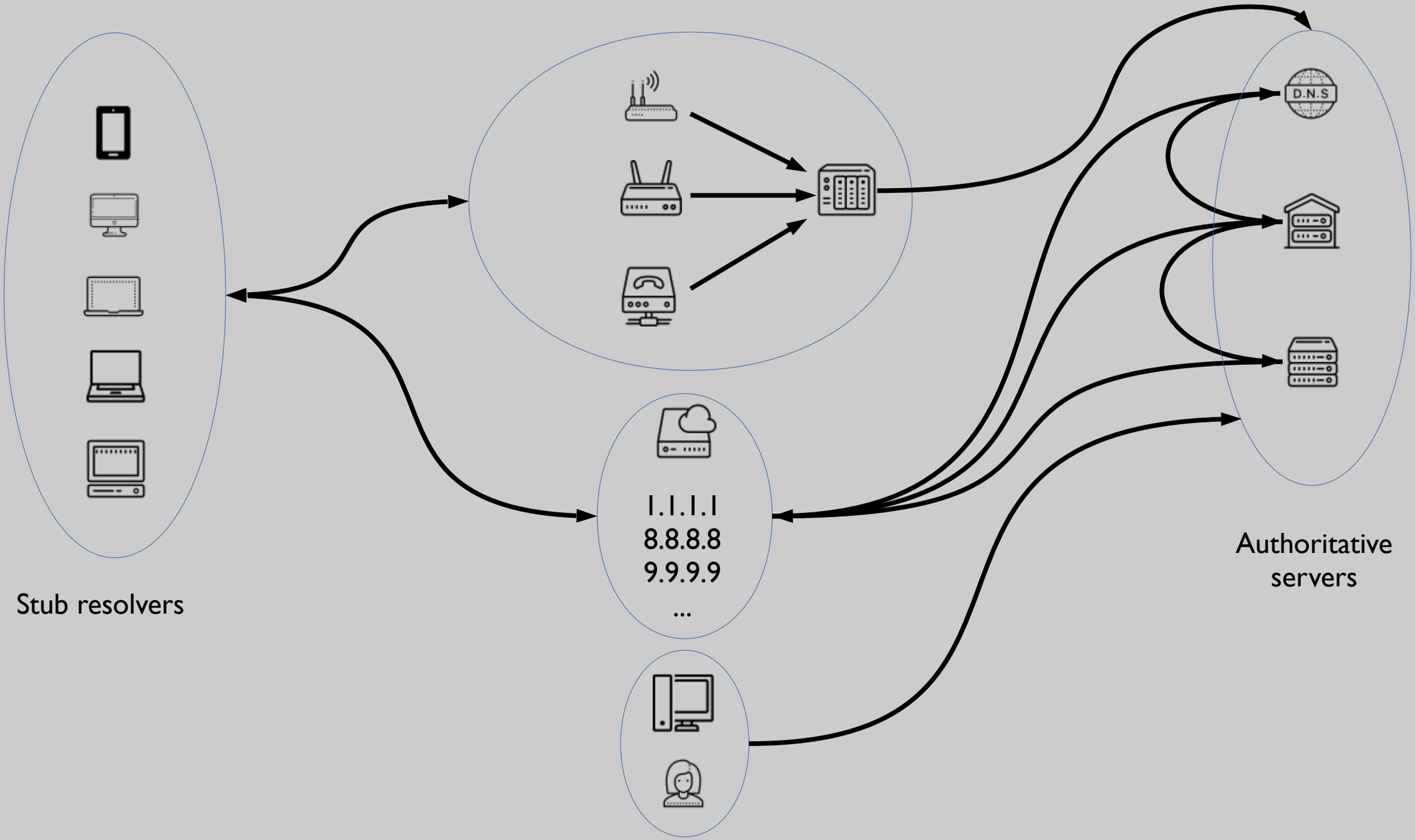
DNSSEC

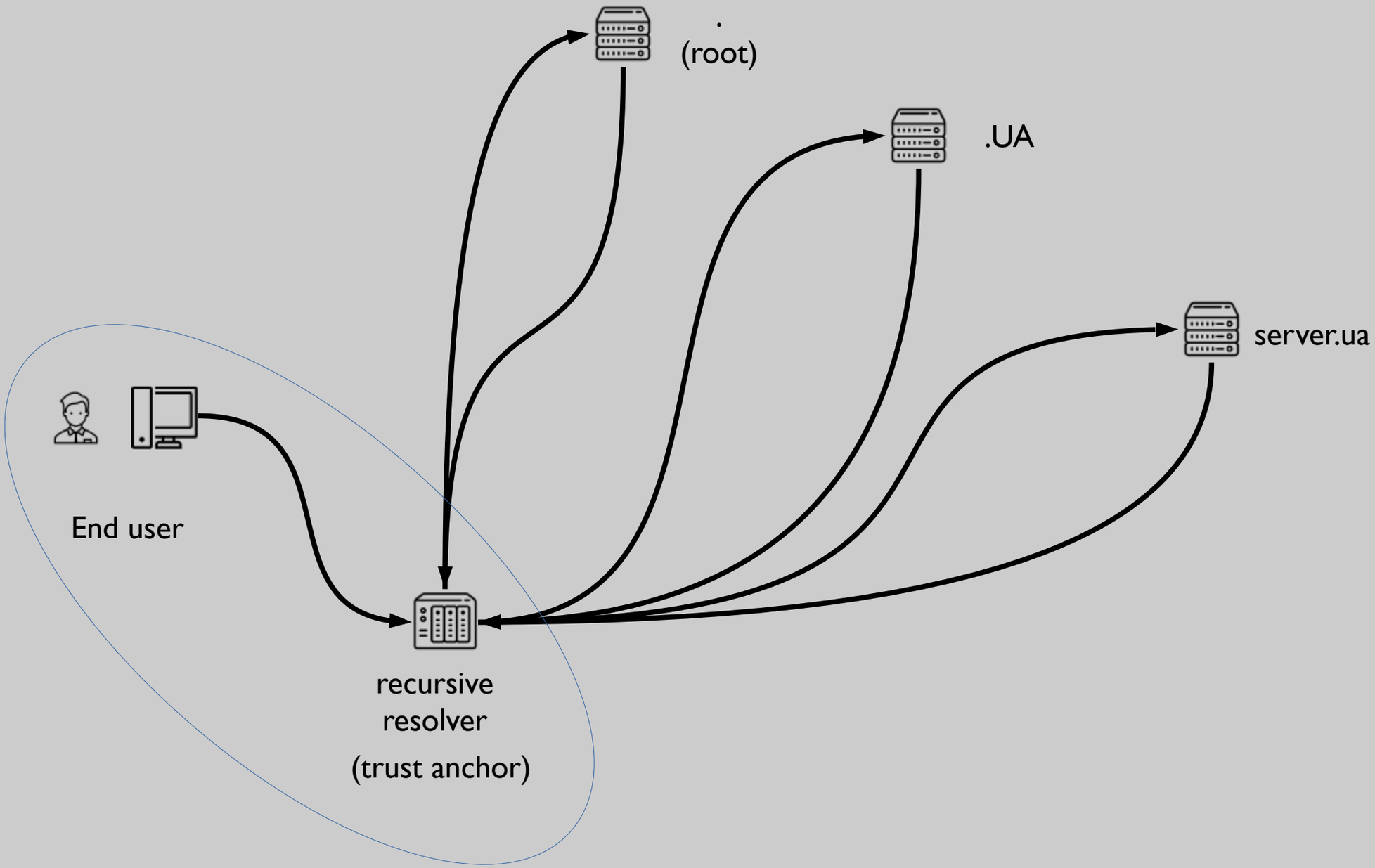
and other DNS security

Taras Heichenko
tasic@academ.kiev.ua

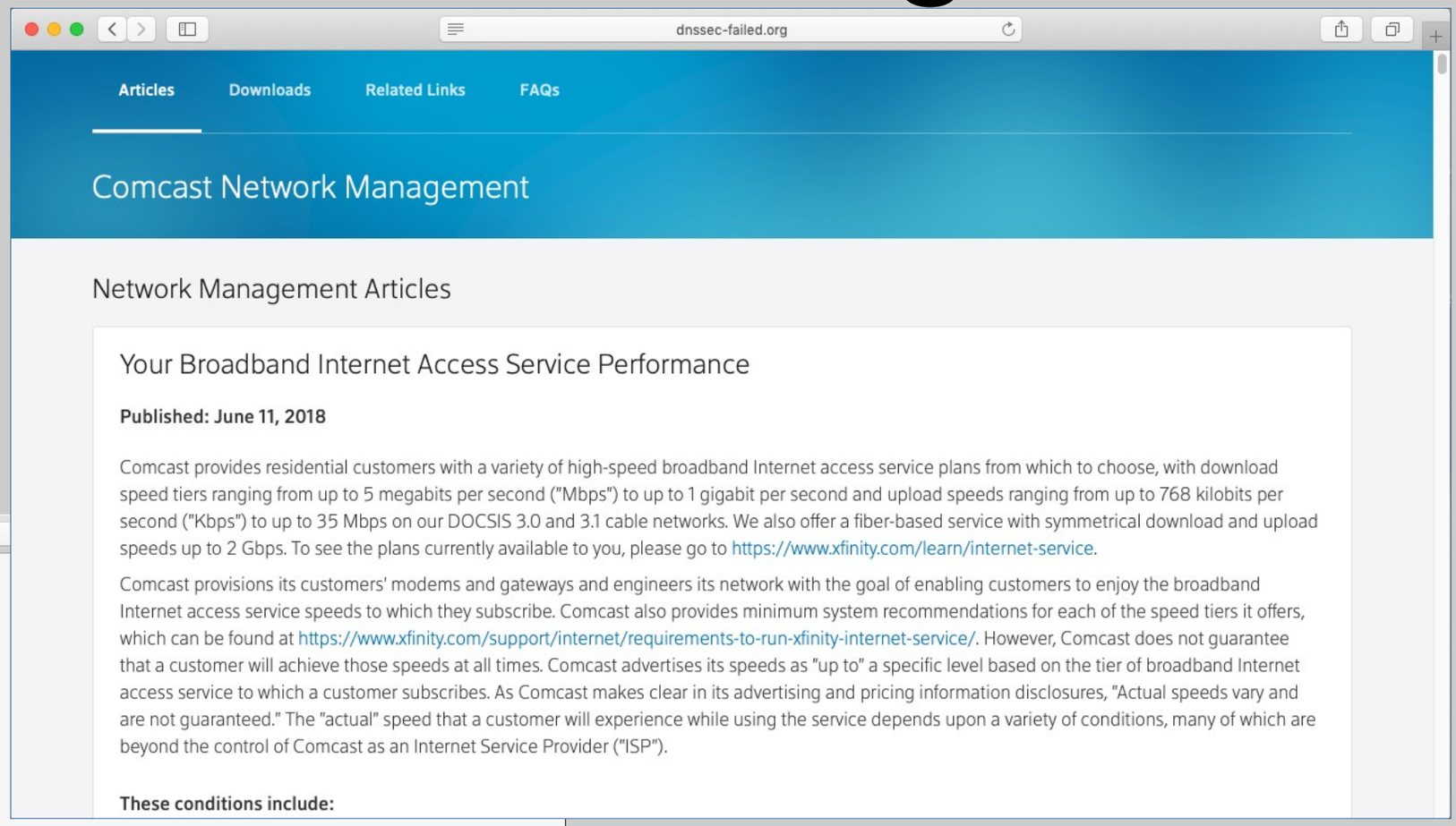
How DNS works

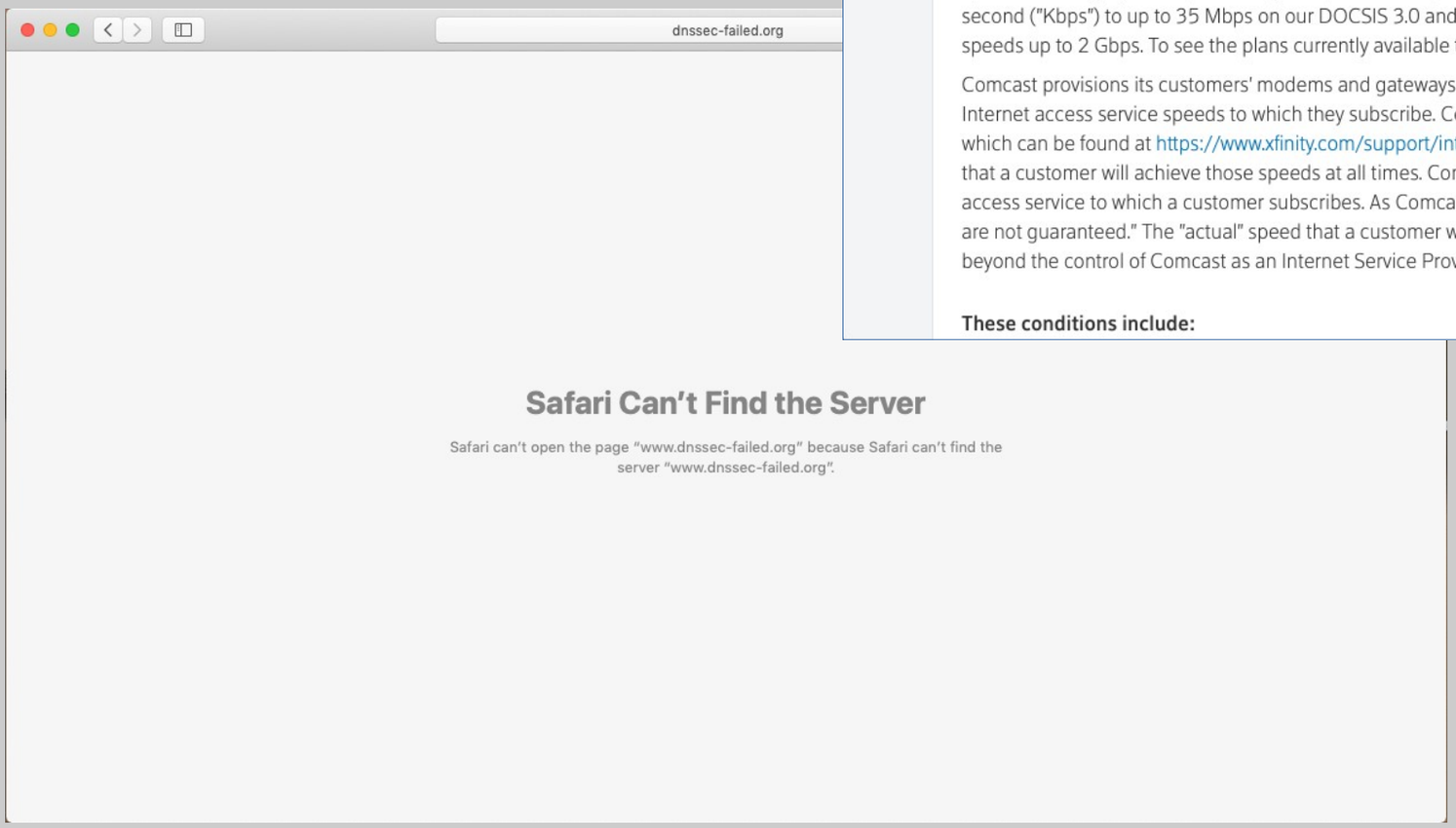


Chain of trust



Check your recursive resolver
www.dnssec-failed.org

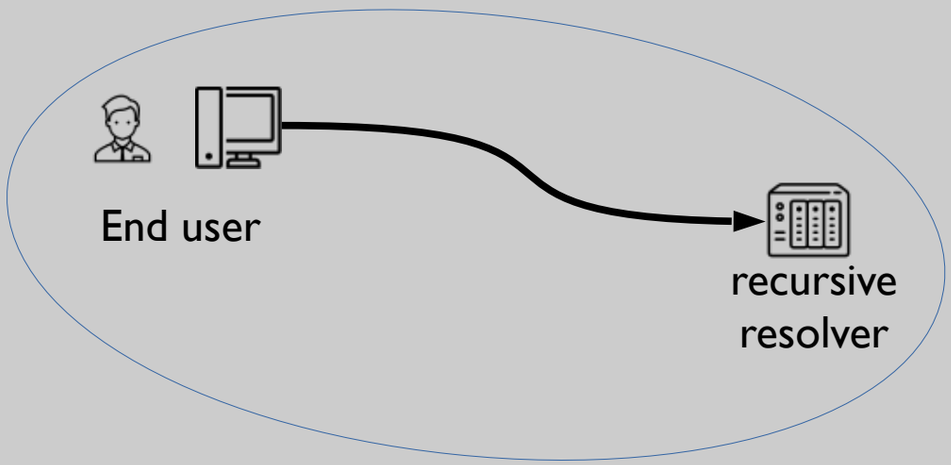




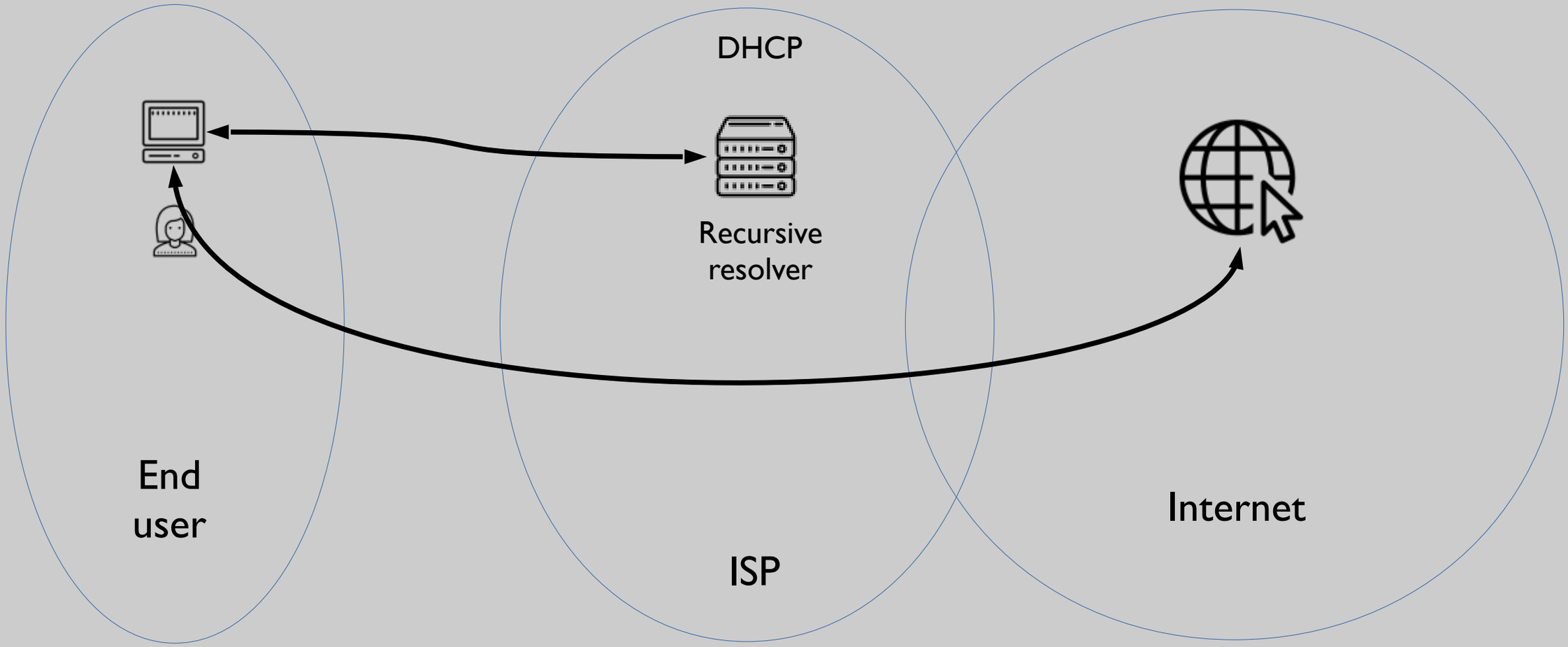
DoT & DoH – between stub and recursive

DoT – DNS over TLS
DoH – DNS over HTTPS

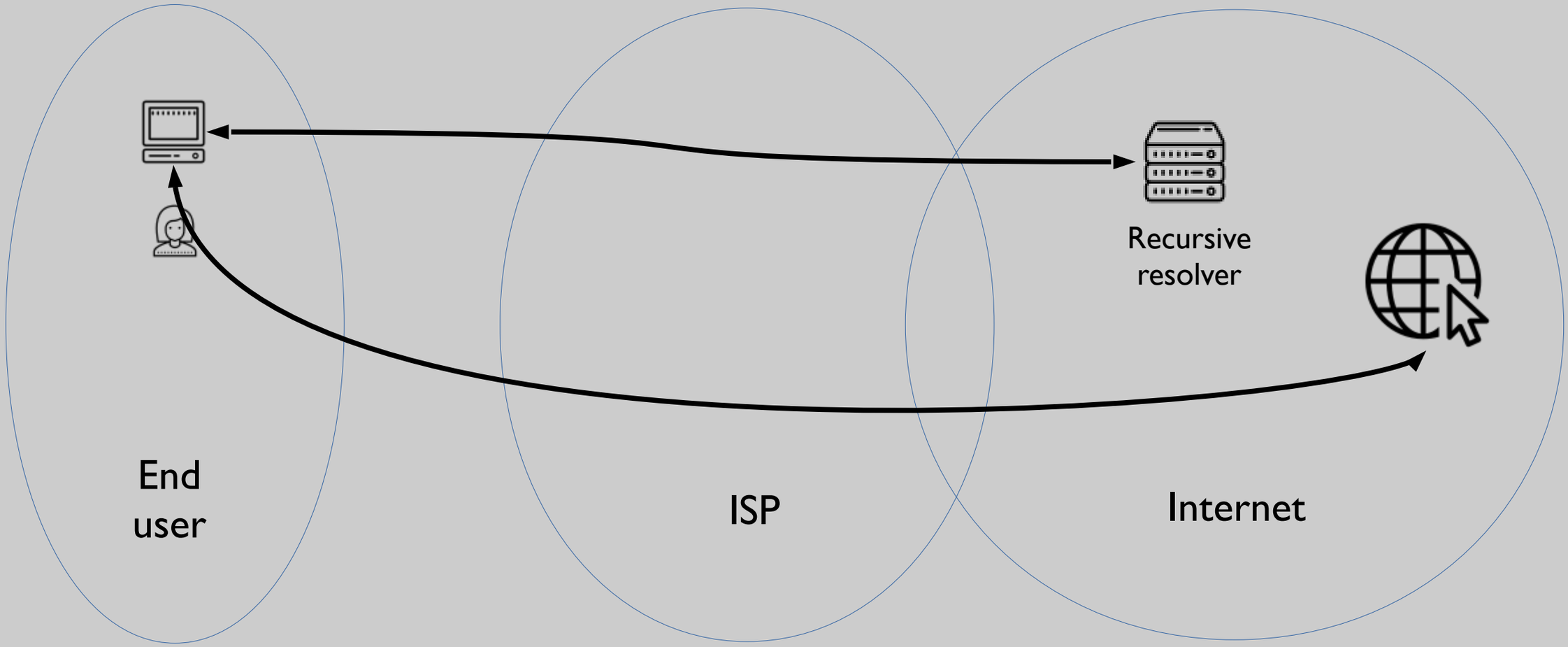
- Minimum protection – security channel between stub and recursive resolvers
- Full protection – recursive resolver authorization



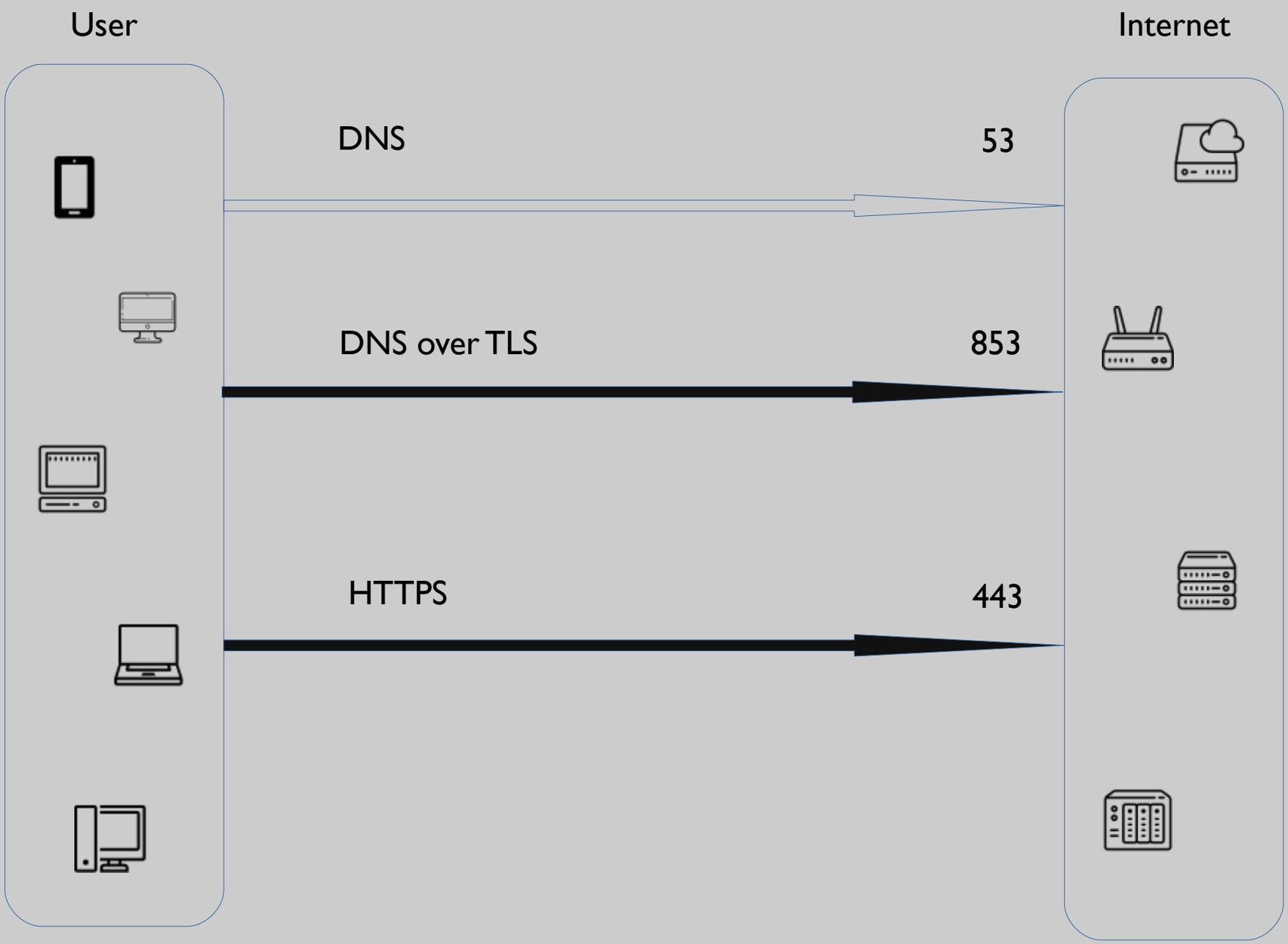
Usual DNS schema



Usual DoT or DoH schema



DoH vs DoT



Issues of protocols

DoH

- Hidden from ISP or admin
- Potentially different resolvers for each application =>different applications see different IP for the same names

DoT

- ISP can see presence of traffic
- One resolver for all system

Common for both

- Centralization => stability decreasing
- Lack of the ISP influence on recursive resolver selection
- Impossible to set ACL on recursive resolvers
- Difficulties for ISP to diagnose user problems
- Enterprise data leaks
- Difficulties for CDN localization
- Potential DNS traffic data commercialization

Google Chrome

...

The Google Public DNS anycast IP addresses are distinct from the IP addresses used to host web content for Google properties. This will allow operators to control access to the Google Public DNS DoH service on their networks without impeding access to other Google services.

…

Puneet Sood

TL/Manager for the Google Public DNS team.

- To not set the DoH resolver in Chrome by default

- The Google Public DNS privacy policy:

https://developers.google.com/speed/public-dns/privacy

Mozilla

There were not any promises to not use DoH resolver in config by default, but

network.trr.early-AAAA	default	boolean	false
network.trr.max-fails	default	integer	5
network.trr.mode	**modified**	**integer**	**5**
network.trr.request-timeout	default	integer	1500
network.trr.uri	default	string	https://mozilla.cloudflare-dns.com/dns-query
network.trr.useGET	default	boolean	false
network.trr.wait-for-portal	default	boolean	true

network.trr.mode

0 - Off (default). use standard native resolving only (don't use TRR at all)

1 - Race native against TRR. Do them both in parallel and go with the one that returns a result first.

2 - First. Use TRR first, and only if the name resolve fails use the native resolver as a fallback.

3 - Only. Only use TRR. Never use the native (after the initial setup).

4 - Shadow. Runs the TRR resolves in parallel with the native for timing and measurements but uses only the native resolver results.

5 - Off by choice This is the same as 0 but marks it as done by choice and not done by default.

DoT & DoH services

DNS over TLS

- Cloudflare
- Quad9
- CleanBrowsing

DNS over HTTPS

- Cloudflare
- Google public DNS
- CleanBrowsing

Questions?

Taras Heichenko

tasic@academ.kiev.ua