DOH/DOT AT SCALE

October 31, 2019

Joe Crowe

DNS-OARC 31

WHO AM I?

JOE CROWE

SENIOR ENGINEER

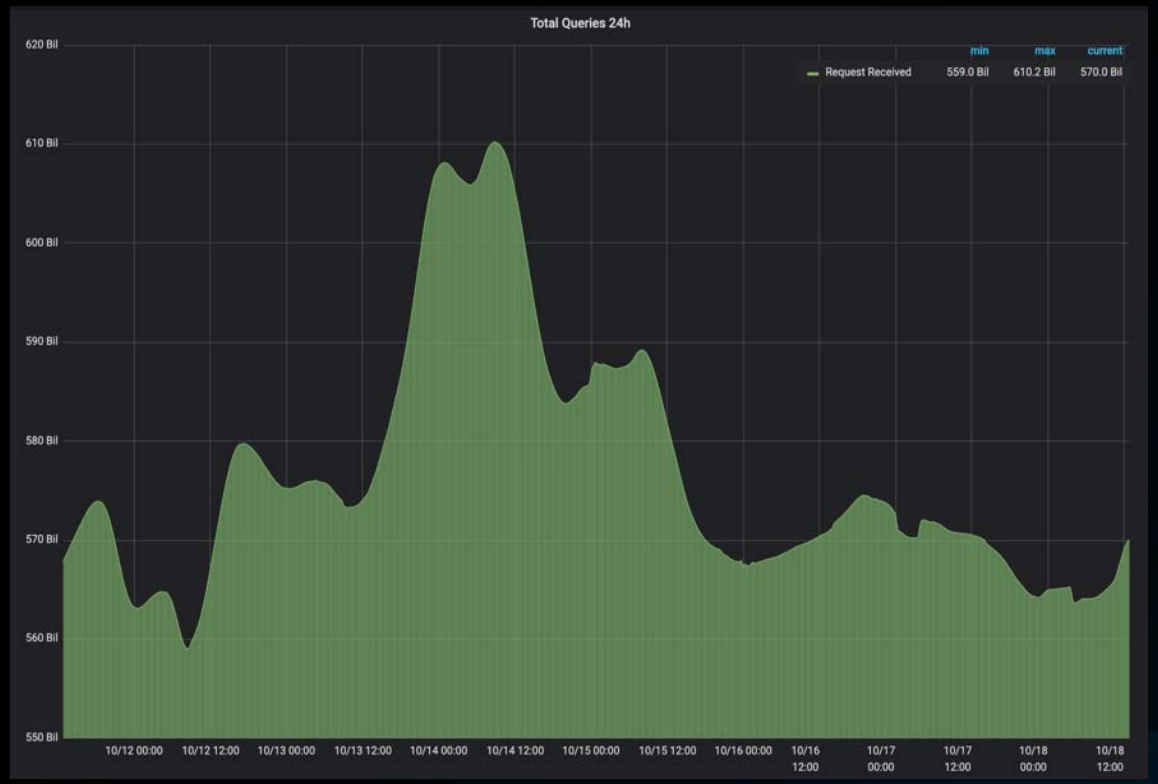
CORE NETWORK SERVICES

JOSEPH_CROWE@COMCAST.COM

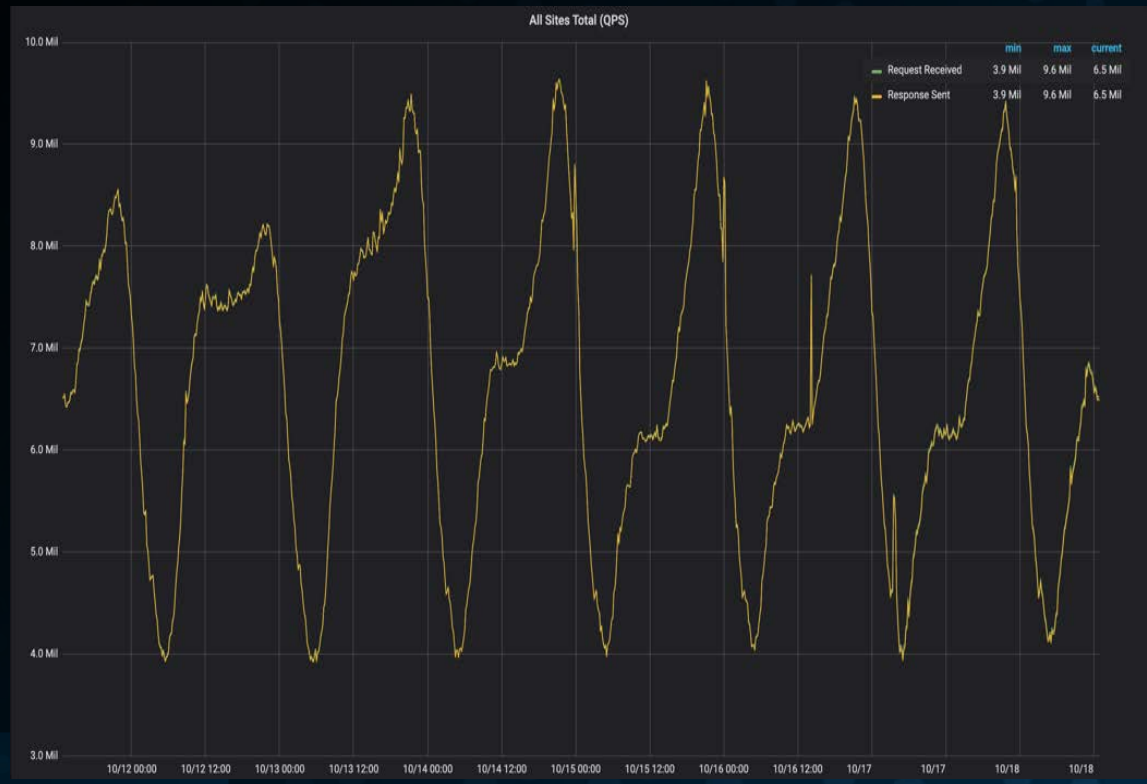
COMCAST

COMCAST'S DNS QUERIES AT A GLANCE

WE CURRENTLY EXCEED 600B QPD



THAT'S ~10M QPS AT PEAK



* Graphs showing 7 days of data

COMCAST

THAT'S A LOT OF QUERIES!

CURRENT INFRASTRUCTURE NEEDS

- Capacity to handle all those UDP packets along with some TCP packets
- DNSSEC validation & native dual-stack support (IPv4/IPv6)
- Load spread across our footprint
- Low latency expectations for customer experience
- Expectation of 100% uptime barring any network issues out of our control

COMCAST

LET’S ENCRYPT ALL THE THINGS, INCLUDING DNS!

SHOULD WE ENCRYPT DNS DATA?

- **WHAT'S THE POTENTIAL GAIN?**
  - Protection from MITM attacks
  - Resilience against DNS response modification across the Internet
  - Improved DNS privacy (depends on the practices of the resolver operator)

Photo credit: https://unsplash.com/photos/bOy4OPu98lI

COMCAST CARES ABOUT DNS PRIVACY

1 DNS DATA

We delete the DNS queries generated by our Internet customers every 24 hours except in very specific cases where we need to research a security or network performance issue, protect against security threats, or comply with a valid legal request. We've never used that data for any sort of marketing or advertising – and we have never sold it to anyone.

2 OPT-IN SERVICES

Comcast offers parental controls and protected browsing for customers that want to use those services.

3 DNSSEC VALIDATION

In 2012 Comcast implemented DNSSEC validation on all DNS resolvers

4 DNS-OVER-HTTPS AND DNS-OVER-TLS

Comcast is currently working towards DoH and DoT solutions to provide to customers.

COMCAST

WAIT WHAT?!

THAT'S CORRECT, COMCAST WILL OFFER DOH/DOT

THERE ARE SOME CONCERNS THOUGH

- How can we offer this utilizing our current infrastructure?
- How can we ensure the best customer experience?
- What tools are available to stress test these solutions?
- What happens to some of our services when web browsers or applications turn on DoH for all their users?
- Comcast encrypted DNS deployment dates:
  - Beta 1 – Functional Testing:
    - DoH started 10/22/2019 via https://doh.xfinity.com/dns-query
    - DoT started 10/28/2019 via dot.xfinity.com
  - Beta 2: Performance testing and architecture bake-off 4Q2019
  - Production Deployment: 2020

COMCAST

GENERAL CONCERNS

NEW INFRASTRUCTURE NEEDS

- We are now going to need an infrastructure that can handle TLS offload and multiple TCP connections
- We needed to figure out how to provide geolocation for DNS queries for our customers
- Initial latency is going to happen, but how can we better that for our customers? (But will latency be better once the initial connection is established?)

WHAT ARE SOME KNOWNS?

- We know that without adding more capacity to our footprint, current performance may decline if we were to use a software-only solution
- For DoH, a translator and TLS offload will add complexity that we need to now understand and be able to troubleshoot
- CDN geolocation could be impacted so we need to work on localization to provide the best customer experience for CDN-based content
- There aren’t many tools available to do testing, while this need is growing, we have to come up with other ways to do testing with what’s available
- We will need to lean on other teams and vendors for their expertise

DNS FILTERING AND ENTERPRISE NETWORKS

USING CENTRALIZED DOH CAN BREAK THINGS

- Our customers use opt-in services to protect their household from malware and to protect their children from visiting sites they don’t want
- Those services use DNS to redirect known bad sites to a block page for Xfinity
- Turning on centralized DoH can allow for someone to bypass these services
- Similarly, enterprise networks have access to internal resources via DNS queries (split DNS)
- Turning on centralized DoH can leak those internal DNS queries to the centralized DoH endpoint, dependent on how you have centralized DoH implemented
- One browser has introduced a “canary domain” for disabling the centralized DoH default opt-out service in these situations, which is good – and another browser will not change default DNS provider

COMCAST

DOH IS OUR FIRST FOCUS*

*There are reasons

UTILIZE CURRENT INFRASTRUCTURE

- We worked internally to create a DoH translator that will forward the DoH packets to our DNS servers and then back.
- Worked with vendors to do similar functions, but based off hardware or software supported by them.

ENSURE GOOD CUSTOMER EXPERIENCE

- Work towards a geo balanced solution to provide the best DNS responses for customers
- Working towards not being reliant on a browser or app for DoH/DoT
- Will need to add capacity closer to customers as demand sees fit.

TOOLS

- dox
- doh curl client
- dns-perf w/dot
- doh-client
- This is area needs the help of people like you.

COMCAST

WHAT CAN WE DO TOGETHER?

Encrypted DNS Deployment Initiative

- *Our goal is to work together to adopt new encrypted DNS standards on a global basis to improve user privacy & security, while also preserving the distributed architecture of DNS operations & administration, maintaining global DNS security and stability, and supporting existing DNS-based technical functions.*
- Currently there are >40 organizations that are participating in EDDI
- There are a few ways to get involved
  - Open discussion on the https://www.encrypted-dns.org/mailing-list
  - Work Streams on GitHub https://github.com/Encrypted-DNS-Deployment-Initiative
  - We are open to new orgs adding the logo - to do so send it to glenn_deen@comcast.com
  - The list is open to anyone who wants to signup - it's commitment free and no membership agreement needed

COMCAST

SOME TAKEAWAYS

- Comcast is working to encrypt DNS data
- Definitely not an easy task at scale and there is a bit to be learned
- DoH has a lot of attention right now and is being focused on first
- DoT is preferred and being worked in tandem
- Beta Phase 1: Functional testing - Started 10/22 (DoH) and 10/28 (DoT)
  - DoH URI = https://doh.xfinity.com/dns-query
  - DoT = dot.xfinity.com
- Beta Phase 2: Performance testing & A/B architecture testing – date TBD in 4Q2019
- The community should come together and push for decentralized encrypted DNS solutions, along with best practices and standards
- Encrypted DNS Deployment Initiative could use the support from DNS operators like yourselves to push those forward

Photo credit: https://unsplash.com/photos/wxDoZRigMxE

LINKS

DNS Over ”X” GUI
dox: https://github.com/wttw/dox

DNS-Over-HTTPS Server and Client
dns-over-https: https://github.com/m13253/dns-over-https

DNS-Over-HTTPS Standalone DNS lookup tool
doh curl client: https://github.com/curl/doh

DNS Performance testing
dns-perf: https://github.com/DNS-OARC/dnsperf

Encrypted DNS Deployment Initiative
EDDI: https://www.encrypted-dns.org


COMCAST