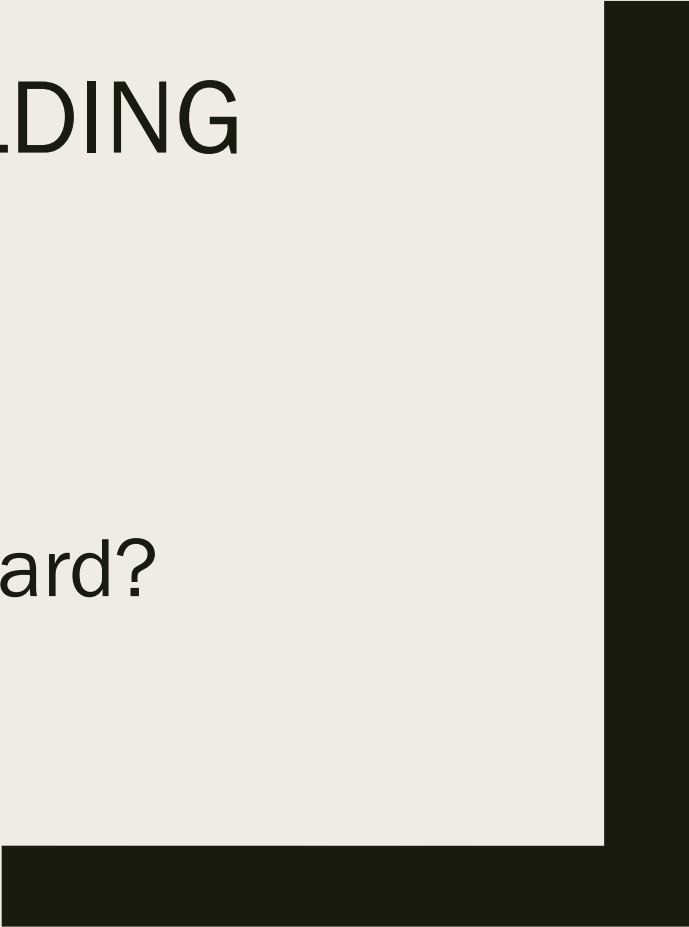




AT-LARGE CAPACITY BUILDING WEBINAR

DoH/DoT:
Steps Forward, Steps Backward?



DoH/DoT

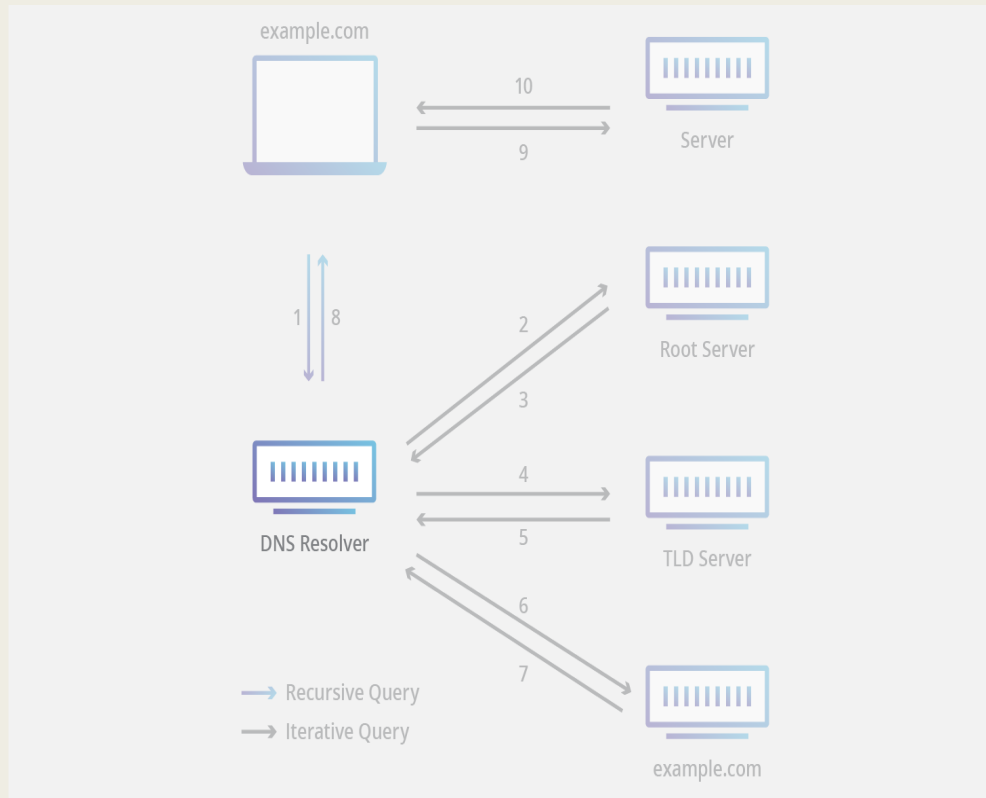
- What do they mean?
- How Do They Work
- The Benefits
- The Disadvantages
- Ways Forward?

DoH/DoT: Basic Terms

- DNS messages – DNS is a query/response protocol in which every transaction is started by a DNS query from a client and is finished by a DNS response from a resolver or authoritative server. Each DNS query and each DNS response is a DNS message.
- *DoT* – Domain Names over Transport Layer Security (TLS). The TLS protocol aims primarily to provide privacy and data integrity between two or more communicating computer applications
- *DoH* – Domain Names over Hypertext Transfer Protocol secure (HTTPS) - the secure version of HTTP, the primary protocol used to send data between a web browser and a website
- *Middlebox* – A system in the network between a client and a server that observes and possibly modifies traffic. In this document, middleboxes are usually firewalls operated by network managers to protect users and system assets in their network.

Paul Hoffman, *Local and Policy Implications of Encrypted DNS*

The basics



- DNS (<https://atlarge.icann.org/alac>) typed into browser
- Recursive resolver queries root server – response returned to recursive resolver
- Recursive resolver query to TLD server response returned to resolver
- Recursive resolver query to name server(s) – final response returned to authoritative resolver
- Packets to the address (the final response)
- Without further protection, all of the text in red UNENCRYPTED

The threats/benefits???

Growing awareness of threats and benefits to the 'classical' look up process

- Even with DNSSEC, TLS and other security measures, the **look up process** was still unencrypted
- DNS Abuse: Man in the middle, spoofing, etc
- Privacy - collection of data without consent (or even knowledge) - particularly after Edward Snowden, and how much data was being collected.
- Controls/filtering

DoT/DoH

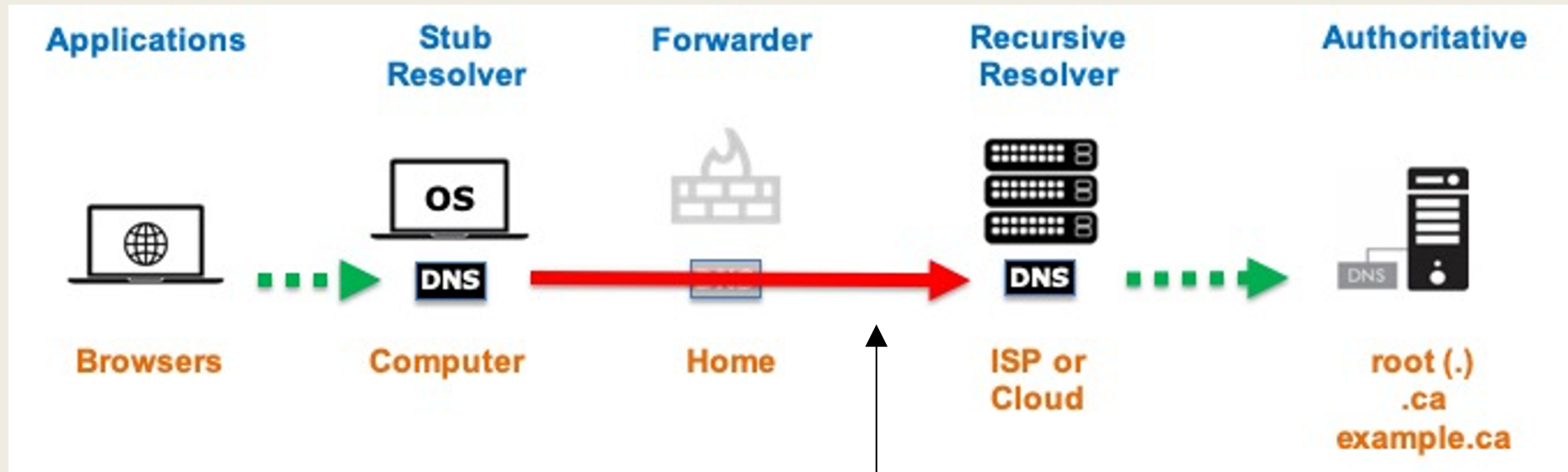
- The only change by either DoT or DoH is the use of **encrypted transport on the look up process.**
- Neither of the two protocols change the queries and responses nor to the mechanism used to build the responses (DNS resolution).
- Any changes beyond the use of encrypted transport are a result of implementation and deployment choices, and not of the DoT and DoH protocols themselves.

DoT: DNS over the Transport Layer Security

- Developed by the IETF in 2016
- DoT uses the same message structure as classic DNS, but adds encryption with Transport Layer Security (TLS) to DNS packet exchanges. Currently, DoT only defines how to encrypt DNS traffic **between end user's computer and recursive resolver, not between recursive resolvers and authoritative servers, and not between authoritative servers.**
- Designed primarily as a more private transport for DNS messages for operating systems.

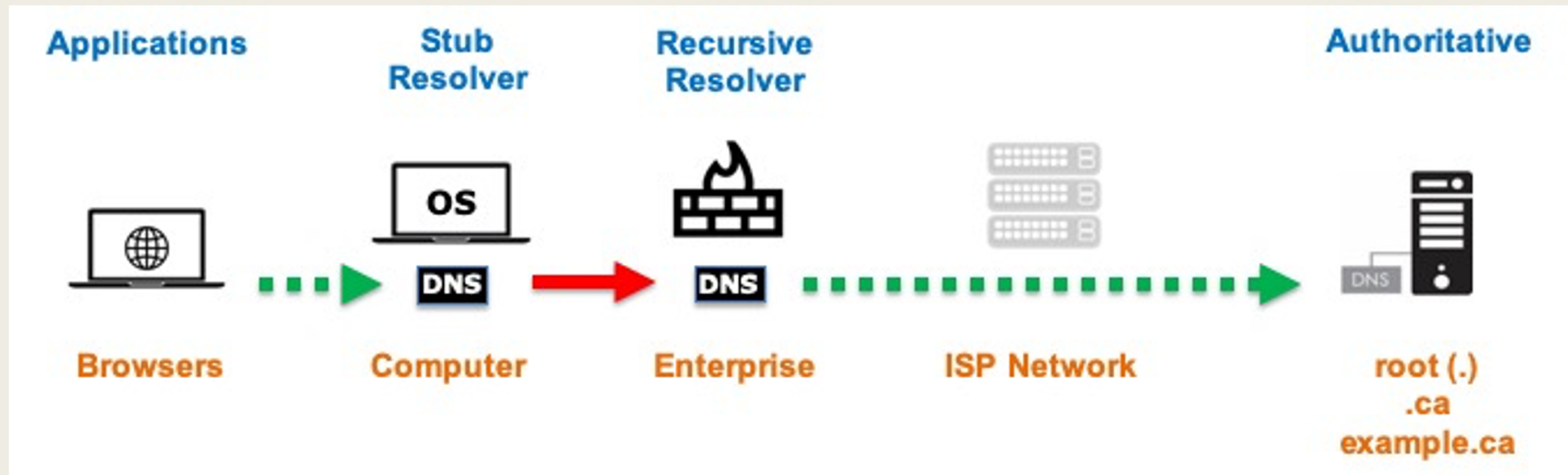
Paul Hoffman, Local and Internet Policy Implications of Encrypted DNS

Possible DNS over TLS Deployment in a Home Network



(red solids show encrypted paths)

Possible DNS over TLS Deployment in an Enterprise Network



DoH: DNS over HTTPS

Developed by the IETF in 2018

- DoH is “DNS messages wrapped in HTTP messages, transported over HTTP over TLS.”
....DoH has some operational and security properties that made it significantly more attractive to browser vendors than DoT, such as allowing servers to push DNS responses before being requested. DoH is primarily designed to encrypt DNS traffic for applications, such as web browsers on end users’ computers

Paul Hoffman

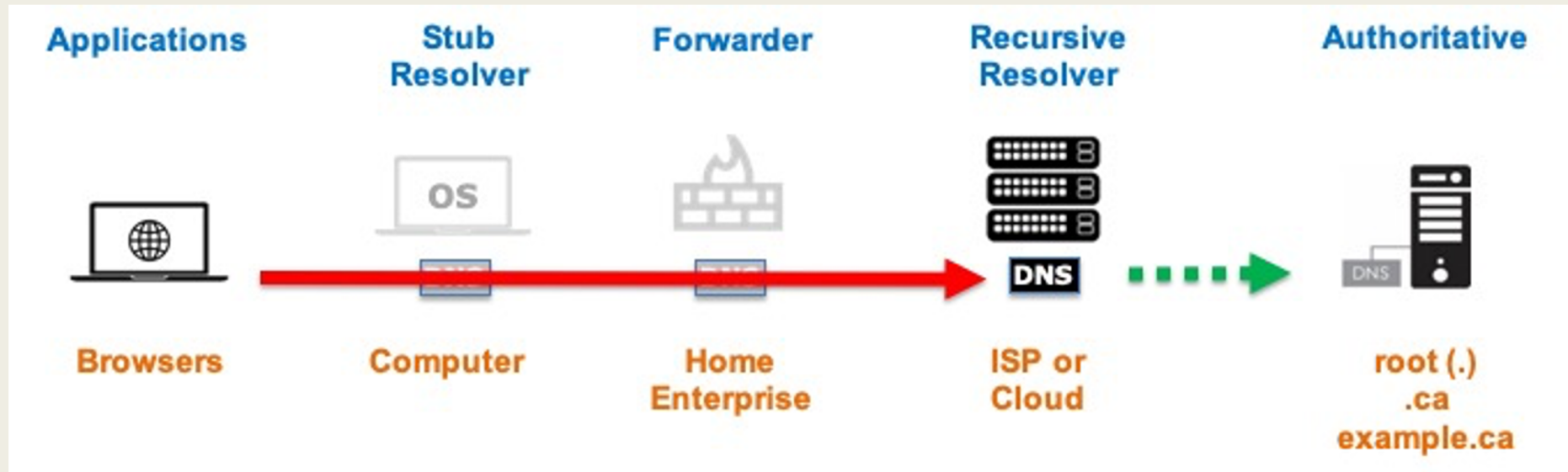
- DoH also provides some ability to hide DNS transactions in a stream of activity related to other protocols and content, defeating some metadata collection.

SSAC 109

- If DOH is in use, the content of a DNS query is visible only to the users’ browsers and the DNS resolver, not to third parties between them on the network

US Congressional Research Service

Possible DNS over HTTPS Deployment



DoT/DoH - Differences

Another important distinction between DoT and DoH is that DoT uses well known TCP port 853 by default, while DoH makes use of HTTPS port 443. Thus, **DoT can be identified and blocked by intermediaries such as network administrators.** Many firewalls block all ports by default and only white list specific well-known ports such as port 443 for HTTPS. DoT adoption may face obstacles because deployed firewalls and other middle boxes will not permit traffic on TCP port 853 to leave the network, thereby blocking the query traffic.

DoH is designed to be indistinguishable from normal HTTPS to the same server, making it harder to block by intermediaries. All DoH traffic cannot be blocked without potentially blocking other important HTTPS traffic if a server handles both DoH and regular web traffic.

DoT/DoH: Understanding?

My Lords, I thank the Minister for that Answer, and I apologise to the House for this somewhat geeky Question. This Question concerns the danger posed to existing internet safety mechanisms by an encryption protocol that, if implemented, would render useless the family filters in millions of homes and the ability to track down illegal content by organisations such as the Internet Watch Foundation. Does the Minister agree that there is a fundamental and very concerning lack of accountability when obscure technical groups, peopled largely by the employees of the big internet companies, take decisions that have major public policy implications with enormous consequences for all of us and the safety of our children? What engagement have the British Government had with the internet companies that are represented on the Internet Engineering Task Force about this matter?

Baroness Thornton, House of Lords 14 May 2019

DoH/DoT: The pluses - Privacy

For both DoT and DoH –the information on where YOU are going is encrypted

- For DoT: the connection between you and the recursive resolver
- For DoH: the look up trip is over HTTPS

DoT/DoH: The pluses - Security

- DNS queries can be intercepted to manipulate legitimate traffic, make services unavailable or cause delay, harvest information like credentials or emails, or cause a range of other malicious activities – PREVENTED by encryption

DoT/DoH: Filtering – benefits (or not)

can prevent

- Visiting websites that install malware
- Getting email from servers that typically send malware
- Communicating with malware servers after being infected

Parents can use controls to protect against sites

Governments – can require blocking of sites

Enterprises – may monitor the exfiltration of material

BUT

- Can prevent communications by dissident groups
- Can access information on sites visited, etc

DoH/DoT: Centralization of DNS Resolution

Benefits:

- ease of configuration
- having just a single set of DNS policies to understand
- larger caches leading to faster responses.

Negatives:

- making the resolver a more interesting target for those who want to surveil DNS traffic
- making the resolver a more interesting target for denial of service,
- unnoticed malicious actions by the resolver operators
- slower web traffic due to geographic misidentification.

DoT/DoH – Users

- Mozilla – has its Trusted Recursive Resolver (TRR) program. Currently, only uses Cloudflare and NextDNS as part of its program
- Being tested by Google Chrome
- Google’s Android operating system, which is popular on many cell phones and tablets, was the first to support automatic encryption of DNS traffic
- In November 2019, Microsoft announced plans to start supporting automatic encryption in the Windows operating system using DoH.

Solutions???

(from Hoffman paper)

- Encrypted DNS messages cannot be read by middleboxes that filter or monitor, so that filtering or monitoring becomes impossible by those middleboxes, **unless a middlebox and the associated computers are configured in such a way as to provide the middlebox with the key to decrypt TLS traffic.** Filtering and monitoring can be done on resolvers because those resolvers are an endpoint for the encrypted DNS traffic and thus the traffic would be unencrypted by the resolver.
- Note that a middlebox still knows the endpoints of the traffic. For example, if a resolver that supports DoH and/or DoT has one or more known IP addresses, a middlebox can assume that encrypted traffic to those addresses is DNS traffic and **can enforce local policy**, such as blocking encrypted traffic to those addresses.

References for DOH/DoT

ICANN meetings of DoH/DoT

12 March 2019, at 1515 hrs and 10 March 2020 at 1300 hrs

- <https://meetings.icann.org/en/>

Paul Hoffman's Paper

- <https://www.icann.org/en/system/files/files/octo-003-en.pdf>

SSAC Paper #109

- <https://www.icann.org/groups/ssac/documents>

Council of European National Top-Level Registries (CENTR), *CENTR Issue Paper on DNS over HTTPS*, 17 June 2019

US Congressional Research Service, *DNS over HTTPS—What Is It and Why Do People Care?*, 16 October 2019

- <https://crsreports.congress.gov>

The image features two large, thick, black L-shaped corner brackets. One is positioned in the top-left corner, and the other is in the bottom-right corner. They are oriented towards each other, framing the central text.

THANK YOU