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

HPI Hasso Plattner Institut
Digital Engineering · Universität Potsdam

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.**

www.hpi.de

# Data-Intensive Internet Computing

Prof. Dr. Vaibhav Bajpai

Hasso Plattner Institut
Digital Engineering · Universität Potsdam

## 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.**

www.hpi.de

# DNS Centralisation

## Evaluating Public DNS Services in the Wake of Increasing Centralization of DNS NETWORKING'21

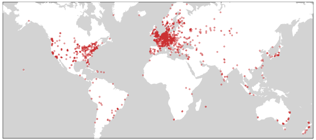
Trinh Viet Doan, Justus Fries, Vaibhav Bajpai

### 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

- >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.

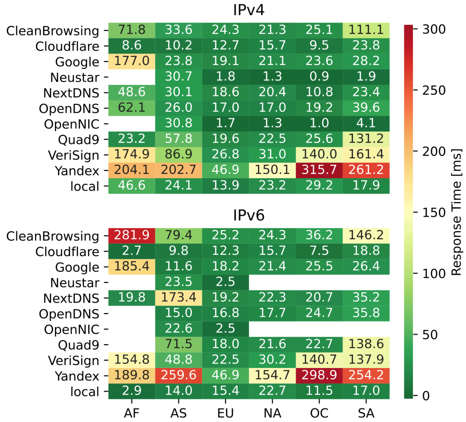
| | # Probes | # Probes with $n$ Publ. Services | # Employing Probes |
|---|---|---|---|
| Public only | 1,371 (12.9%) | 978, $n=1$ (71.3%)<br>355, $n=2$ (25.9%)<br>38, $n=3$ (2.8%) | Google: 1,001 (55.5%)<br>Cloudflare: 527 (29.2%)<br>Quad9: 126 (7.0%)<br>OpenDNS: 122 (6.8%)<br>Yandex: 12 (0.7%)<br>NextDNS: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

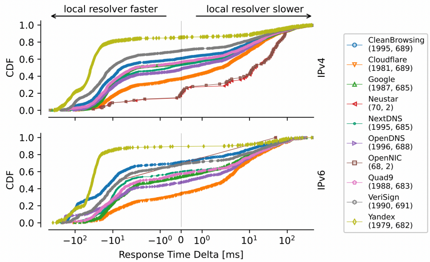
>28% of 10.6k RIPE atlas probes (and their host network) use at least one public DNS service

>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 | 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 over TCP

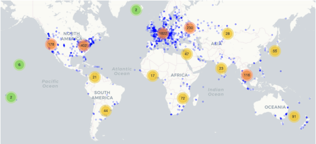
## Measuring DNS over TCP in the Era of Increasing DNS Response Sizes: A View from the Edge CCR'22

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 over TCP | Reliability

Failure Rate Difference to DoUDP (colour scale: -20% to 20%)

| | Total | Europe | North America | Asia | Oceania | South America | Africa |
|---|---|---|---|---|---|---|---|
| Public Resolver | -0.1% | 1.1% | -2.2% | -2.8% | -5.2% | -2.8% | -3.0% |
| CleanBrowsing | -0.3% | 0.0% | -0.4% | -3.0% | -0.1% | -0.2% | -0.1% |
| Cloudflare | -0.1% | 0.1% | -0.3% | -0.3% | 0.0% | 0.0% | -0.2% |
| Comodo | 21.0% | 29.9% | -1.9% | 8.8% | -1.2% | -0.3% | 4.2% |
| Google | -0.1% | -0.1% | -0.3% | -0.5% | -0.1% | -0.1% | -0.3% |
| Neustar | 2.5% | 6.1% | 0.0% | -6.4% | -28.0% | -13.3% | -22.0% |
| OpenDNS | -0.3% | -0.1% | -0.3% | -3.0% | -0.3% | 0.0% | -0.5% |
| OpenNIC | -0.5% | -0.3% | -1.5% | 0.2% | 0.0% | -1.0% | -0.4% |
| Quad9 | -1.1% | -1.8% | 0.3% | -0.1% | 1.3% | 1.4% | 3.0% |
| UncensoredDNS | -20.4% | -22.2% | -15.4% | -18.6% | -22.6% | -12.5% | -12.0% |
| Yandex | -1.3% | -0.9% | -1.8% | -4.2% | -1.1% | -1.3% | -1.1% |
| Probe Resolver | 73.4% | 76.4% | 68.4% | 61.9% | 64.6% | 63.5% | 69.3% |

| | DTAG | COMCAST | VODANET | PROXAD | ORANGE | ATT | UUNET | TNF | NTL | IBSNAZ |
|---|---|---|---|---|---|---|---|---|---|---|
| Public Resolver | 4.7% | -1.6% | 3.3% | -3.2% | -1.9% | -4.4% | -0.3% | -2.8% | -1.3% | 5.9% |
| CleanBrowsing | -0.6% | -0.1% | 0.0% | -0.2% | -0.4% | -2.6% | -0.2% | 0.0% | -0.1% | 0.1% |
| Cloudflare | -0.1% | 0.0% | 0.0% | -0.2% | -0.4% | -2.5% | 0.0% | -0.1% | 0.1% | -0.1% |
| Comodo | 66.0% | -2.7% | 67.5% | -0.4% | -1.2% | -3.7% | -1.5% | -0.4% | -0.1% | 64.9% |
| Google | 0.0% | -0.1% | -0.1% | -0.3% | -0.3% | -2.6% | 0.0% | -0.2% | 0.0% | -0.1% |
| Neustar | 1.3% | -2.8% | 6.0% | 2.2% | -3.2% | -9.1% | 12.1% | 5.7% | -2.1% | 11.5% |
| OpenDNS | -0.2% | -0.1% | -0.1% | -0.1% | -0.4% | -2.6% | -0.1% | -0.1% | 0.0% | -0.1% |
| OpenNIC | -0.2% | 0.0% | -0.3% | -0.3% | 0.0% | -3.1% | -3.2% | -0.3% | -0.3% | 0.0% |
| Quad9 | -7.1% | 0.7% | -7.0% | -0.6% | -0.2% | -1.9% | 0.7% | 0.4% | 0.1% | -6.9% |
| UncensoredDNS | -9.8% | -9.1% | -31.8% | -31.0% | -11.6% | -11.8% | -10.2% | -31.5% | -9.9% | -9.3% |
| Yandex | -2.0% | -1.3% | -1.0% | -1.3% | -1.4% | -3.6% | -0.9% | -1.1% | -1.1% | -1.1% |
| Probe Resolver | 84.5% | 53.3% | 89.8% | 75.0% | 90.2% | 79.1% | 82.5% | 75.2% | 64.0% | 71.2% |

- 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 over TLS

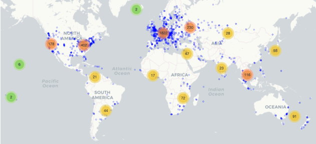
## Measuring DNS over TLS from the Edge: Adoption, Reliability, and Response Times PAM'21

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

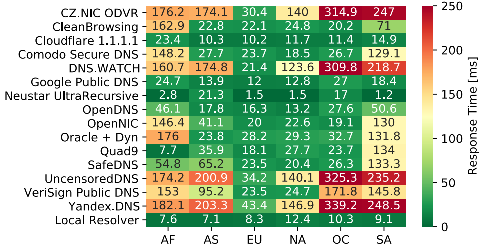


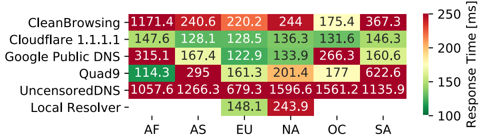

>3.2K RIPE Atlas home probes
>15 public resolvers (5 with DoT) + local resolvers.
>200 domains queried for A records over IPv4.
>90M DNS requests/responses overall.

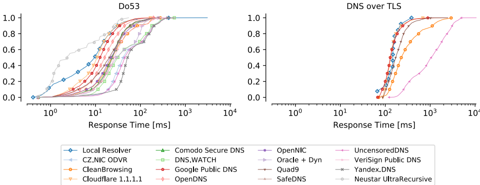
What is the state of adoption and traffic share of DoT at the edge?

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

# DNS 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 over QUIC

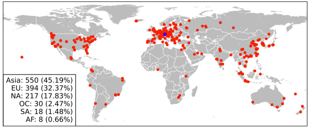
A First Look at DNS over QUIC PAM'22

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

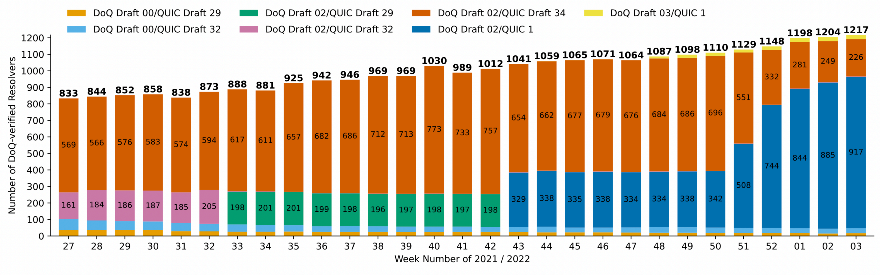
* developed `dnsperf` to measure DoQ, DoTCP, DoUDP, DoT, DoH response times by querying an `A` record.

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 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%)

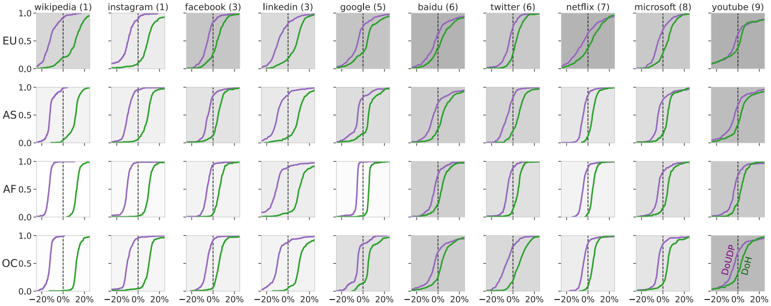
AdGuard and nextDNS use DoQ as part of the DNS-based ad and tracker blocking services

# DNS over QUIC | Impact on Web

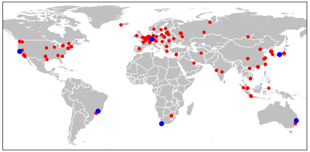
DNS Privacy with Speed? Evaluating DNS over QUIC and its Impact on Web Performance IMC ’22

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

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




## Methodology



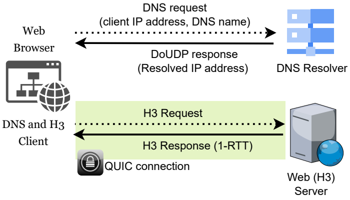
>300 verified DoX resolvers (red dots)
>6 distributed Amazon EC2 instances (blue dots)

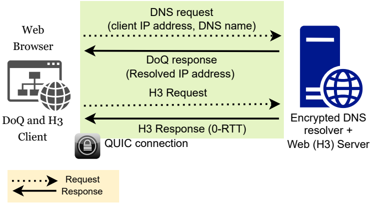
DoQ makes encrypted DNS much more appealing for the encrypted Web.

# 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

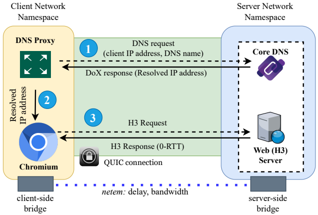
- Benefits of QUIC over DNS and Web are uncoupled.
- An opportunity to reuse QUIC connection.
- Encrypted DNS using DNS over QUIC.
- Web content delivery using HTTP/3 over 0-RTT.

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

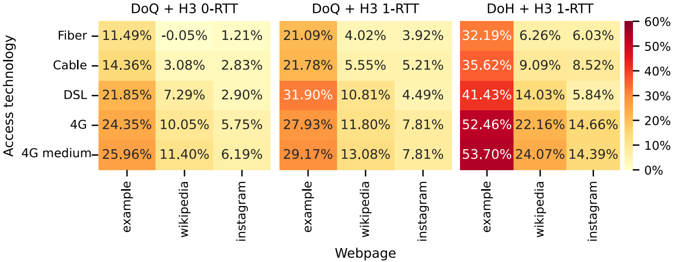
# QUIC Coalescing

- 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

## Methodology




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

# Recap

- Evaluating Public DNS Services in the Wake of Increasing Centralization NETWORKING '21
  Users in EU/NA do not substantially benefit in latency with a public DNS service.
  Latencies offered by public DNS services over IPv6 remain inflated in AF and SA.
- Measuring DNS over TCP in the Era of Increasing DNS Response Sizes CCR'22
  DoTCP exhibits higher failures and latencies than DoUDP.
  TCP optimisations (TFO and TCP keepalives) are not supported.
- Measuring DNS over TLS from the Edge PAM '21
  DoT exhibits higher failures than Do53, and are more pronounced over local resolvers.
  DoT response times are inflated by >100 ms compared to Do53.

# Recap

- A First Look at DNS over QUIC PAM '22
  Large fraction of DoQ resolvers observed in Asia (>45%) and Europe (>32%)
  DoQ offers the best choice for DNS privacy, outperforms both DoT and DoH in latency.

- DNS Privacy with Speed? Evaluating DNS over QUIC and its Impact on Web IMC'22
  The cost of DoQ encryption amortises with increasing web complexity.

- Evaluating Cross-layer Interactions of QUIC, DNS and H/3 NETWORKING'23
  Coalescing with QUIC reduces PLT by 1/3 over wired and 1/2 over mobile.

# References | Publications Covered in the Talk


NETWORKING'21 Evaluating Public DNS Services in the Wake of Increasing Centralization of DNS
https://doi.org/10.23919/IFIPNetworking52078.2021.9472831

CCR'22 Measuring DNS over TCP in the Era of Increasing DNS Response Sizes
https://doi.org/10.1145/3544912.3544918

PAM'21 Measuring DNS over TLS from the Edge: Adoption, Reliability, and Response Times
https://doi.org/10.1007/978-3-030-72582-2_12

PAM'22 One to Rule them All? A First Look at DNS over QUIC
https://doi.org/10.1007/978-3-030-98785-5_24

IMC'22 DNS Privacy with Speed? Evaluating DNS over QUIC and its Impact on Web Performance
https://doi.org/10.1145/3517745.3561445

NETWORKING'23 Web Privacy By Design: Evaluating Cross-layer Interactions of QUIC, DNS and H/3
https://doi.org/10.23919/IFIPNetworking57963.2023.10186362