

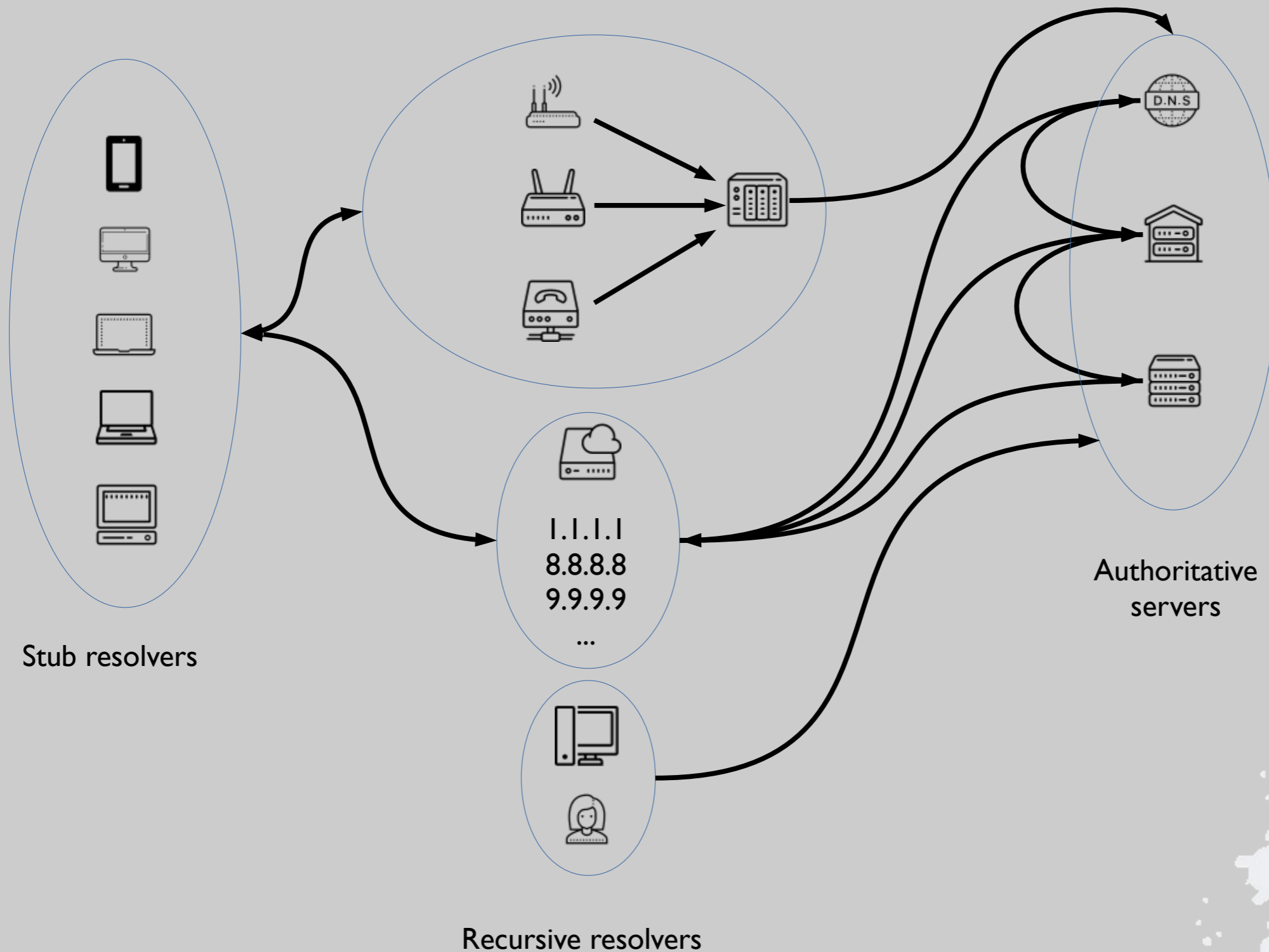
DNSSEC

and other DNS security

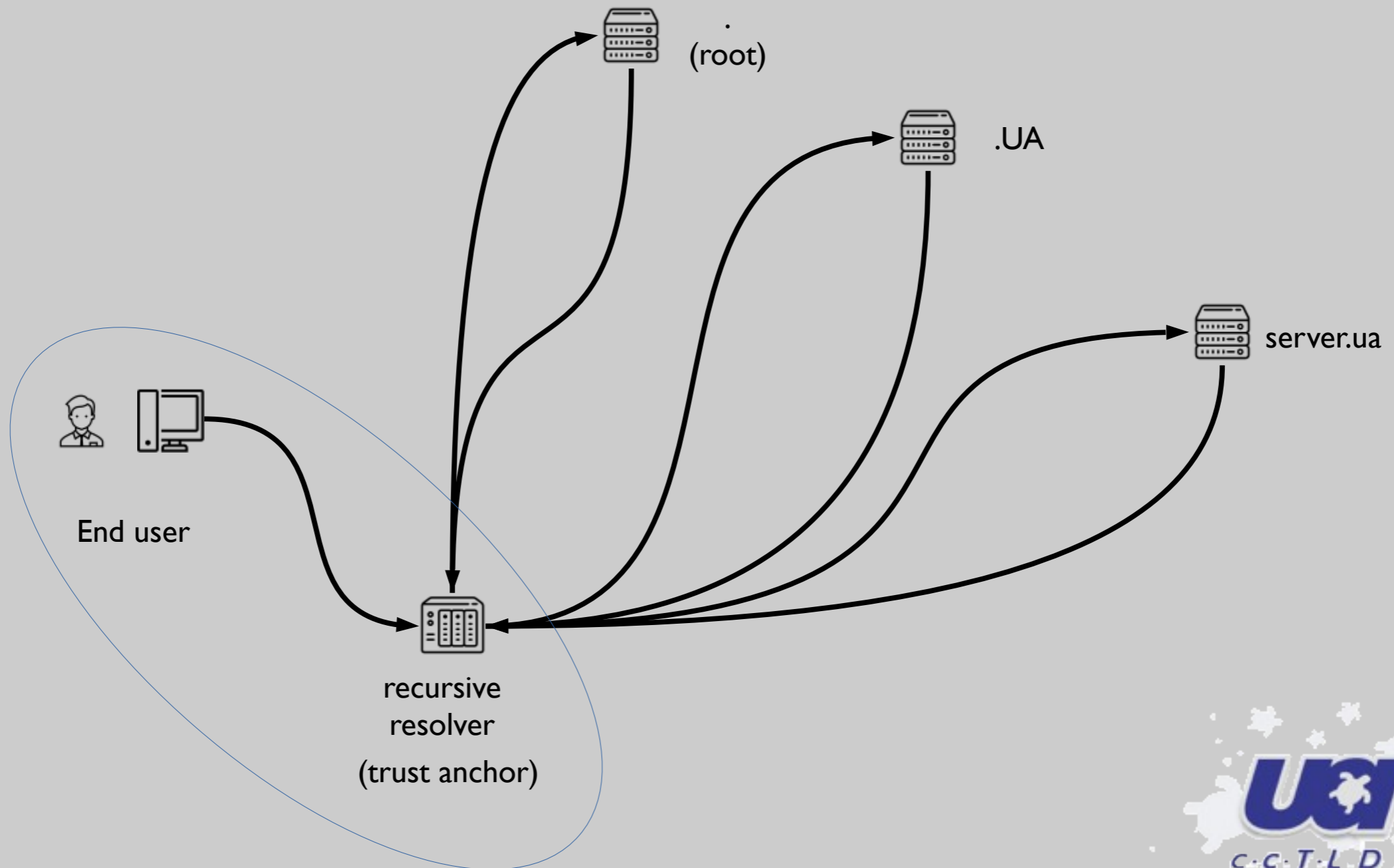
Taras Heichenko
Hostmaster



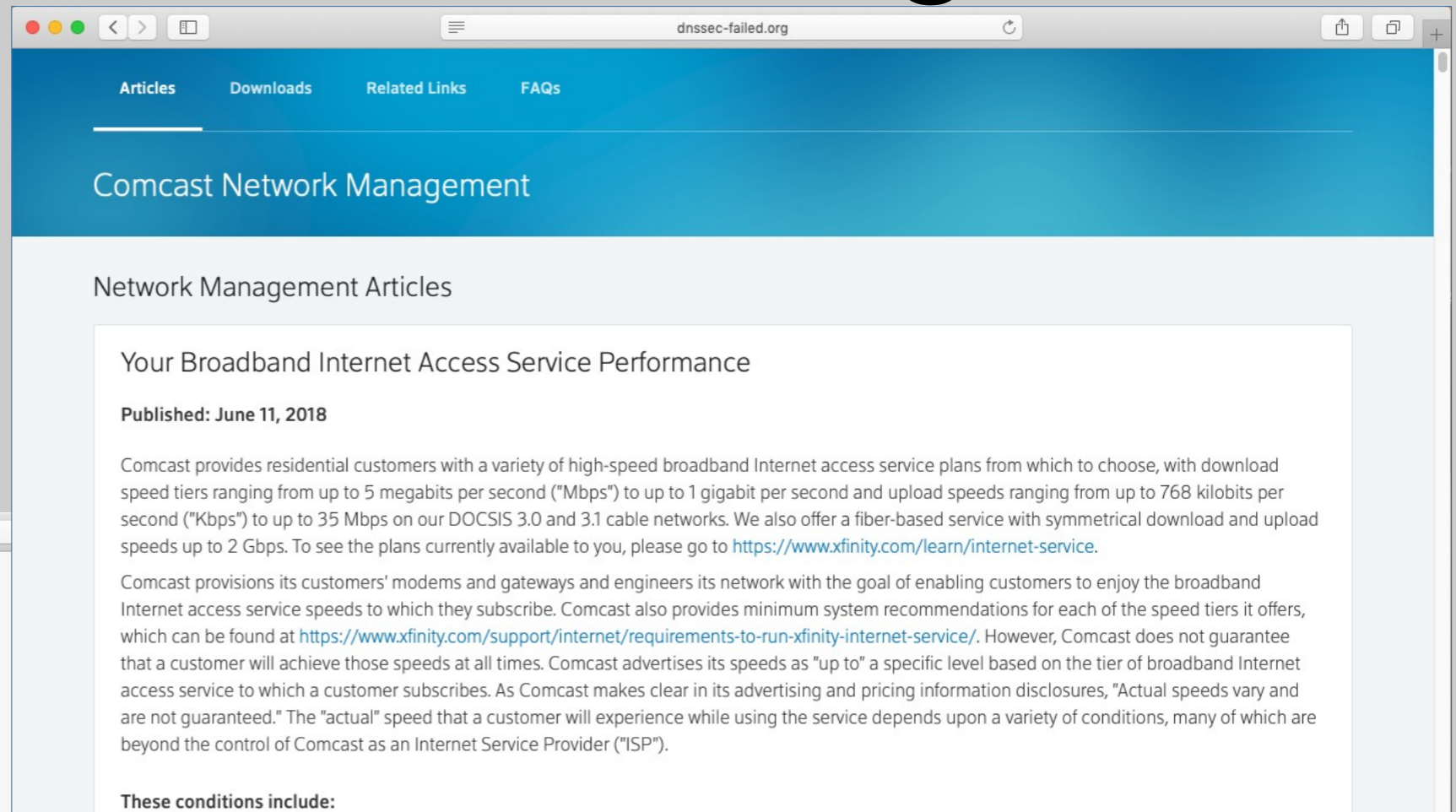
How DNS works



Chain of trust



Check your recursive resolver www.dnssec-failed.org



The screenshot shows a web browser window with the URL `dnssec-failed.org`. The page has a blue header with navigation links: **Articles**, **Downloads**, **Related Links**, and **FAQs**. Below the header is a section titled **Comcast Network Management**. Underneath, there is a sub-section **Network Management Articles**. The main article is titled **Your Broadband Internet Access Service Performance** and was published on **June 11, 2018**. The article text discusses Comcast's residential broadband services, including download and upload speeds, and provides links to Comcast's service plans and support pages. It also mentions that Comcast does not guarantee speeds and that actual speeds depend on various conditions.

Articles Downloads Related Links FAQs

Comcast Network Management

Network Management Articles

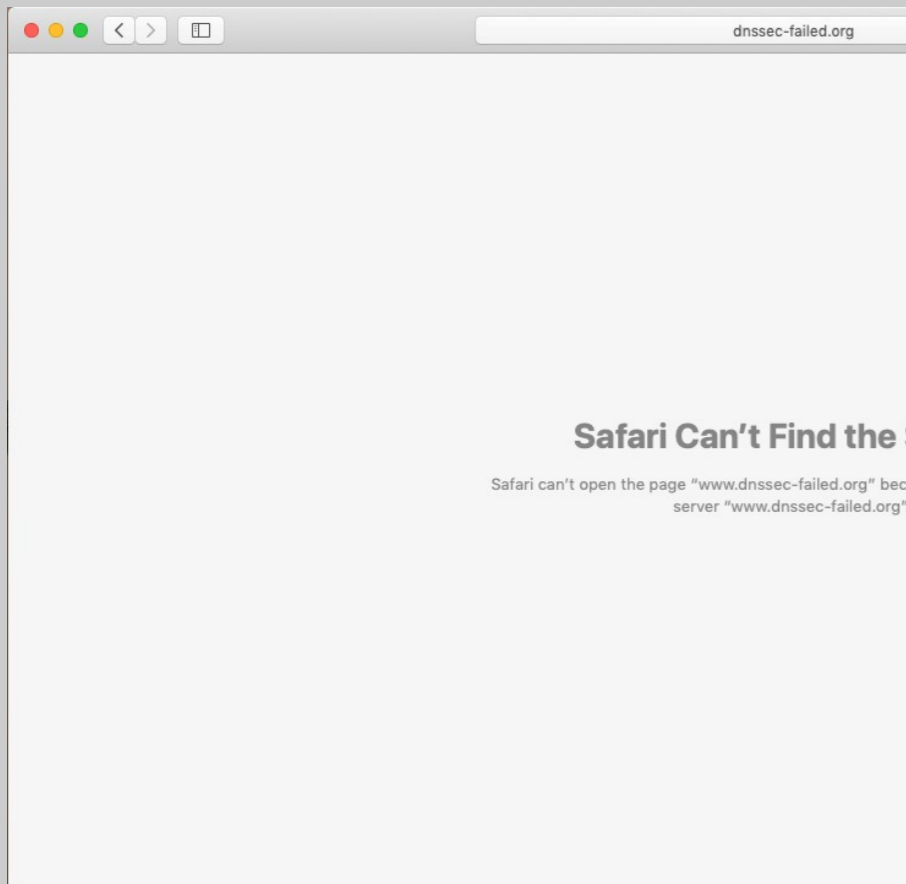
Your Broadband Internet Access Service Performance

Published: June 11, 2018

Comcast provides residential customers with a variety of high-speed broadband Internet access service plans from which to choose, with download speed tiers ranging from up to 5 megabits per second ("Mbps") to up to 1 gigabit per second and upload speeds ranging from up to 768 kilobits per second ("Kbps") to up to 35 Mbps on our DOCSIS 3.0 and 3.1 cable networks. We also offer a fiber-based service with symmetrical download and upload speeds up to 2 Gbps. To see the plans currently available to you, please go to <https://www.xfinity.com/learn/internet-service>.

Comcast provisions its customers' modems and gateways and engineers its network with the goal of enabling customers to enjoy the broadband Internet access service speeds to which they subscribe. Comcast also provides minimum system recommendations for each of the speed tiers it offers, which can be found at <https://www.xfinity.com/support/internet/requirements-to-run-xfinity-internet-service/>. However, Comcast does not guarantee that a customer will achieve those speeds at all times. Comcast advertises its speeds as "up to" a specific level based on the tier of broadband Internet access service to which a customer subscribes. As Comcast makes clear in its advertising and pricing information disclosures, "Actual speeds vary and are not guaranteed." The "actual" speed that a customer will experience while using the service depends upon a variety of conditions, many of which are beyond the control of Comcast as an Internet Service Provider ("ISP").

These conditions include:



The screenshot shows a Safari browser window with the URL `dnssec-failed.org`. The page displays an error message: **Safari Can't Find the Server**. Below the title, it says: "Safari can't open the page "www.dnssec-failed.org" because Safari can't find the server "www.dnssec-failed.org"."

Safari Can't Find the Server

Safari can't open the page "www.dnssec-failed.org" because Safari can't find the server "www.dnssec-failed.org".

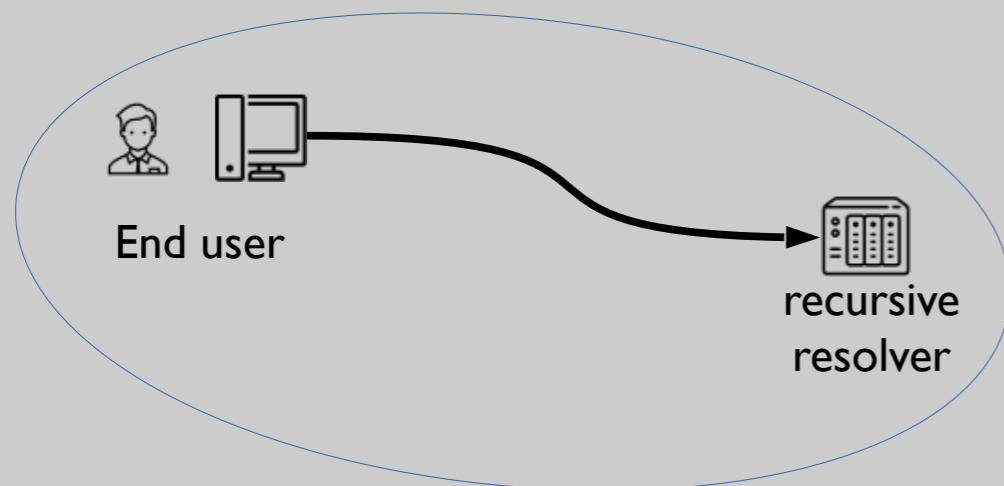


DoT & DoH – between stub and recursive

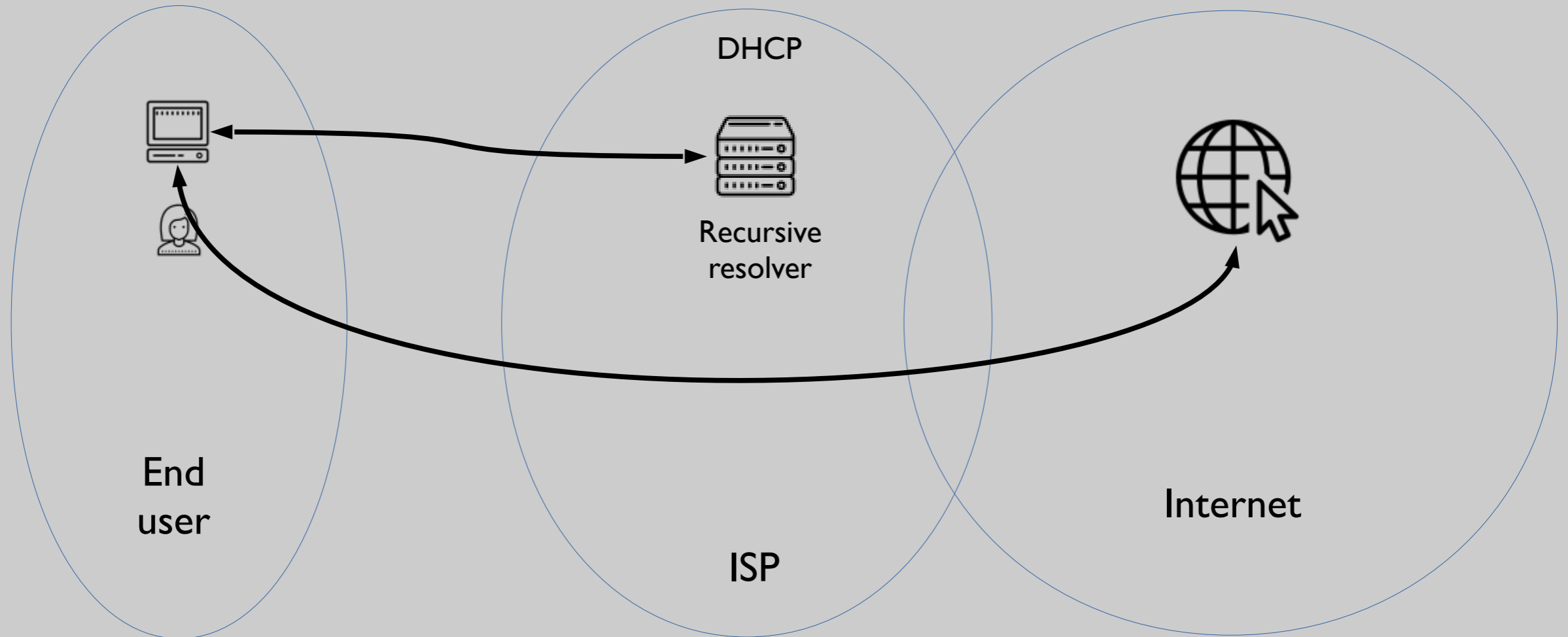
DoT – DNS over TLS

DoH – DNS over HTTPS

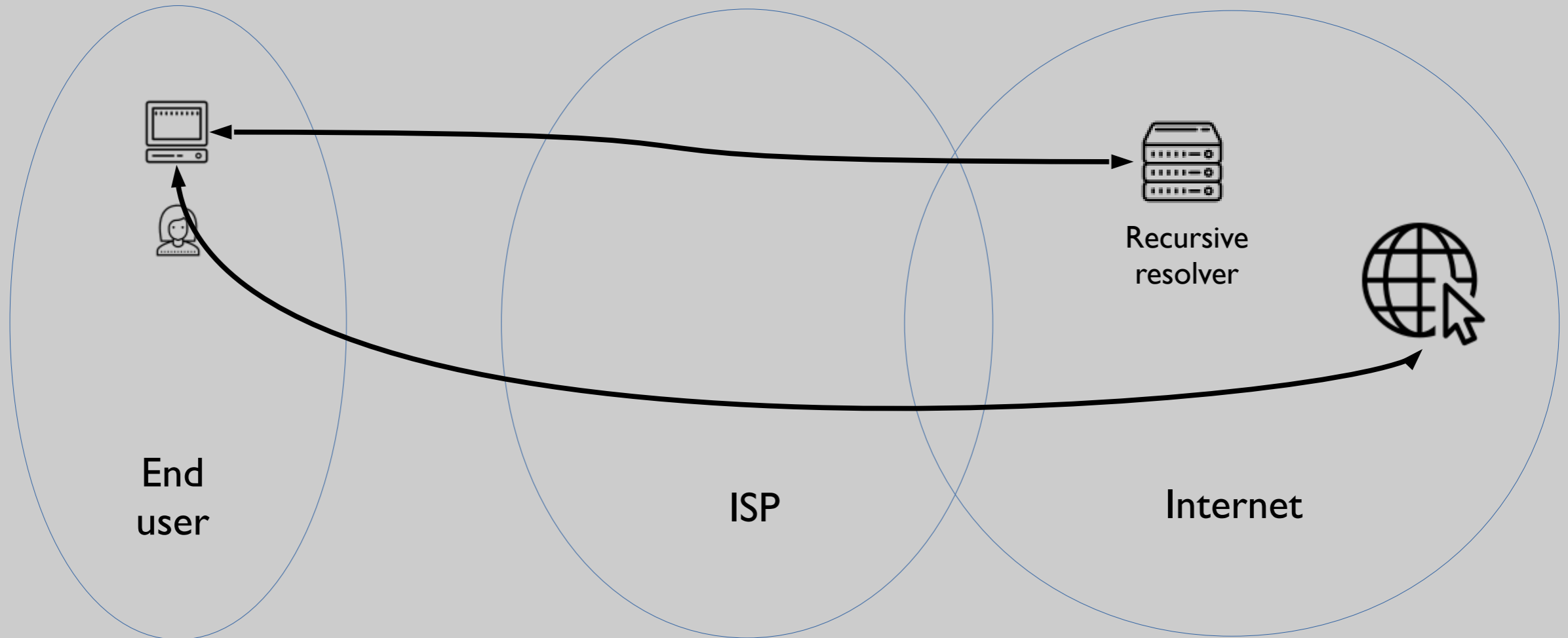
- Minimum protection – security channel between stub and recursive resolvers
- Full protection – recursive resolver authorization



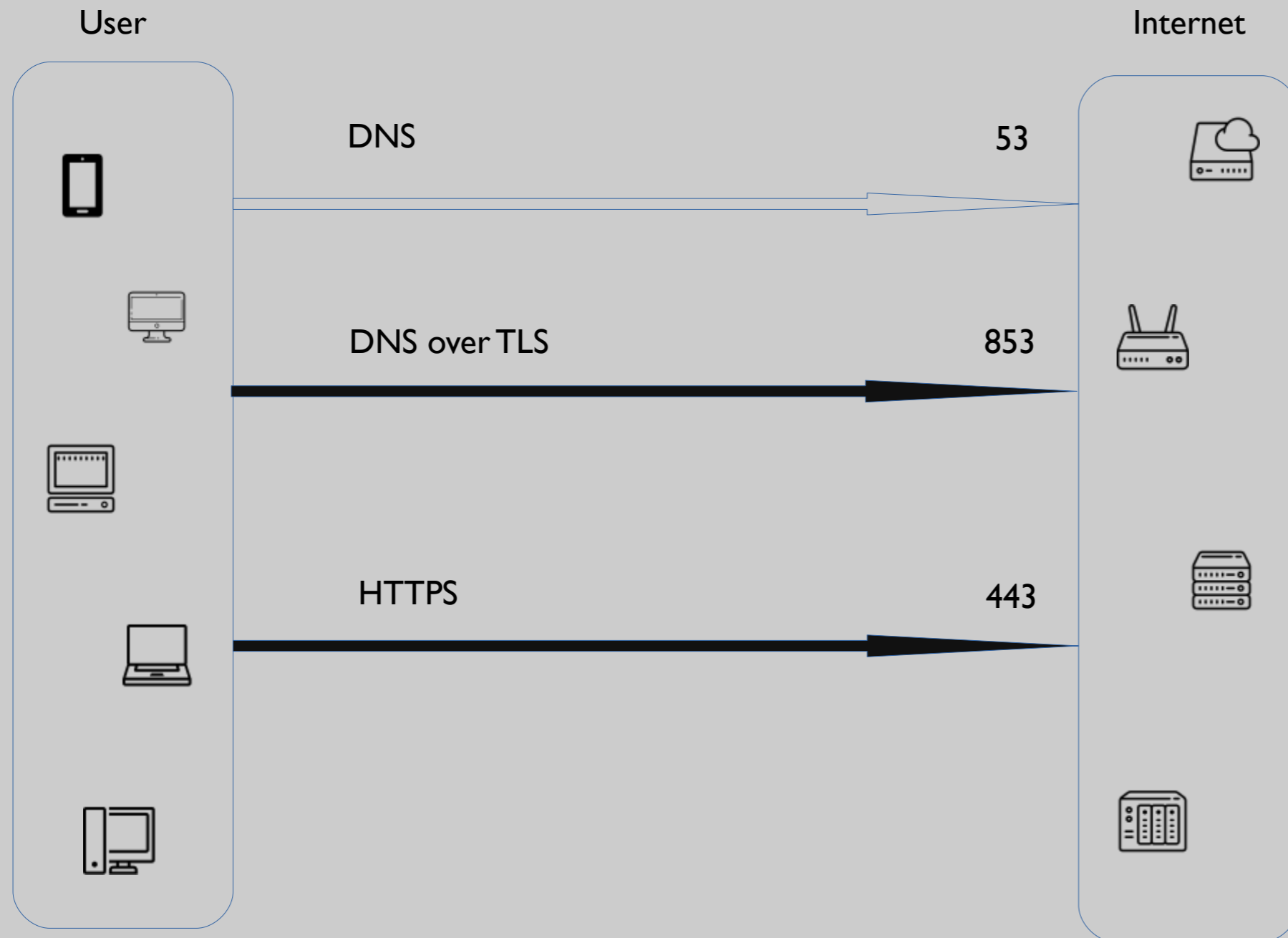
Usual DNS schema



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 и DoH services

DNS over TLS

- Cloudflare
- Quad9
- CleanBrowsing

DNS over HTTPS

- Cloudflare
- Google public DNS
- CleanBrowsing



Questions?

*Taras Heichenko
Hostmaster LLC
tasic@hostmaster.ua*

