Creating Infinite Possibilities.

SCTE
a subsidiary of CableLabs

Encrypted DNS from Pilot to Production

Joe Crowe

Principal Engineer
Comcast Cable
joseph_crowe@comcast.com

SCTE CABLE-TEC EXPO 22
SEPTEMBER 19-22 • PHILADELPHIA, PA

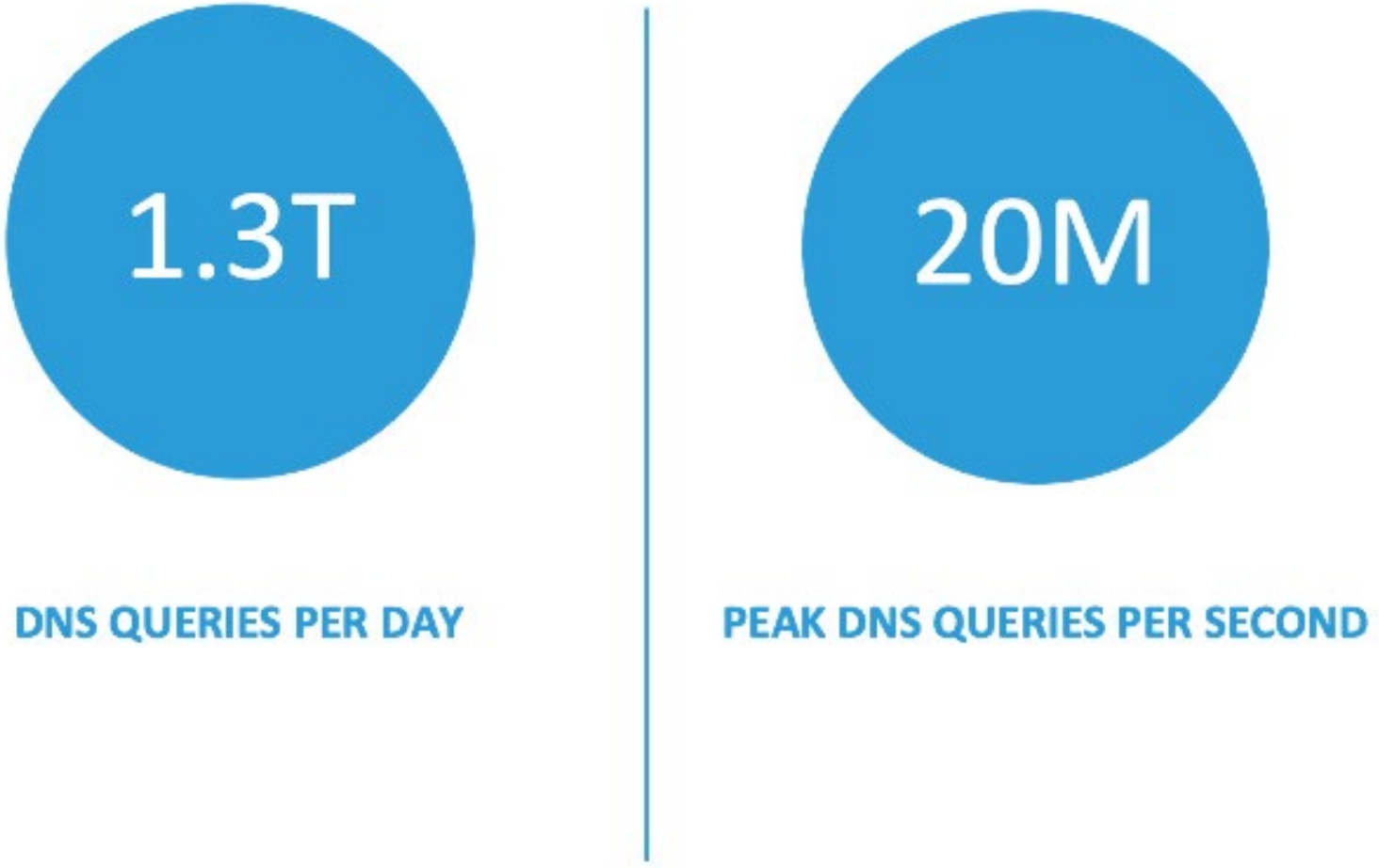
2022 Fall Technical Forum
SCTE • CABLELABS • NCTA

DNS in a nutshell

- Critical internet service for most networked applications that use fully qualified domain names
- Translates human readable domain names to IP addresses
- Inherently insecure

Image Credits: Cosmic Jans/Flickr under a CC BY 2.0 license.

Current scale of Comcast's DNS



RFC 8484

- Originally presented as an IETF RFC draft in 2017 by P. Hoffman (ICANN) and P. McManus (Mozilla)
- Outlines the requirements for DNS over HTTPS, a DNS protocol that uses port 443 to encrypt and hide DNS traffic
- October of 2018 was adopted as RFC 8484
- 2019 adopted by Mozilla and Cloudflare to make as default “opt-out” in the Firefox browser

Image Credits: Ryan Somma/Flickr under a CC BY 2.0 license.

Key points of DNS over HTTPS

Lose visibility

- DoH utilizes port 443
- Same port that HTTPS uses
- Hard to distinguish traffic type between the two protocols
- Client software can send DoH traffic to any endpoint of their choosing
- Possibility to break some services that Comcast offers

No auto-discovery of DoH

- Unlike the DHCP offering DNS servers to clients
- Currently most clients are using a programmatic way to shape DoH traffic
- There are workshops in IETF dedicated to creating an RFC for auto-discovery of DoH

Requirements of Comcast for DoH

- Understanding of the DoH protocol
- DoH translator
- High availability
- Localized DNS responses for customers
- Solution able to handle query load

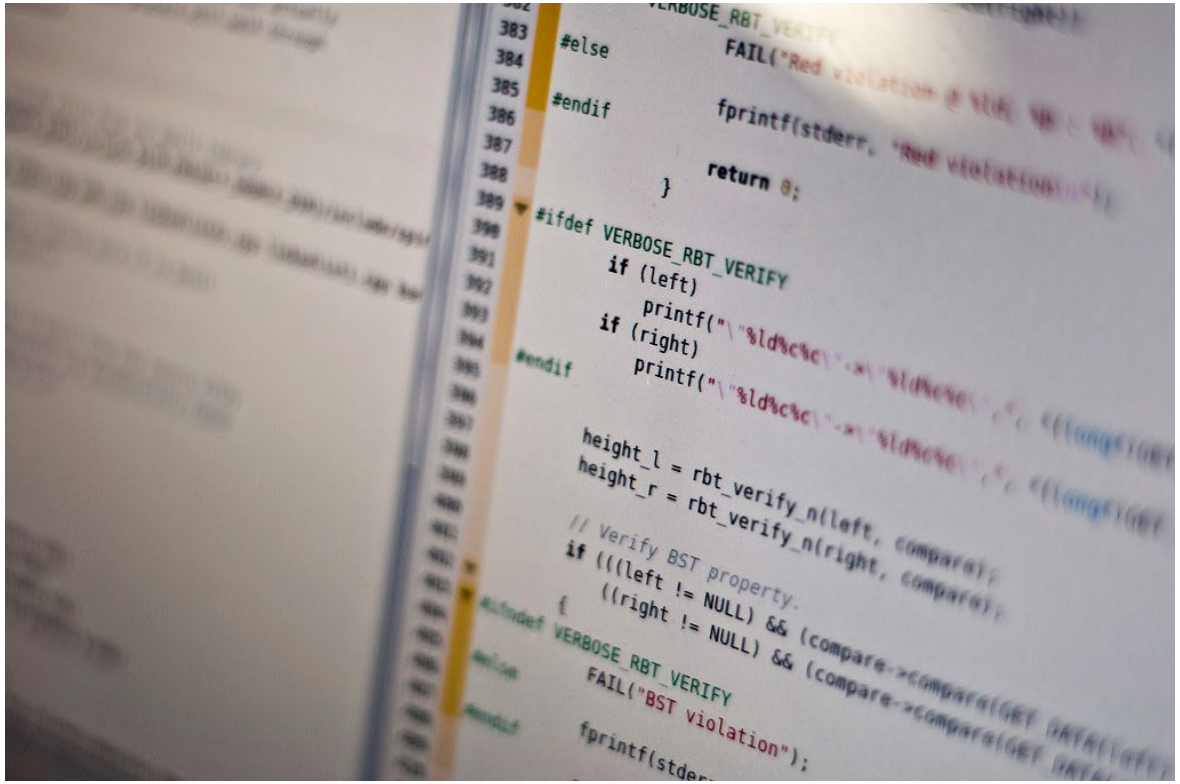
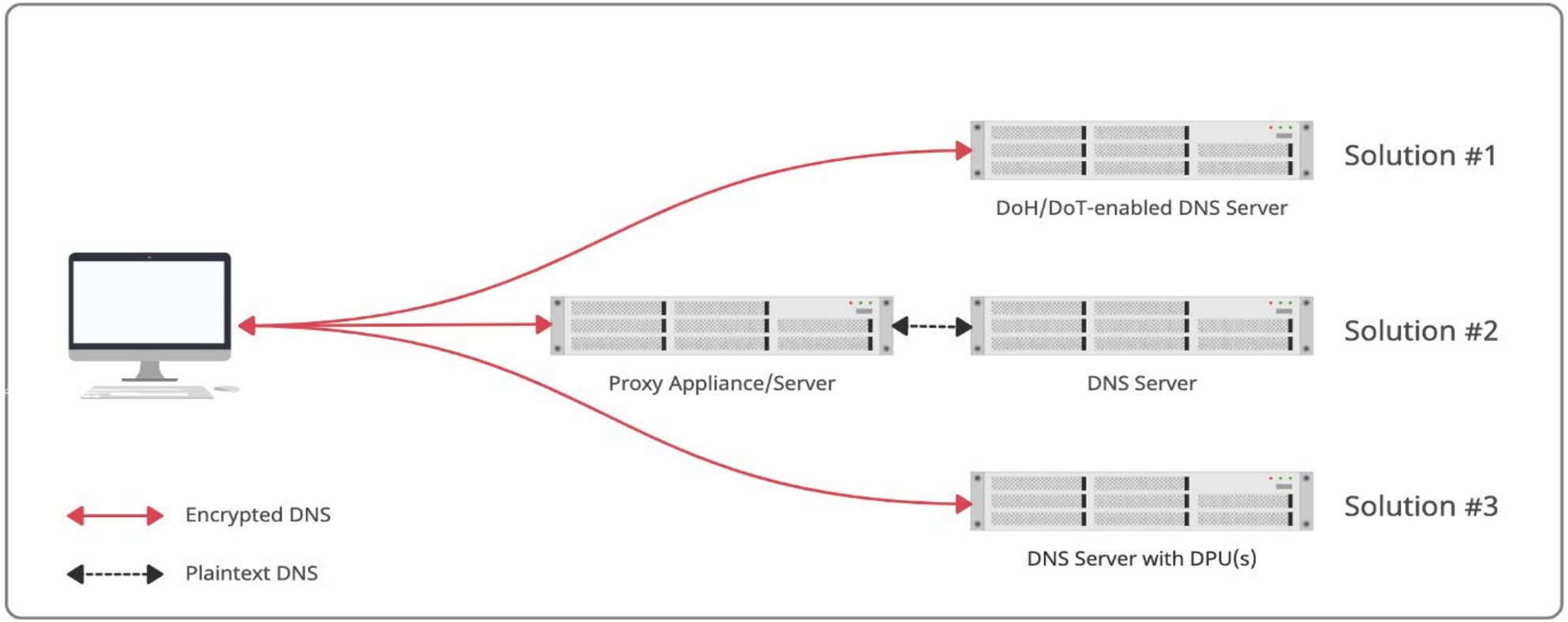


Image Credits: Michael Himbeault/Flickr under a CC BY 2.0 license.

Encrypted DNS Infrastructure Possibilities



Solution #1: Spec mismatch, adding capacity means increased space, power and possible licensing costs

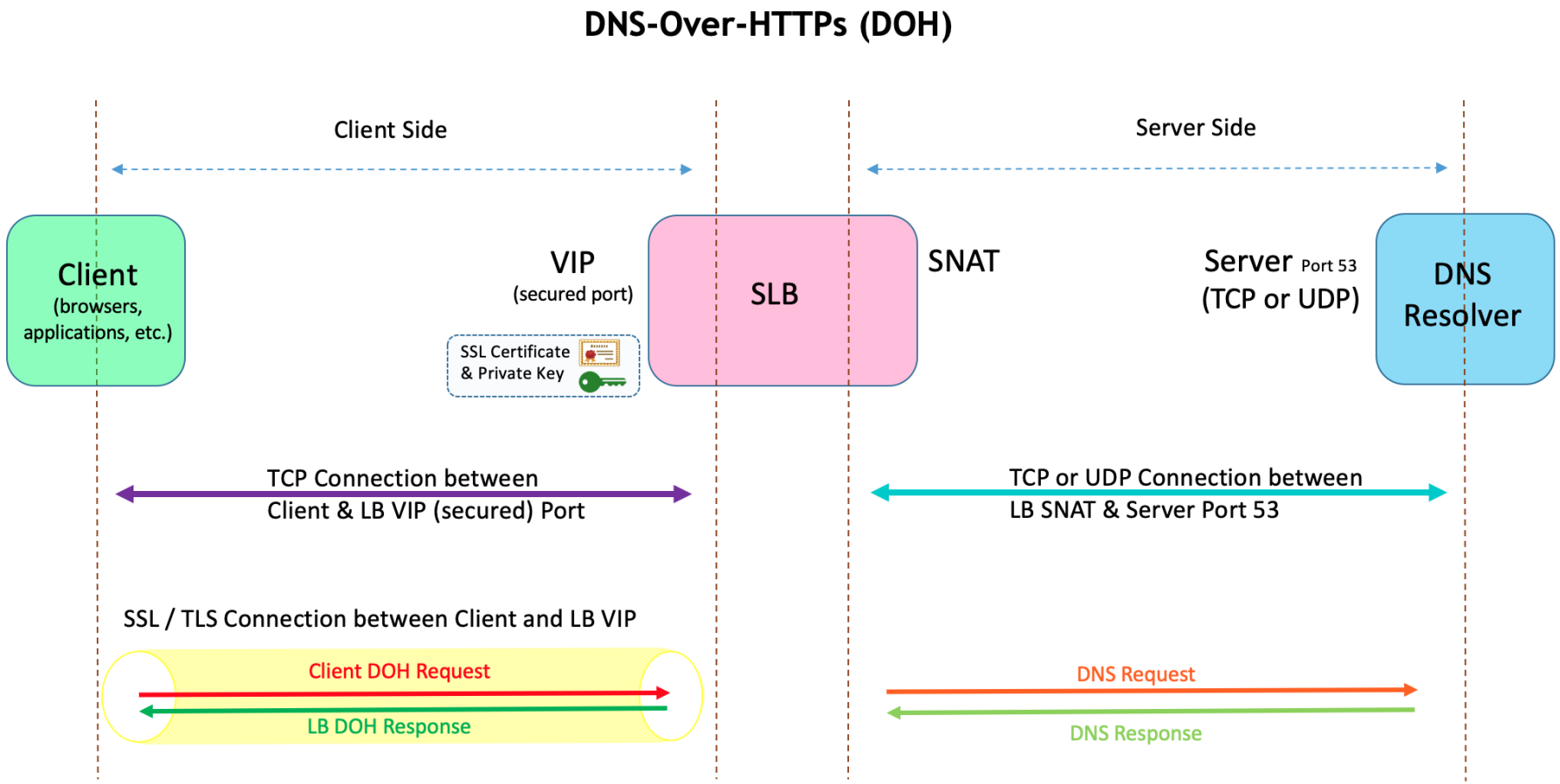
Solution #2: The current proxy appliance model is also expensive to scale.

Solution #3: Developed at Comcast, DPU upgrade, cheaper and added opportunities at the edge

Lead-up to Pilot

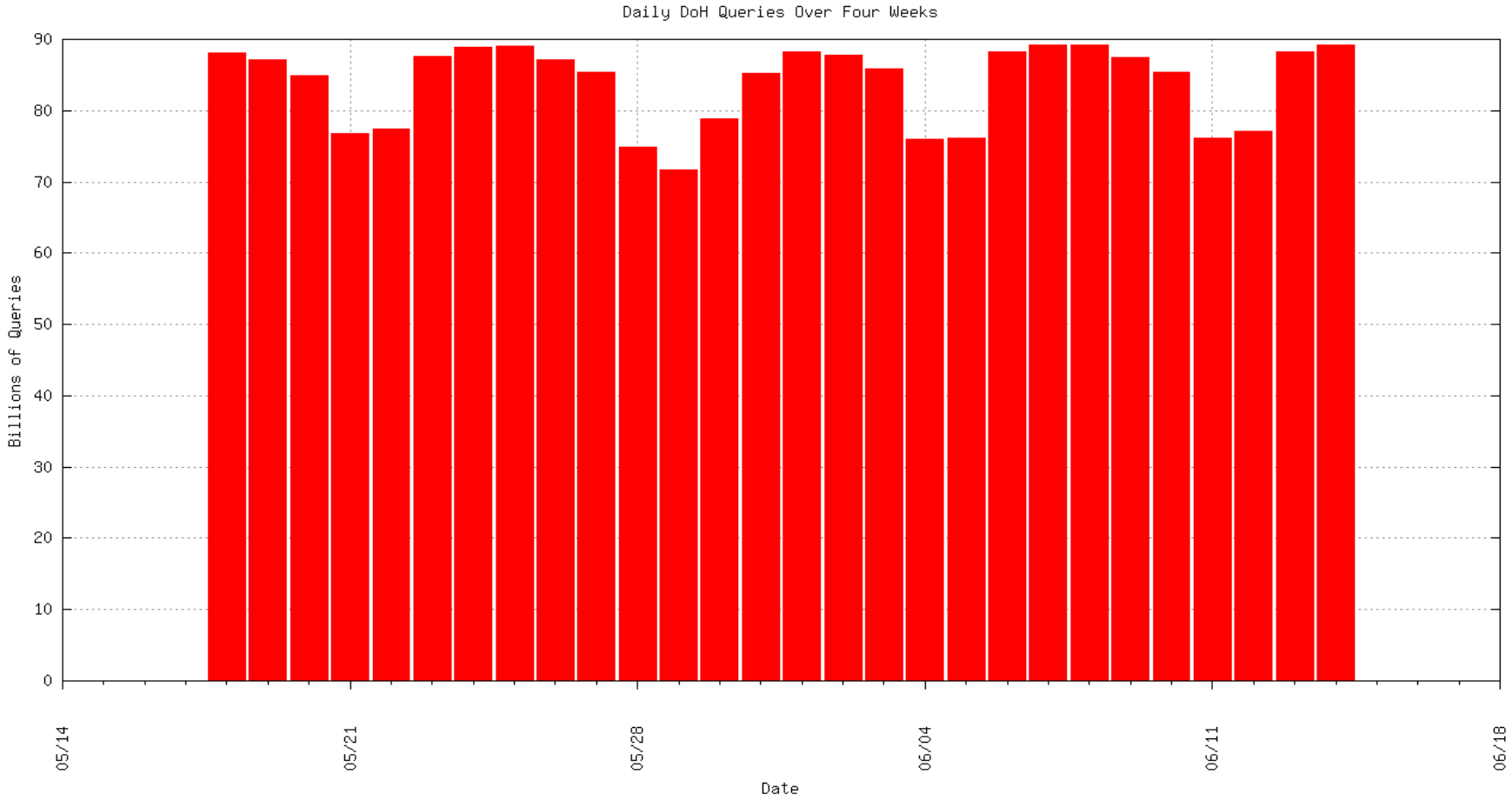
- Comcast engineers pitched a lab week project to build an in-house DoH translator
- Lab week project was put together in 2019
- Team had proven out and developed the translator
- After a better understanding conversations started with network appliance vendors

Current Production Infrastructure



Production Stats

- Current Daily DoH queries stand around 90 Billion queries in a day at peak
- This accounts for approximately 7% of overall DNS traffic
- Most traffic is coming from browsers



Comcast's Commitment to Privacy

- In 2019 Comcast offered a beta version of https://doh.xfinity.com/dns-query
- This allowed for other DNS operators to test
- After some tweaks, a commitment was to offer to all Comcast customers in Q2 2020
- Comcast released a privacy policy dedicated solely to DNS, along with updates to the internet privacy policy as a whole
- https://www.xfinity.com/privacy/policy/dns
- https://www.xfinity.com/privacy/policy

Commitment to Privacy (cont..)

- Comcast was the first major ISP to join Mozilla's Trusted Recursive Resolver program
- Comcast contributes to the Encrypted DNS deployment initiative
- Collaboration with other DNS operators helped identify and fix issues found in pilot

Future of Encrypted DNS

- As DNS software vendors test more on hardware, there is more of an opportunity to keep a translator on the same hardware as the DNS software
- Possibility of utilizing current or future hardware with data processing units (DPU)
- Keep working with other DNS operators and open-source developers to create or maintain encrypted DNS toolsets
- Keep an eye on other encrypted DNS technologies like DNS over QUIC and DNS over TLS

References

- Encrypted DNS Deployment Initiative: https://www.encrypted-dns.org
- Hoffman, P., & McManus, P. (n.d.). *DNS Queries over HTTPS (DoH).* Retrieved from RFC 8484, DOI 10.17487/RFC8484: https://www.rfc-editor.org/info/rfc8484
- Mozilla. (2020, June). *Comcast's Xfinity Internet Service Joins Firefox's Trusted Recursive Resolver Program*. Retrieved from https://blog.mozilla.org/en/products/firefox/firefox-news/comcasts-xfinity-internet-service-joins-firefoxs-trusted-recursive-resolver-program/
- Mozilla. (n.d.). *Security/DOH-resolver-policy.* Retrieved from https://wiki.mozilla.org/Security/DOH-resolver-policy
- Xfinity. (2021, October). *Our Privacy Policy explained.* Retrieved from https://www.xfinity.com/privacy/policy

Creating Infinite Possibilities.

Thank You!

Joe Crowe

Principal Engineer
Comcast Cable
joseph_crowe@comcast.com