that the port may be blocked.
- Enable web applications to access DNS through existing browser APIs.

DNS over QUIC

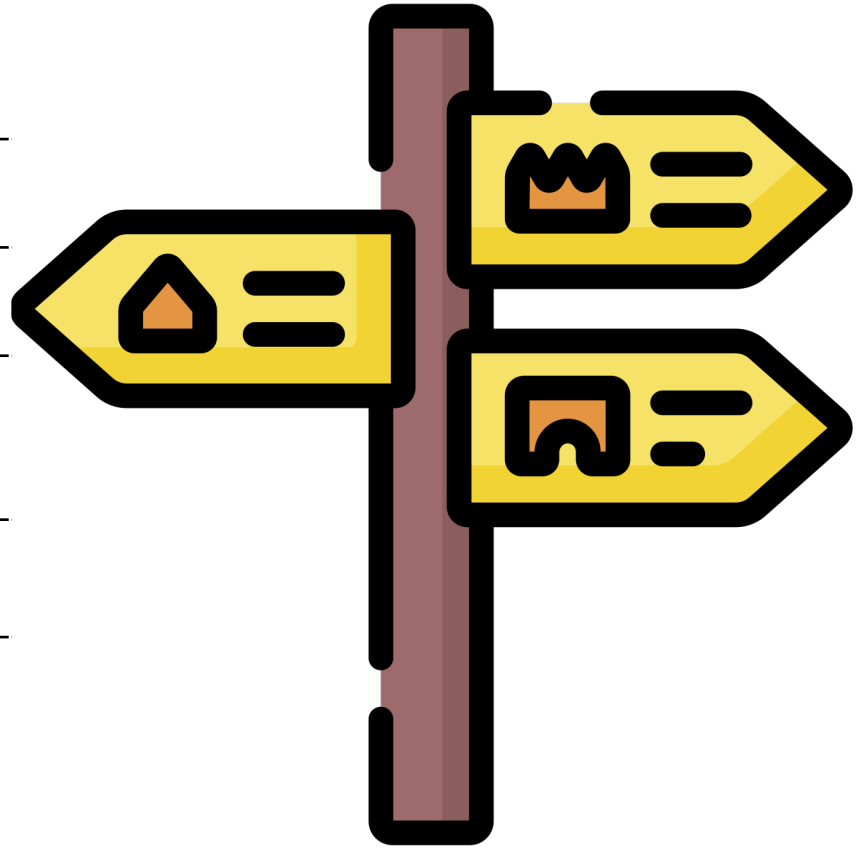
DNS over QUIC (DoQ) is still in development at IETF and is relatively new.

DoQ requires a UDP port to be accessible and will probably use a new port.

QUIC is similar to DoT, but without the head-of-line blocking problem due to the use of QUIC. It has implemented TLS1.3 by design.

Comparing DoT and DoH

DoT	DoH
RFC 7858	RFC 8484
New Port 853	Existing Port 443
Traffic can be blocked	Traffic looks like every other encrypted web traffic
No API capabilities	API capabilities
Might be faster due to missing HTTPS layer	Build-in browser support



Conclusion

One of the cornerstones of the Internet is mapping names to an address using DNS. It has traditionally used insecure, unencrypted transports.

DoT is a more straightforward transport mode than DoH as the HTTP layer is removed, making it easier to be blocked, either deliberately or by accident.

The DoT and DoH transport protocols are ready for us to move to a more secure Internet. DoQ will undoubtedly play a role in the future as soon as the standard is completed, and Quick handles more traffic.

Thank you!