

Data-Intensive Internet Computing

Prof. Dr. Vaibhav Bajpai

Research Areas

Systems and Security
Measurement Methods

Research Targets

Academic Venues (SIGCOMM & IMC)
IETF and RIPE meetings

Team

1 Postdoc, 1 Office Assistance
5 Masters thesis students

Open Positions

Postdoc and PhD positions
Research visits and Internships

**Design IT.
Create Knowledge.**



Measuring the State of DNS Privacy: Past, Present and Future

Prof. Dr. Vaibhav Bajpai



Trinh Viet
Doan



Mike
Kosek



Justus
Fries



Jayasree
Sengupta



Simon
Huber



Irina
Tsareva



Malte
Granderath



Luca
Schumann

**Design IT.
Create Knowledge.**



DNS Centralisation

Evaluating Public DNS Services in the Wake of Increasing Centralization of DNS

NETWORKING'21

Trinh Viet Doan, Justus Fries, Vaibhav Bajpai

Motivation and Problem Statement

- ▶ Many new public DNS services have lately emerged.
- ▶ They promise reliability, lower latency and security.
- ▶ Previous studies (>5 years old) showed ISP resolvers are commonly used and provide better performance.
- ▶ However, there exists a **large gap** in the evaluation of new public DNS services.

What is the popularity, closeness (path lengths), and latency of these new public DNS services?

Methodology



- * 2.5K RIPE Atlas home probes (>1K IPv6 capable)
- * covering 720 ASes in > 85 countries.
- * 10 public resolvers + ISP local resolvers.
- * 30K ICMP traceroutes to DNS + ISP local resolvers.
- * 12M DNS over UDP/53 requests/responses.

Launch		IPv4 Address	IPv6 Address
2020-05	NextDNS	45.90.28.0	2a07:a8c0::
2018-04	Cloudflare DNS	1.1.1.1	2606:4700:4700::1111
2017-11	Quad9	9.9.9.9	2620:fe::9
2017-02	CleanBrowsing	185.228.168.168	2a0d:2a00:1::1
2017-02	Neustar UltraRecursive	156.154.70.1	2610:a1:1018::1
2015-09	VeriSign Public DNS	64.6.64.6	2620:74:1b::1:1
2013-11	Yandex DNS	77.88.8.8	2a02:6b8::feed:ff
2009-12	Google Public DNS	8.8.8.8	2001:4860:4860::8888
2006-07	OpenDNS	208.67.222.123	2620:0:ccc::2
2000-06	OpenNIC	185.121.177.177	2a05:dfc7:5::5353

In which scenarios would switching to these public DNS services offer benefit?

DNS Centralisation

Popularity
Path Lengths
Latency

DNS over TCP

Reliability
Response Times

DNS over TLS

Adoption
Reliability
Response Times

DNS over QUIC

Adoption
Response Times

QUIC Coalescing

Recap

DNS Centralisation | Popularity

- ▶ >7.5k probes use local ISP resolvers. (>71%)
- ▶ **3k** probes use at least one public DNS service.
 - 1.4k probes use **only** public DNS services.
 - 1.6k probes use a mix of local ISP + public DNS service.
 - Google is the most popular DNS service.
- ▶ 1k probes use **one and only one** public DNS service.

	# Probes	# Probes with <i>n</i> Publ. Services	# Employing Probes
Public only	1,371 (12.9%)	978, <i>n</i> = 1 (71.3%)	Google: 1,001 (55.5%) Cloudflare: 527 (29.2%) Quad9: 126 (7.0%) OpenDNS: 122 (6.8%) Yandex: 12 (0.7%) NextDNS: 8 (0.4%) VeriSign: 3 (0.2%) Neustar: 2 (0.1%)
		355, <i>n</i> = 2 (25.9%)	CleanBrowsing: 1 (<0.1%)
		38, <i>n</i> = 3 (2.8%)	
Public + local	1,636 (15.4%)	825, <i>n</i> = 1 (50.4%)	Google: 1,357 (56.7%) VeriSign: 656 (27.4%) Cloudflare: 263 (11.0%) OpenDNS: 54 (2.3%) Quad9: 47 (2.0%)
		811, <i>n</i> = 2 (49.6%)	Yandex: 13 (0.5%) Neustar: 2 (0.1%) NextDNS: 2 (0.1%) OpenNIC: 1 (<0.1%)

>28% of 10.6k RIPE atlas probes (and their host network) use at least one public DNS service

>9% use one and only one public DNS service

Probes that use public DNS service by default will conduct measurements with **unintended** side-effects

DNS Centralisation

Popularity

Path Lengths

Latency

DNS over TCP

Reliability

Response Times

DNS over TLS

Adoption

Reliability

Response Times

DNS over QUIC

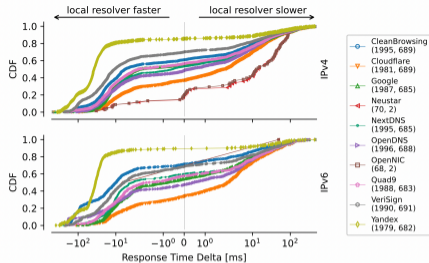
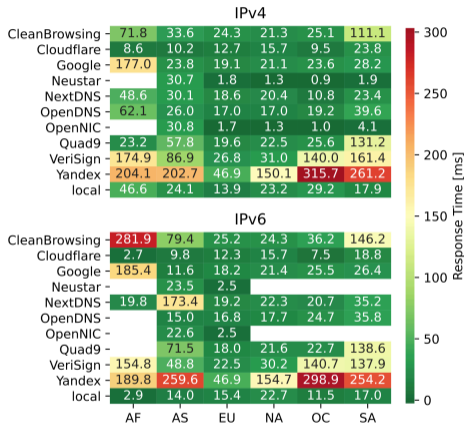
Adoption

Response Times

QUIC Coalescing

Recap

DNS Centralisation | Latency



- ▶ 75% of all samples within 40ms latency.
- ▶ Cloudflare and OpenDNS faster than ISP resolvers in 50% of the probes.
- ▶ Google public DNS latencies inflated in AF.
- ▶ Public DNS resolvers slower than ISP resolvers in regions beyond EU and NA.

Users in EU and NA **do not** substantially benefit in latency when switching to a public DNS service.

Latencies offered by public DNS services over **IPv6** remain inflated in AF and SA.

DNS Centralisation

Popularity

Path Lengths

Latency

DNS over TCP

Reliability

Response Times

DNS over TLS

Adoption

Reliability

Response Times

DNS over QUIC

Adoption

Response Times

QUIC Coalescing

Recap

DNS over TCP

Measuring DNS over TCP in the Era of Increasing DNS Response Sizes: A View from the Edge CCR'22

Mike Kosek, Trinh Viet Doan, Simon Huber, Vaibhav Bajpai

Motivation and Problem Statement

- ▶ The Domain Name System (DNS) is a cornerstone of communication on the Internet.
- ▶ DNS specifications mandate supporting both DoUDP and DoTCP, although DoUDP is predominantly used.
- ▶ The trend of increasing DNS response sizes (IPv6 and DNSSEC) lead to **truncation** and **IP fragmentation**, requiring fallback to DoTCP.
- ▶ However, the effects of using DoTCP from the edge (stub resolvers) is **not known** yet.

Methodology



- > 2.5K RIPE Atlas home probes
- > 10 public resolvers + local resolvers.
- > 200 domains queried for A records over IPv4.
- > 12M DNS requests/responses overall.

How reliably can DoTCP be used from the edge of the network?

How do DoTCP response times compare with that of DoUDP? Do DoTCP interactions leverage TCP optimisations to reduce DNS response times?

DNS Centralisation

Popularity
Path Lengths
Latency

DNS over TCP

Reliability
Response Times

DNS over TLS

Adoption
Reliability
Response Times

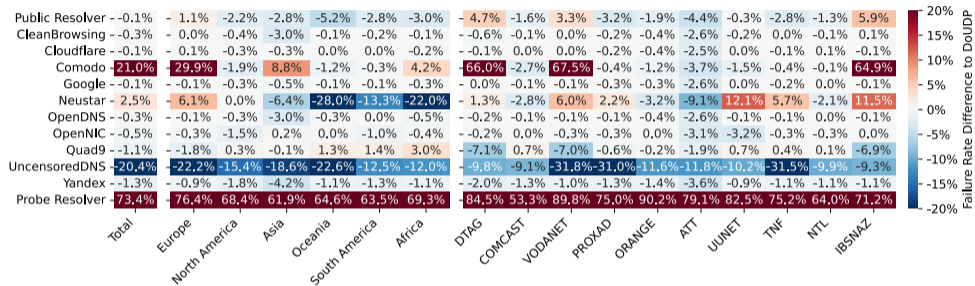
DNS over QUIC

Adoption
Response Times

QUIC Coalescing

Recap

DNS over TCP | Reliability



- ▶ Failure rates (DoTCP and DoUDP) are comparable towards public resolvers.
- ▶ DoTCP failure rates are significantly higher with ISP resolvers.
- ▶ In 3/4 cases, ISP resolvers fail to send large DNS responses over DoTCP.

DoTCP exhibits **higher failures** than DoUDP. Failures are more pronounced over local resolvers.

DNS Centralisation

- Popularity
- Path Lengths
- Latency

DNS over TCP

- Reliability
- Response Times

DNS over TLS

- Adoption
- Reliability
- Response Times

DNS over QUIC

- Adoption
- Response Times

QUIC Coalescing

Recap

DNS over TLS

Measuring DNS over TLS from the Edge: Adoption, Reliability, and Response Times

PAM'21

Trinh Viet Doan, Irina Tsareva, Vaibhav Bajpai

Motivation and Problem Statement

- ▶ The Domain Name System (DNS) is a cornerstone of communication on the Internet.
- ▶ However, DNS over UDP/53 is vulnerable to **eavesdropping and information exposure**.
- ▶ **DNS over TLS/853** (DoT) standardized in 2016 (RFC 7858) to encrypt DNS messages.
- ▶ DoT is supported since Android 9 (2018) and iOS/macOS (2020).
- ▶ However, previous work on DoT largely considers university – proxy – data-center networks.

Methodology



- > 3.2K RIPE Atlas home probes
- > 15 public resolvers (5 with DoT) + local resolvers.
- > 200 domains queried for A records over IPv4.
- > 90M DNS requests/responses overall.

What is the state of adoption and traffic share of DoT at the edge?

Do home users experience benefit (or suffer) from using DoT (in terms of reliability and latency) when compared to traditional DNS/53?

DNS Centralisation

Popularity
Path Lengths
Latency

DNS over TCP

Reliability
Response Times

DNS over TLS

Adoption
Reliability
Response Times

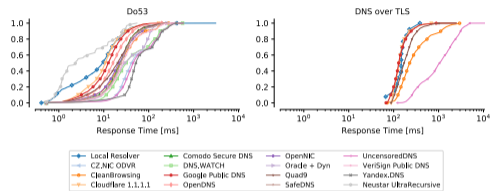
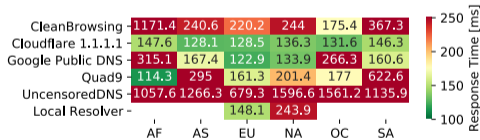
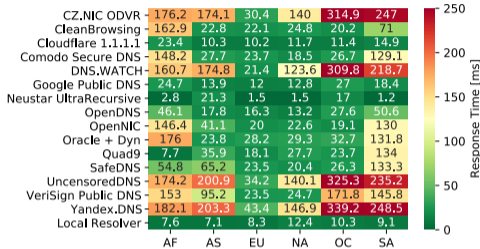
DNS over QUIC

Adoption
Response Times

QUIC Coalescing

Recap

DNS over TLS | Response Times



- ▶ Do53: <30 ms for most resolvers (median)
- DoT: <150 ms for faster resolvers (median)
- ▶ Higher response times in AF and SA.

DoT response times inflated by >100 ms compared to Do53.

DoT response times for local resolvers comparable to that of public resolvers.

DNS Centralisation

Popularity
Path Lengths
Latency

DNS over TCP

Reliability
Response Times

DNS over TLS

Adoption
Reliability
Response Times

DNS over QUIC

Adoption
Response Times

QUIC Coalescing

Recap

DNS over QUIC

A First Look at DNS over QUIC PAM'22

Mike Kosek, Trinh Viet Doan,
Malte Granderath, Vaibhav Bajpai

Motivation and Problem Statement

- ▶ DNS over TLS (standardized in 2016) and DNS over HTTPs (in 2018) leverage TLS/TCP for transport.
- ▶ However, both are **constrained** by limitations of TCP.
- ▶ **QUIC** solves head of line blocking, supports multiplexing, and lowers handshake times.
- ▶ DNS over QUIC (RFC 9250) is the natural evolution to improve DNS performance and privacy.
- ▶ However, there exists **no previous work** on **DoQ** yet.

Methodology



Measurements from the TUM research network (blue dot)

>25 weeks of ZMAP scans towards DoQ/DoUDP ports.

* A three step validation phase using:

- QUIC version negotiation
- ALPN identifiers and
- QUIC connection establishment

* developed `dnsperf` to measure DoQ, DoTCP, DoUDP, DoT, DoH response times by querying an **A** record.

What is the state of adoption of DoQ?

Do DoQ servers and clients leverage the full potential of QUIC to improve privacy and lower response times?

DNS Centralisation

Popularity

Path Lengths

Latency

DNS over TCP

Reliability

Response Times

DNS over TLS

Adoption

Reliability

Response Times

DNS over QUIC

Adoption

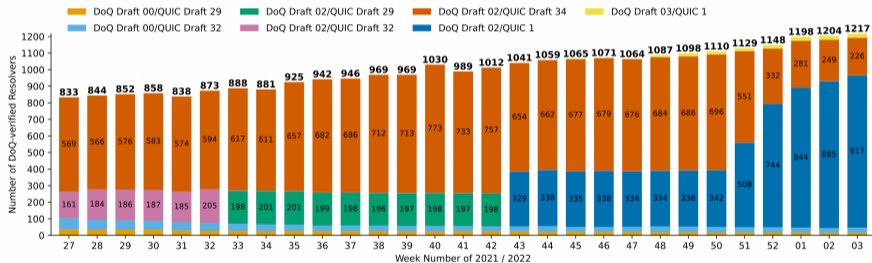
Response Times

QUIC Coalescing

Recap

DNS over QUIC | Adoption

- ▶ Number of DoQ verified resolvers (>1.2k) steadily rose by >46% in 29 weeks.
- ▶ Multiple resolvers use [Adguard Home](#) DoQ server implementation (using QUIC v1).



Large fraction of DoQ resolvers observed in Asia (>45%) and Europe (>32%)

AdGuard and nextDNS use DoQ as part of the DNS-based [ad and tracker blocking](#) services

DNS Centralisation

Popularity
Path Lengths
Latency

DNS over TCP

Reliability
Response Times

DNS over TLS

Adoption
Reliability
Response Times

DNS over QUIC

Adoption
Response Times

QUIC Coalescing

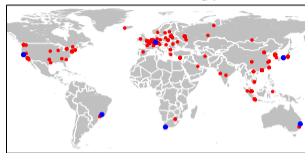
Recap

DNS over QUIC | Impact on Web

DNS Privacy with Speed? Evaluating DNS over QUIC and its Impact on Web Performance IMC '22

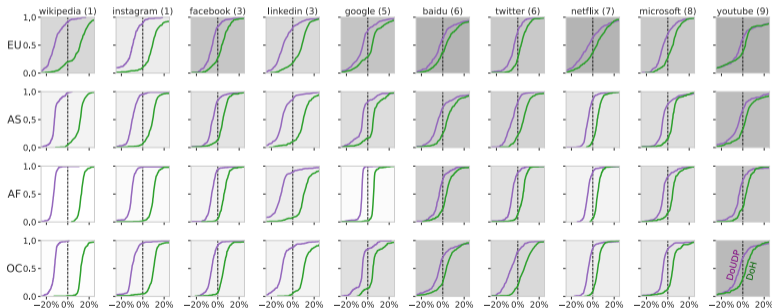
M. Kosek, L. Schumann, TV. Doan, R. Max, V. Bajpai

Methodology



>300 verified DoX resolvers (red dots)
>6 distributed Amazon EC2 instances (blue dots)

With **increasing complexity** of webpages, DoQ catches up to DoUDP in latency, as cost of encryption amortises



DoQ makes encrypted DNS much more appealing for the encrypted Web.

DNS Centralisation

Popularity
Path Lengths
Latency

DNS over TCP

Reliability
Response Times

DNS over TLS

Adoption
Reliability
Response Times

DNS over QUIC

Adoption
Response Times

QUIC Coalescing

Recap

QUIC Coalescing

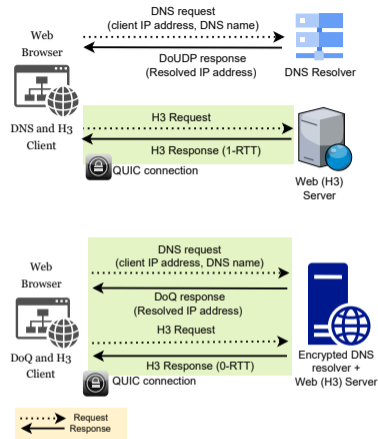
Web Privacy By Design: Evaluating Cross-layer Interactions of QUIC, DNS and H/3

NETWORKING'23

J.Sengupta, M.Kosek, P.Dikshit, V.Bajpai

Motivation and Problem Statement

- ▶ Benefits of QUIC over DNS and Web are **uncoupled**.
- ▶ An opportunity to reuse QUIC connection.
- ▶ Encrypted DNS using DNS over QUIC.
- ▶ Web content delivery using HTTP/3 over 0-RTT.



Can reusing the same QUIC connection over encrypted DNS and Web further improve performance?

DNS Centralisation

Popularity
Path Lengths
Latency

DNS over TCP

Reliability
Response Times

DNS over TLS

Adoption
Reliability
Response Times

DNS over QUIC

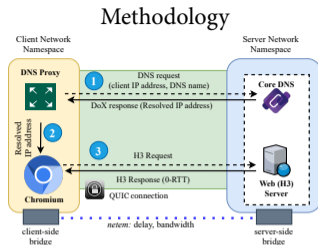
Adoption
Response Times

QUIC Coalescing

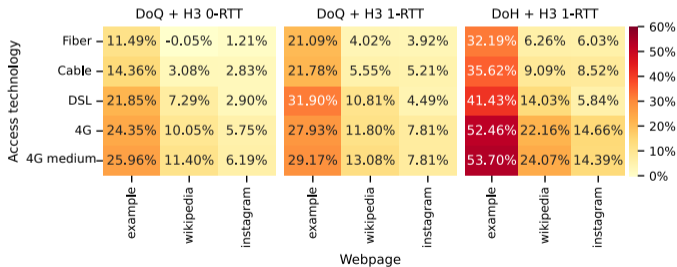
Recap

QUIC Coalescing

- ▶ Emulated network (fiber, cable, DSL, 4G) using netem. with FCC (wired) and ERRANT (mobile) datasets.
- ▶ Evaluated 3 categories of webpages: HTML, +javascript, +javascript +css +cookies



Using H3 1-RTT, page load times with DoH can get **inflated** by >30% over fixed-line and by >50% over mobile compared to unencrypted DoUDP.



Coalescing with QUIC (DoQ + H3 0-RTT) reduces PLT by 1/3 over wired and 1/2 over mobile

DNS Centralisation

- Popularity
- Path Lengths
- Latency

DNS over TCP

- Reliability
- Response Times

DNS over TLS

- Adoption
- Reliability
- Response Times

DNS over QUIC

- Adoption
- Response Times

QUIC Coalescing

Recap