Encrypted DNS From Pilot To Production

A Technical Paper prepared for SCTE by

Joe Crowe
Product Development Engineer 5
Comcast
1800 Arch St Philadelphia, PA 19103
215.433.2103
joseph_crowe@comcast.com

Janardhan Bollineni, Comcast

Charlie Helfinstine, Comcast

Thomas Modayil Jacob, Comcast

Table of Contents

Title **Page Number**

List of Figures

Title **Page Number**

1. Introduction

The domain name service (DNS) is one of the most critical internet services. It is often referred to as "the phonebook of the Internet", meaning that the DNS facilitates a human-readable fully qualified domain name (FQDN) to be translated to a network IP address, which in turn allows networked devices to communicate to one other and provide content or needed services to allow applications to work as expected. The DNS was first introduced in 1983 by Paul Mockapetris and is one of the original Internet Standards per the IETF since 1986 (https://en.wikipedia.org/wiki/Domain_Name_System).

Since the advent of the DNS, it has been inherently insecure because DNS packets are transmitted in clear text either via the User Datagram Protocol (UDP) or the Transmission Control Protocol (TCP). There have been numerous initiatives to secure the DNS, notably DNS security extensions (DNSSEC), which encourage authoritative DNS operators to add extensions and caching DNS operators to perform validations. While this enhances security for the user, it doesn't solve the clear text request and response problems.

More recently, encrypted DNS protocols have been implemented across the Internet, including but not limited to, DNS over HTTPS (DoH), DNS over TLS (DoT), DNSCrypt, and in the near future DNS over QUIC (DoQ). Comcast is one of the first major ISPs to provide DoH and DoT to their customers and has also become a trusted recursive resolver with Mozilla's browser Firefox.

2. DNS at Comcast

Comcast's DNS infrastructure currently handles approximately 1.3 trillion queries per day at peak (fig. 1). with a portion of that traffic being encrypted. Decryption is accomplished using a network appliance front end to handle the DoH and DoT translations, which in turn hand off DNS queries to the backend DNS servers. Comcast also implemented DNSSEC validation at the caching layer and DNSSEC signing on most of their zones in 2011, with a commitment to make the DNS infrastructure more secure for their customers. (https://corporate.comcast.com/comcast-voices/dnssec)

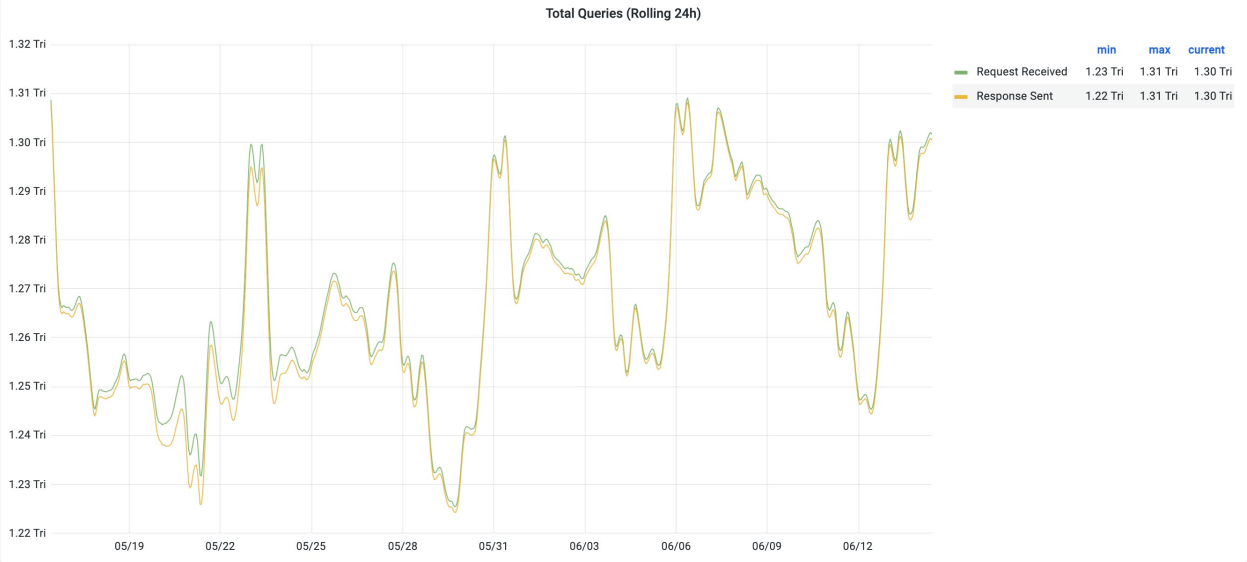

Figure 1 – Recent 30-Day Graph of Comcast DNS Queries

3. First Steps into Encrypted DNS

In 2017, Mozilla was looking to design a new encrypted DNS protocol to help protect their users' privacy by limiting the exposure to the cleartext DNS packets. A request for comments draft (RFC) was submitted to the Internet Engineering Task Force (IETF), to outline the requirements and goals of DoH. RFC 8484 was published in October of 2018. This RFC helped drive some of the first DoH translators to take a TLS handshake, decrypt the packet, send the DNS query, get a response, re-encrypt, and send back to the client. (Hoffman & McManus)

In 2019, Mozilla partnered with Cloudflare to turn this feature on as a default for all Firefox users. The feature, which was turned on for all US-based customers in 2020, sends encrypted DNS traffic to Cloudflare's implementation of the protocol. Comcast engineers kept a close eye on what was being proposed and started looking into how to implement this protocol without a complete redesign of the whole DNS infrastructure.

Initially, Comcast's goal was to gain a comprehensive understanding of the protocol and how it works before the next steps of designing a solution that could go into production. Comcast hosts "lab weeks" twice a year for their engineers and in 2019 there was a proposal to create a DoH translator and to test it on the DNS infrastructure (fig. 2). This gave the engineers an opportunity to understand how the protocol works, latency measurements, and if it would affect any other services that Comcast offers to their customers.

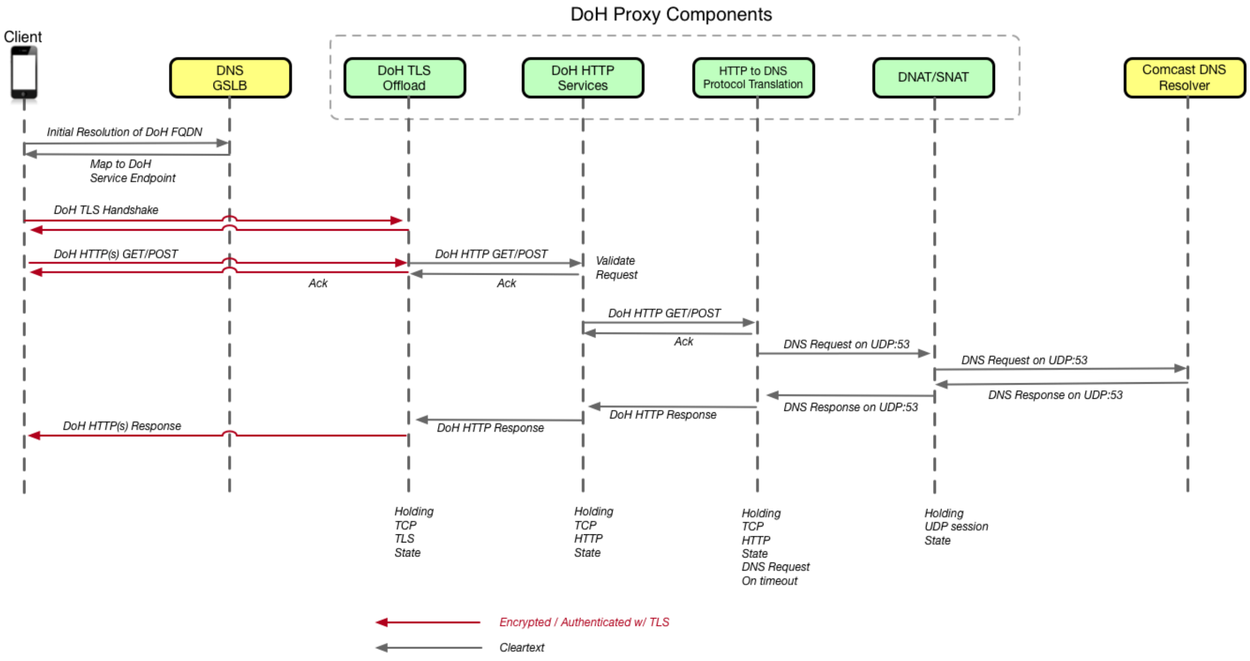

Figure 2 – DoH Proxy Components

DoH traffic utilizes Port 443, the same port that HTTPS uses. DNS traffic is hidden within packets on this port; therefore, a translator is needed to translate from HTTPS to UDP and vice versa. After the lab week in 2019, there was a push to utilize the learnings from the lab week project to build a solution that would work for Comcast. Since the DNS protocol uses mainly UDP and some TCP, the engineers did not want to install a translator on the current DNS servers, due to unknown and hard-to-test performance capabilities on the current systems. The current server hardware was scoped out for a UDP-centric DNS server application, and the compute required for a TCP application with encryption at scale is drastically different. Therefore, a solution that efficiently reuses current infrastructure was pursued. During some of the initial conversations it was suggested to utilize a network appliance that can handle TLS offloading already, to front-end the DNS servers, and to have a translator on that appliance handle the TLS offloading, encryption/decryption, and forward to the current DNS infrastructure already in place.

4. Path from the Lab into Production

The team determined that using network appliances to perform the encryption and decryption was the most efficient way to introduce a solution to Comcast's infrastructure quickly. The engineering teams engaged with network appliance vendors and internal teams familiar with network appliances operation to develop a workable solution. The opening conversations were around the new DoH protocol and sharing RFC 8484 with the vendors. There was a need to have a network appliance handle the HTTPS connections, store the TLS certificate for the DoH FQDN, decrypt the DoH packet, translate the DoH packet to a DNS packet, forward that packet to backend DNS servers, receive that response, encrypt the packet, and then respond back to the client (Fig. 3).

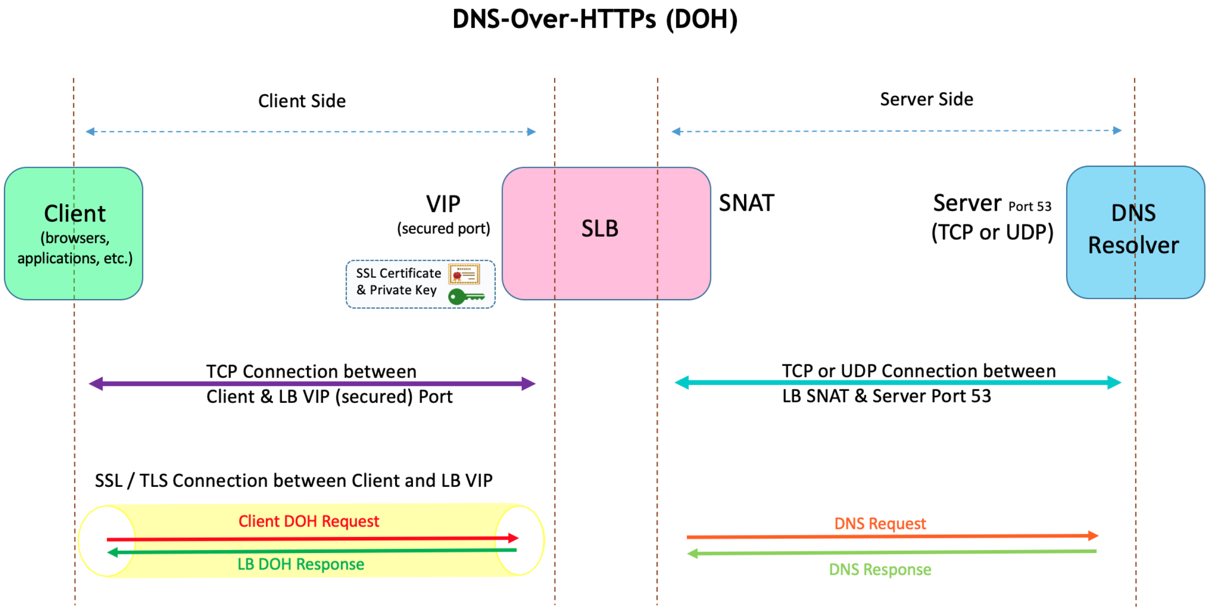
DNS-Over-HTTPs (DOH)
Client Side
Server Side
Client
(browsers, applications, etc.)
VIP
(secured port)
SSL Certificate & Private Key
SLB
SNAT
Server Port 53
(TCP or UDP)
DNS Resolver
TCP Connection between Client & LB VIP (secured) Port
TCP or UDP Connection between LB SNAT & Server Port 53
SSL / TLS Connection between Client and LB VIP
Client DOH Request
LB DOH Response
DNS Request
DNS Response

Figure 3 – DoH Using a Network Appliance

Each of the network appliance vendors were able to provide their versions of the specialized software that included the DoH translator and gave Comcast's engineers a chance to test and determine what would work from both a performance and financial perspective. Discussions landed on a specific device that could handle the query load and was relatively cost effective. During this early phase, there was discussion within EDDI and other DNS operator forums on how to stress test this new protocol. The toolsets for DoH operators to test the functionality, latency, capacity, and other unknown scenarios, were very limited in the early stages of testing. One of the toolsets that helped was an open-sourced tool called DoX which can be found at https://github.com/wttw/dox. This tool allowed testing against the DoH endpoint set up and comparisons with other known DoH endpoints. A few other tools were used internally at Comcast to benchmark DoH end-points such as wrk and wrk2. The tools offer parameters that can be tuned to measure important metrics such as requests per second, connections per second, and performance provided by a DoH end-point at different levels of concurrent connection load. After there was comfortability with the network appliances and DoH functionality, there was an opt-in public beta test of the Comcast DoH service in October of 2019. This allowed other DNS operators to test the endpoint https://doh.xfinity.com/dns-query, give feedback, and help identify some of the issues that were not found in initial testing. The path to production involved knowing what the architecture would look like and how to provide the best service for customers.

5. Encrypted DNS at Comcast

Launching an encrypted DNS architecture posed a few technical challenges, particularly around ensuring high availability and localizing DNS responses for a given area where DNS is already being served to customers. Currently the way clients are directed to doh.xfinity.com is to either have the FQDN and IP address hard coded into the client or to utilize DNS to get a response. Utilizing geo load-balancing, the DNS lookups to doh.xfinity.com are shaped by where the DNS query originates. The DoH endpoint, doh.xfinity.com, utilizes a canonical name (CNAME) record that is directed to a geo network appliance, to help shape traffic to the correct DoH IP address for a region. Client lookup will go as follows, assuming that the customer is using Comcast's DNS servers provided by the dynamic host configuration protocol (DHCP):

1. Customer's client (browser, application, DNS forwarder..) will do an initial look up for doh.xfinity.com utilizing Comcast's DNS servers.
2. Based on the Comcast DNS resolver that queried for the CNAME endpoint, doh2.gslb2.xfinity.com, the network appliance will give a response for the corresponding caching DNS region's virtual IP (VIP) address.
3. The client will then connect to the encrypted DNS network appliance using the VIP and all subsequent DNS queries are now encrypted, with the VIP acting as the "client" doing queries for that customer.

The last step obfuscates the customers' source IP addresses to Comcast's DNS servers and give an extra layer of privacy. In Q2 2020 Comcast offered encrypted DNS to their customers. The queries per day for DoH currently sits around 90 billion at peak. (fig. 4). There are currently 12 points of presence on Comcast's network that handle the encrypted DNS functions, with 3 more points of presences slated to be deployed in 2022.

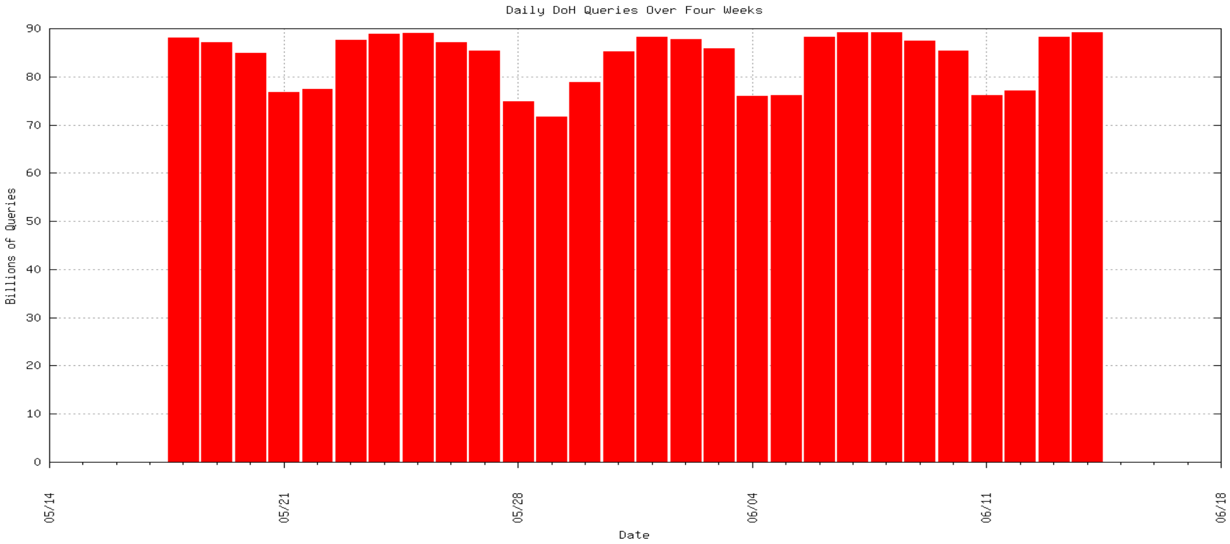

Figure 4 – Comcast DoH Queries Per Day

6. Comcast's Commitment to Privacy

During the initial path towards encrypted DNS services, Comcast worked closely with engineers from Mozilla, to find out how Comcast's DoH implementation could be offered to Firefox customers. Mozilla's trusted recursive resolver (TRR) policy had to be followed by any DNS operator to be considered as a DoH endpoint within Mozilla's Firefox browser. (Mozilla) Some of the requirements prompted Comcast to release a privacy statement just for DNS (Xfinity), along with updates to the broader privacy policy for the internet services. (Xfinity, 2021) Comcast has brought support and privacy commitments to Mozilla's TRR program, becoming the first major ISP to be part of that program and advocating for the privacy concerns of their customers (Mozilla, 2020)Along with becoming part of Mozilla's TRR program, work was done in conjunction with Google engineers to help provide Comcast's DoH endpoint to users of the Chrome browser. Furthering the exposure of the commitment to privacy utilizing encrypted DNS. Comcast also contributes to the Encrypted DNS Deployment Initiative (EDDI) (https://www.encrypted-dns.org/), a forum for DNS operators to collaborate on their findings of deploying encrypted DNS protocols on their respective DNS infrastructures, while helping shape some of the best practices for encrypted DNS deployments.

7. Encrypted DNS in the future

At Comcast, engineers are constantly looking at ways to improve on solutions in terms of scalability, cost-efficiency, and performance. One such work is harnessing the power of data processing units (DPUs) or SmartNICs to provide DNS encryption. Comcast has built a software solution that utilizes hardware TLS offload components provided by DPUs to efficiently translate between DoH and traditional UDP DNS. The rationale for exploring this method for solving the encrypted DNS problem is illustrated in the following diagram.

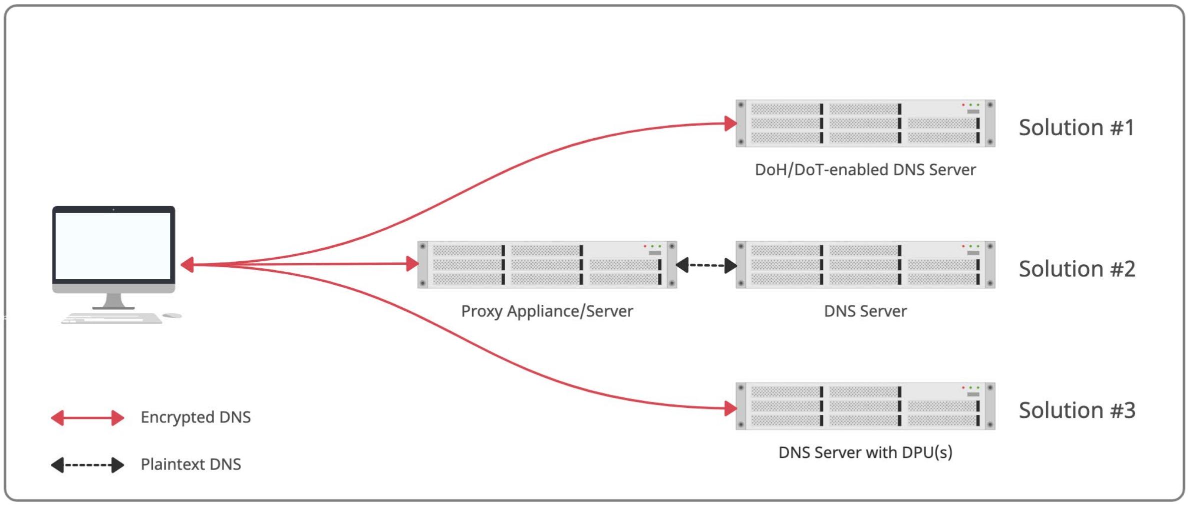

Figure 5 – Encrypted DNS Architecture Possibilities

Solution #1 describes enabling DoH and DoT features on the current DNS server application running on present hardware. As mentioned earlier, current server specifications do not account for DoH/DoT application requirements. In this model, scaling for capacity means adding more servers which results in increased power, space, and licensing costs.

Solution #2 scaling involves increasing the number of expensive hardware proxy appliances in the network.

Solution #3 offers a solution developed at Comcast using open-source components. The components are vendor DPU agnostic and can easily integrate with different DPU vendor offerings. The DPUs are a lot more cost-efficient compared to proxy appliances. Scaling capacity in this model means replacing DPUs with next generation DPUs or adding more DPUs per server. This method provides opportunities to deploy new services at the edge and gives Comcast the ability to cater to the evolving landscape of encrypted DNS standards.

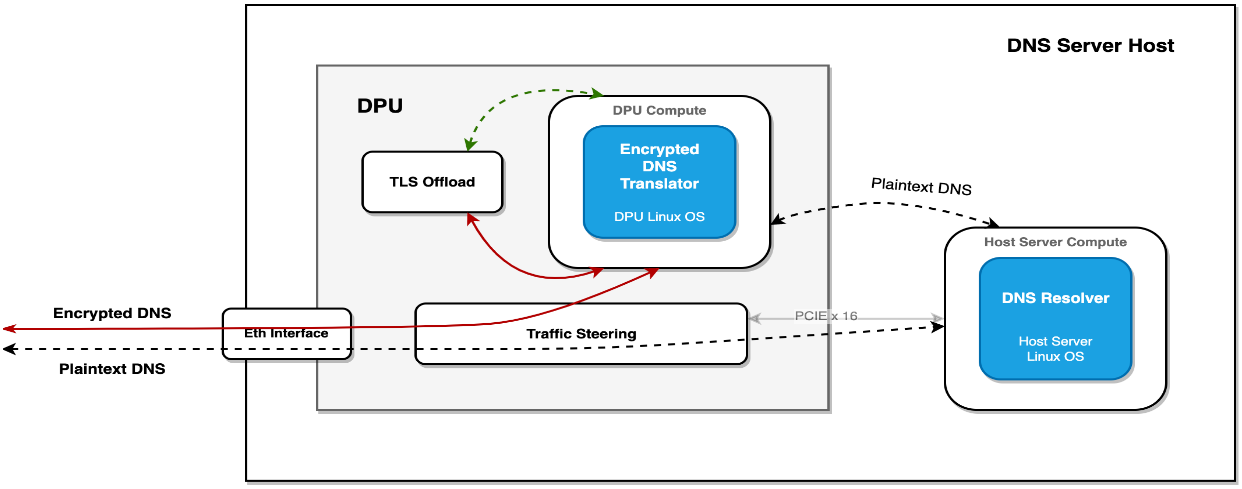

Figure 6 – Encrypted DNS Using DPUs Block Diagram

This solution is being actively benchmarked and tested and is a potential method to add encrypted DNS capacity across the Comcast footprint.

8. Conclusion

As mentioned previously, encrypted DNS continues to evolve, and internet providers have moving targets to hit as new standards are proposed and adopted by the industry. DNS over QUIC (DoQ) is currently a proposed standard for encrypting DNS using QUIC as the underlying protocol. QUIC is designed to reduce protocol induced delays with features such as mitigation of head of line blocking, zero round trip time session resumption (0-RTT) and advanced packet loss and congestion control mechanisms. Additionally, the next version of the HTTP protocol, HTTP/3, is also designed to run on QUIC as the underlying protocol. Comcast is closely monitoring these developments and is working on integrating QUIC into its encrypted DNS capabilities.

Abbreviations

DNS	domain name service
DHCP	Dynamic Host Configuration Protocol
DoH	DNS over https
DoT	DNS over TLS
DoQ	DNS over QUIC
DPU	data processing unit
FQDN	fully qualified domain name
HTTP(S)	Hypertext Transfer Protocol (secure)
QUIC	quick UDP internet connection
UDP	User Datagram Protocol
TCP	Transmission Control Protocol
FQDN	fully qualified domain name
TLS	transport layer security
VIP	virtual IP

Bibliography

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

Xfinity. (n.d.). *Xfinity Internet DNS Privacy Statement.* Retrieved from https://www.xfinity.com/privacy/policy/dns