

# Towards Digital Sovereignty in the Age of Hyper-giants

Vaibhav Bajpai



## Team



Trinh Viet Doan



Mike Kosek



Simon Huber



Justus Fries



Irina Tsareva



Malte Granderath

TMA 2022 Keynote  
Enschede, NL

June 30 / 2022

## Thanks!



supported by



## Preamble

### Web Consolidation

- Landing Pages
- Web Content
- Ads and Trackers
- TLS 1.3

### 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

## Recap

## 1. Age of Hyper-giants

- An Empirical View on Consolidation of the Web **TOIT '22**  
Evaluating Public DNS Services in the Wake of Increasing Centralization **NETWORKING '21**

## 2. Towards Digital Sovereignty: Improving Privacy in DNS

- Measuring DNS over TCP in the Era of Increasing DNS Response Sizes **CCR '22**
- Measuring DNS over TLS from the Edge **PAM '21**
- A First Look at DNS over QUIC **PAM '22**

### Preamble

#### Web Consolidation

- Landing Pages
- Web Content
- Ads and Trackers
- TLS 1.3

#### 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

#### Recap

# Towards Digital Sovereignty in the Age of Hyper-giants



The Internet is getting centralised

1. A long-term perspective on the growth and ubiquity of hyper-giants.

leading to security & privacy concerns

## Preamble

### Web Consolidation

- Landing Pages
- Web Content
- Ads and Trackers
- TLS 1.3

### 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

## Recap

## An Empirical View on Consolidation of the Web TOIT '22

Trinh Viet Doan, Roland van Rijswijk-deij,  
Oliver Hohlfeld, Vaibhav Bajpai

### Motivation and Problem Statement

- ▶ The Web was initially (30 years ago) designed to be a decentralised system.
- ▶ Lately, there are concerns of Web traffic increasingly getting brokered via hyper-giants.
- ▶ Such Web **consolidation** raises technical, societal (privacy) and economical (innovation) concerns.
- ▶ However, contemporary empirical studies on Web consolidation are **still lacking**.

To what extent does web content centralise at hyper-giants (Google *et al.*) for content delivery and hosting?

How lop-sided is the deployment of new innovations on the Internet (protocols) due to such large hyper-giants?

Preamble

Web Consolidation

Landing Pages  
Web Content  
Ads and Trackers  
TLS 1.3

DNS Centralisation

Popularity  
Path Lengths  
Latency

DNS over TCP

Reliability  
Response Times

DNS over TLS

Adoption  
Reliability  
Response Times

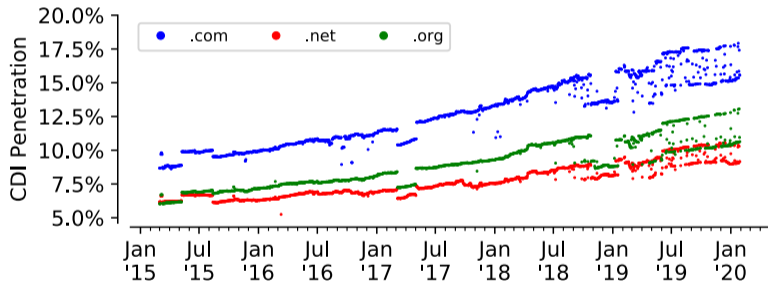
DNS over QUIC

Adoption  
Response Times

Recap

# Consolidation of the Web | Landing webpages

- ▶ .com | .net | .org (>160M domains) – 50% of global DNS namespace
- ▶ Hyper-giant penetration – 8.2% (2015) → 15% (2020), an increase by >83%
- ▶ [Amazon](#) accounts to >50% of hyper-giant growth alone in .com.



Hyper-giant penetration has nearly **doubled** from 2015–2020, and is **higher** among more popular domains.

Preamble

Web Consolidation

Landing Pages

Web Content

Ads and Trackers

TLS 1.3

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

Recap

# Consolidation of the Web | Content and Assets

- ▶ A handful of hyper-giants deliver majority of the Web content.
- ▶ Google and Amazon contribute to >52% of content hosted on hyper-giants.

Provider	# Assets (↓)	Sum of Sizes [GB]	Share of CDI Assets by		Share of All Assets by	
			Num.	Size	Num.	Size
1) Google	76.6M	1,494.9	34.5%	24.0%	19.5%	11.1%
2) Amazon	38.9M	1,277.2	17.5%	20.5%	9.9%	9.5%
3) Cloudflare	27.5M	956.4	12.4%	15.3%	7.0%	7.1%
4) Facebook	17.7M	423.4	8.0%	6.8%	4.5%	3.1%
5) Akamai	15.7M	496.7	7.1%	8.0%	4.0%	3.7%
6) Fastly	10.8M	411.3	4.9%	6.6%	2.7%	3.0%
7) WordPress	4.1M	109.3	1.9%	1.8%	1.1%	0.8%
8) Twitter	4.0M	65.8	1.8%	1.1%	1.0%	0.5%
9) Microsoft	3.8M	181.0	1.7%	2.9%	1.0%	1.3%
10) NetDNA	3.6M	148.5	1.6%	2.4%	0.9%	1.1%

Asset Type	# CDI Assets	CDI Pen. of Type	# All Assets of Type	Share (All) (↓)
image	82,613,713	46.8%	176,660,130	45.0%
javascript	64,223,345	64.1%	100,195,949	25.5%
text	21,676,628	50.4%	43,017,071	11.0%
html	19,590,470	69.6%	28,148,091	7.2%
other	11,864,834	70.4%	16,847,204	4.3%
font	14,245,056	86.0%	16,569,827	4.2%
application	6,303,607	68.4%	9,220,762	2.4%
video	1,135,211	91.8%	1,236,756	0.3%
audio	265,302	62.2%	426,583	0.1%
<b>Total</b>	<b>221,918,166</b>	<b>56.6%</b>	<b>392,322,373</b>	<b>100.0%</b>

- ▶ >56% of the content of 4.3M webpages is hosted on a hyper-giant.
- ▶ Hyper-giant penetration is especially high for JavaScript and fonts.

Preamble

Web Consolidation

Landing Pages

Web Content

Ads and Trackers

TLS 1.3

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

Recap

- ▶ Identification based on *EasyList* and *EasyPrivacy* blocklists.
- ▶ Google delivers **>66%** (ads) and **>55%** (tracker) services.
- ▶ Facebook is under-sampled in the dataset due to missing out on logged in pages (Deep Web).
- ▶ **>22%** of ads delivered by Amazon are via the **online store**, remaining are delivered by users renting **AWS**.

	Provider	# Ads (↓)	Share (all Ads)	Provider	# Trackers (↓)	Share (all Trackers)
(1)	Google	8,776,465	66.6%	Google	15,995,822	55.3%
(2)	—	2,715,437	20.6%	—	5,073,329	17.5%
(3)	Amazon	401,946	3.1%	Amazon	2,466,341	8.5%
(4)	Akamai	362,619	2.8%	Akamai	1,170,836	4.0%
(5)	Yahoo	291,181	2.2%	Facebook	914,088	3.2%
(6)	Cloudflare	220,693	1.7%	Fastly	680,578	2.4%
(7)	Edgecast	123,498	0.9%	WordPress	598,954	2.1%
(8)	Fastly	116,593	0.9%	Twitter	513,694	1.8%
(9)	Highwinds	32,702	0.2%	Cloudflare	423,429	1.5%
(10)	Internap	21,971	0.2%	Microsoft	323,466	1.1%

Google is the **largest** player (with more than half share) in ad and tracking delivery.

Preamble

Web Consolidation

Landing Pages

Web Content

Ads and Trackers

TLS 1.3

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

Recap

# Consolidation of the Web | TLS 1.3

- ▶ **Only** 12% (>50M resources) reveal TLS information in the dataset.
- ▶ Half of the resources over TLS are delivered over TLS 1.3 (while other half over TLS 1.2)
- ▶ Google (>59%), Facebook, and Cloudflare contribute to the majority of TLS 1.3.

	<b>Provider</b>	<b>TLS 1.0</b>	<b>TLS 1.1</b>	<b>TLS 1.2</b>	<b>TLS 1.3 (↓ %)</b>	<b>Identified Resources</b>
(1)	WordPress	0 (0.0%)	0 (0.0%)	0 (0.0%)	692,339 (100.0%)	692,339
(2)	Facebook	0 (0.0%)	0 (0.0%)	8 (0.0%)	3,053,978 (100.0%)	3,053,986
(3)	Google	152 (0.0%)	16 (0.0%)	783,129 (5.0%)	14,914,626 (95.0%)	15,697,923
(4)	Cloudflare	7 (0.0%)	0 (0.0%)	444,503 (17.6%)	2,083,359 (82.4%)	2,527,869
(5)	Highwinds	0 (0.0%)	0 (0.0%)	302,426 (29.8%)	711,909 (70.2%)	1,014,335
(6)	Akamai	6 (0.0%)	0 (0.0%)	1,672,169 (58.3%)	1,194,278 (41.7%)	2,866,453
(7)	Fastly	1 (0.0%)	0 (0.0%)	1,335,349 (92.1%)	114,748 (7.9%)	1,450,098
(8)	—	291,196 (2.2%)	3,329 (0.0%)	11,711,507 (90.3%)	959,160 (7.4%)	12,965,192
(9)	Amazon	35,941 (0.6%)	85 (0.0%)	6,125,713 (97.3%)	130,728 (2.1%)	6,292,467
(10)	NetDNA	0 (0.0%)	0 (0.0%)	677,748 (100.0%)	3 (0.0%)	677,751
	<b>All</b>	<b>332,835 (0.7%)</b>	<b>3,609 (0.0%)</b>	<b>25,225,360 (50.0%)</b>	<b>24,885,884 (49.3%)</b>	<b>50,447,688</b>

Google, Facebook and Wordpress leverage TLS 1.3 almost exclusively (>95%) for content delivery

Hypergiants play a **key** role in deployment of new Internet technologies

Preamble

Web Consolidation

Landing Pages

Web Content

Ads and Trackers

TLS 1.3

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

Recap



# Towards Digital Sovereignty in the Age of Hyper-giants



The Internet is getting centralised

2. Evaluating this recent trend where hyper-giants push to offer new services traditionally delivered by ISPs.

leading to security & privacy concerns

Preamble

Web Consolidation

Landing Pages

Web Content

Ads and Trackers

TLS 1.3

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

Recap

## 1. Age of Hyper-giants

An Empirical View on Consolidation of the Web **TOIT '22**

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

## 2. Towards Digital Sovereignty: Improving Privacy in DNS

Measuring DNS over TCP in the Era of Increasing DNS Response Sizes **CCR '22**

Measuring DNS over TLS from the Edge **PAM '21**

A First Look at DNS over QUIC **PAM '22**

Preamble

Web Consolidation

Landing Pages

Web Content

Ads and Trackers

TLS 1.3

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

Recap

# Age of Hypergiants | 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?

Preamble

Web Consolidation

Landing Pages

Web Content

Ads and Trackers

TLS 1.3

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

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%) CleanBrowsing: 1 (<0.1%)
		355, <i>n</i> = 2 (25.9%)	
		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%) Yandex: 13 (0.5%) Neustar: 2 (0.1%) NextDNS: 2 (0.1%) OpenNIC: 1 (<0.1%)
		811, <i>n</i> = 2 (49.6%)	

>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

Preamble

Web Consolidation

Landing Pages

Web Content

Ads and Trackers

TLS 1.3

DNS Centralisation

Popularity

Path Lengths

Latency

DNS over TCP

Reliability

Response Times

DNS over TLS

Adoption

Reliability

Response Times

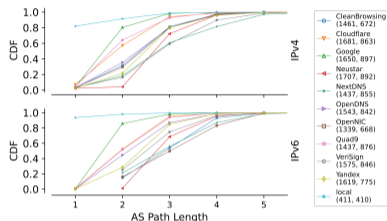
DNS over QUIC

Adoption

Response Times

Recap

# DNS Centralisation | Path Lengths



- ▶ >18% AS paths to ISP resolvers have lengths > 1.
- ▶ >80% AS paths to Google have lengths 2.
- ▶ >90% AS paths to Cloudflare/Quad9 have lengths 3.

Google often directly peers with the ISP.

Google edge caches deployed inside the ISP **do not** (yet) offer public DNS services.

Paths in South America to all public DNS services are **more inflated** than at other regions

Preamble

Web Consolidation

Landing Pages  
Web Content  
Ads and Trackers  
TLS 1.3

DNS Centralisation

Popularity  
Path Lengths

Latency

DNS over TCP

Reliability  
Response Times

DNS over TLS

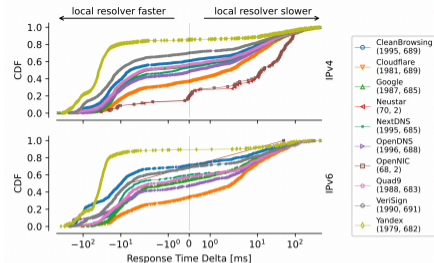
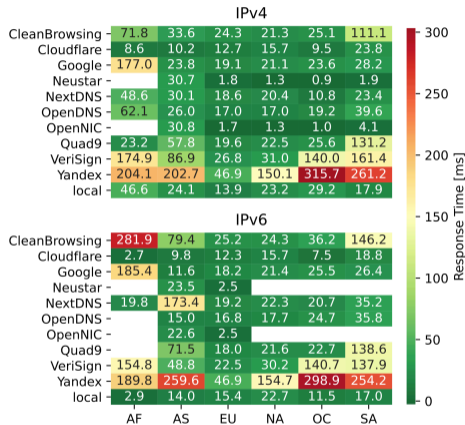
Adoption  
Reliability  
Response Times

DNS over QUIC

Adoption  
Response Times

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.

Preamble

Web Consolidation

Landing Pages

Web Content

Ads and Trackers

TLS 1.3

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

Recap

# Towards Digital Sovereignty in the Age of Hyper-giants

On combating this centralisation trend?

Could new secure (QUIC) and privacy-enhancing protocols (encrypted DNS) be used to give users back *some* control of their data?



Preamble

Web Consolidation

Landing Pages

Web Content

Ads and Trackers

TLS 1.3

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

Recap

## 1. Age of Hyper-giants

An Empirical View on Consolidation of the Web **TOIT '22**

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

## 2. Towards Digital Sovereignty: Improving Privacy in DNS

→ Measuring DNS over TCP in the Era of Increasing DNS Response Sizes **CCR '22**

Measuring DNS over TLS from the Edge **PAM '21**

A First Look at DNS over QUIC **PAM '22**

Preamble

Web Consolidation

Landing Pages  
Web Content  
Ads and Trackers  
TLS 1.3

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

Recap



# Towards Digital Sovereignty | 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 optimizations to reduce DNS response times?

Preamble

Web Consolidation

Landing Pages

Web Content

Ads and Trackers

TLS 1.3

DNS Centralisation

Popularity

Path Lengths

Latency

DNS over TCP

Reliability

Response Times

DNS over TLS

Adoption

Reliability

Response Times

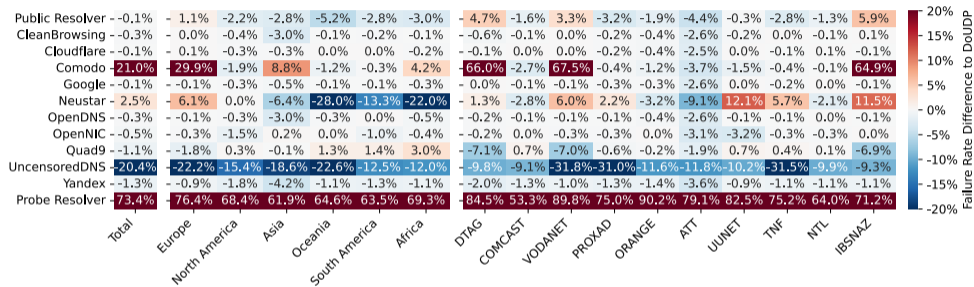
DNS over QUIC

Adoption

Response Times

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.

Preamble

Web Consolidation

Landing Pages

Web Content

Ads and Trackers

TLS 1.3

DNS Centralisation

Popularity

Path Lengths

Latency

DNS over TCP

Reliability

Response Times

DNS over TLS

Adoption

Reliability

Response Times

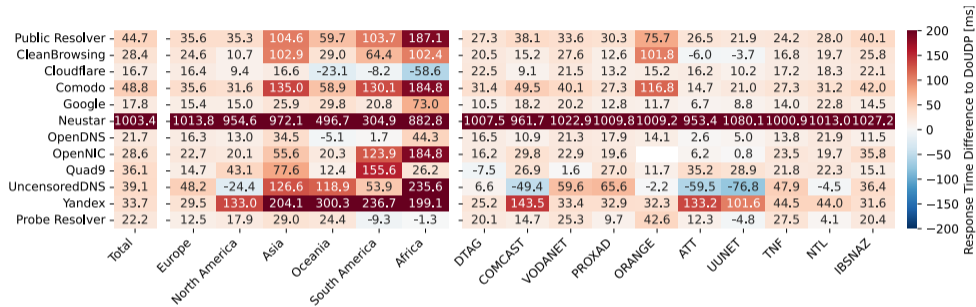
DNS over QUIC

Adoption

Response Times

Recap

# DNS over TCP | Response Times



- ▶ DoTCP is generally slower (37% increase) than DoUDP.
- ▶ TCP optimisations (TFO and TCP keepalives) to reduce latency are not supported.

DoTCP response times are higher but bearable when compared to DoUDP.

- Preamble
- Web Consolidation
  - Landing Pages
  - Web Content
  - Ads and Trackers
  - TLS 1.3
- 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
- Recap

## 1. Age of Hyper-giants

An Empirical View on Consolidation of the Web **TOIT '22**

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

## 2. Towards Digital Sovereignty: Improving Privacy in DNS

Measuring DNS over TCP in the Era of Increasing DNS Response Sizes **CCR '22**

→ Measuring DNS over TLS from the Edge **PAM '21**

A First Look at DNS over QUIC **PAM '22**

Preamble

Web Consolidation

Landing Pages  
Web Content  
Ads and Trackers  
TLS 1.3

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

Recap

# Towards Digital Sovereignty | 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?

Preamble

Web Consolidation

Landing Pages

Web Content

Ads and Trackers

TLS 1.3

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

Recap

- ▶ Step 1: Scan the IPv4 address space for Open DNS resolvers (UDP/53)
- ▶ Step 2: Check DoT support for 1.2M IP endpoints (2019).

	April 2019	January 2020	
DoT Open Resolvers	1,747	2,151	+ 23.1%
Support TLS 1.3	79 (4.5%)	433 (20%)	+ 448%
Support TLS 1.2	1,701 (97%)	2,149 (99.9%)	+ 26.3%
No Support for TLS 1 or 1.1	80 (4.6%)	508 (24%)	+ 535%
Use self-signed cert	11 (0.63%)	355 (17%)	
Use GoDaddy as CA	1,572 (90%)	1,534 (71%)	
Use Let's Encrypt as CA	90 (5.2%)	118 (5%)	

DoT (and subsequently TLS 1.3) adoption has **increased** by >23% (>20%)

Albeit, overall adoption is still **low** (<1%)

Preamble

Web Consolidation

Landing Pages

Web Content

Ads and Trackers

TLS 1.3

DNS Centralisation

Popularity

Path Lengths

Latency

DNS over TCP

Reliability

Response Times

DNS over TLS

Adoption

Reliability

Response Times

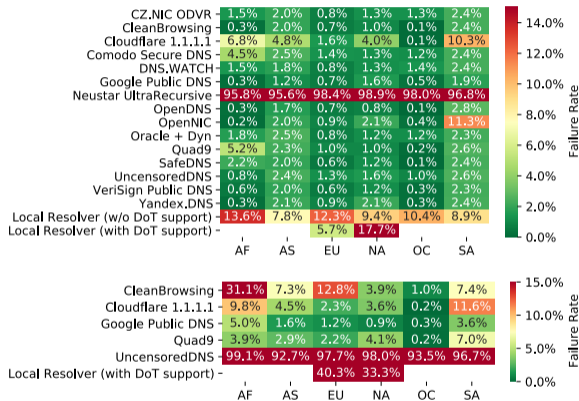
DNS over QUIC

Adoption

Response Times

Recap

# DNS over TLS | Reliability



- ▶ Failures due to timeouts, socket and TCP/TLS errors.
- ▶ DoT failures can be up to >30%
- ▶ Possibly caused by blackholing of DoT packets by middle-boxes.
- ▶ Higher failures in AF and SA.
- ▶ DoT failures higher over local than public resolvers.

DoT exhibits **higher failures** than Do53. Failures are more pronounced over local resolvers.

Preamble

Web Consolidation

- Landing Pages
- Web Content
- Ads and Trackers
- TLS 1.3

DNS Centralisation

- Popularity
- Path Lengths
- Latency

DNS over TCP

- Reliability
- Response Times

DNS over TLS

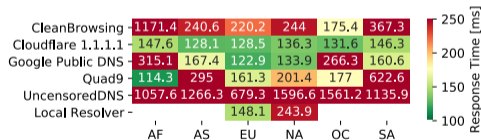
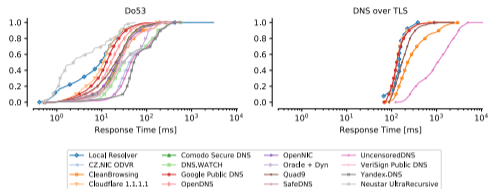
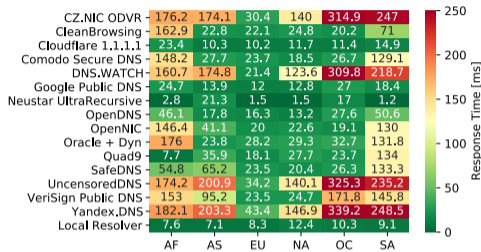
- Adoption
- Reliability
- Response Times

DNS over QUIC

- Adoption
- Response Times

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.

Preamble

Web Consolidation

- Landing Pages
- Web Content
- Ads and Trackers
- TLS 1.3

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

Recap



## 1. Age of Hyper-giants

An Empirical View on Consolidation of the Web **TOIT '22**

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

## 2. Towards Digital Sovereignty: Improving Privacy in DNS

Measuring DNS over TCP in the Era of Increasing DNS Response Sizes **CCR '22**

Measuring DNS over TLS from the Edge **PAM '21**

→ A First Look at DNS over QUIC **PAM '22**

Preamble

Web Consolidation

Landing Pages  
Web Content  
Ads and Trackers  
TLS 1.3

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

Recap

# Towards Digital Sovereignty | 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?

Preamble

Web Consolidation

Landing Pages  
Web Content  
Ads and Trackers  
TLS 1.3

DNS Centralisation

Popularity  
Path Lengths  
Latency

DNS over TCP

Reliability  
Response Times

DNS over TLS

Adoption  
Reliability  
Response Times

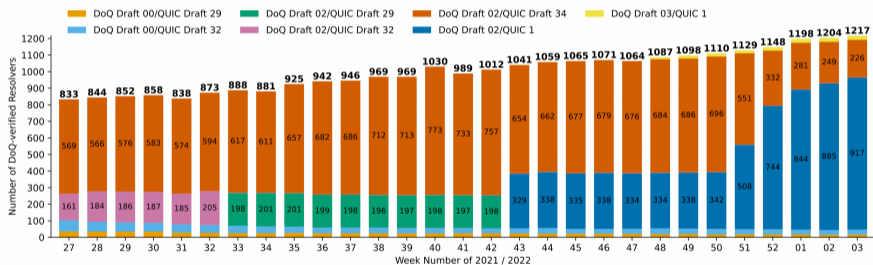
DNS over QUIC

Adoption  
Response Times

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

Preamble

Web Consolidation

Landing Pages

Web Content

Ads and Trackers

TLS 1.3

DNS Centralisation

Popularity

Path Lengths

Latency

DNS over TCP

Reliability

Response Times

DNS over TLS

Adoption

Reliability

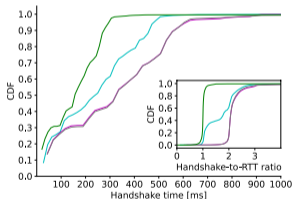
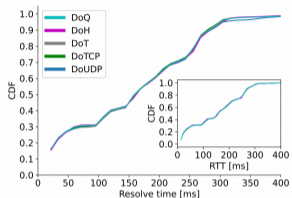
Response Times

DNS over QUIC

Adoption

Response Times

Recap



- ▶ We observed **no support** for TCP keepalives, TFO or 0-RTT.
- ▶ DNS request-response time is comparable across all DoX protocols and **resembles the RTT** of the end-to-end connection.
- ▶ **DoTCP** has the fastest handshake. **DoT and DoH** handshake times are slower and comparable (TCP + TLS 1.3)
- ▶ **Only 20%** DoQ samples match DoTCP handshake times.
- ▶ **40%** DoQ samples exhibit **additional 1 RTT** due to some servers enforcing traffic amplification limits on already validated clients.

DoQ offers the **best** choice for DNS privacy. It **outperforms** both DoT and DoH in latency.

Preamble

Web Consolidation

Landing Pages  
Web Content  
Ads and Trackers  
TLS 1.3

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

Recap

## 1. Age of Hyper-giants

- ▶ **An Empirical View on Consolidation of the Web** TOIT '22  
Hyper-giant penetration has nearly **doubled** from 2015–2020, and is **higher** among more popular domains.
  
- ▶ **Evaluating Public DNS Services in the Wake of Increasing Centralization** NETWORKING '21  
Google edge caches deployed inside the ISP **do not** (yet) offer DNS services. 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.

Preamble

Web Consolidation

Landing Pages  
Web Content  
Ads and Trackers  
TLS 1.3

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

Recap

## 2. Towards Digital Sovereignty: Improving Privacy in DNS

- ▶ **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 adoption has increased year over year, although overall adoption is still **low** (<1%)  
DoT exhibits **higher failures** than Do53, and are more pronounced over local resolvers.  
DoT response times are inflated by **>100 ms** compared to Do53.
- ▶ **A First Look at DNS over QUIC** PAM '22  
DoQ offers the **best** choice for DNS privacy, **outperforms** both DoT and DoH in latency.

Preamble

Web Consolidation

Landing Pages  
Web Content  
Ads and Trackers  
TLS 1.3

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

Recap

TOIT'22

## An Empirical View on Consolidation of the Web

T.V.Doan, R.Rijswijk-Deij, O.Hohlfeld, V.Bajpai

<https://doi.org/10.1145/3503158>

NETWORKING'21

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

T.V.Doan, J.Fries, V.Bajpai

<https://doi.org/10.23919/IFIPNetworking52078.2021.9472831>

CCR'22

## Measuring DNS over TCP in the Era of Increasing DNS Response Sizes

M.Kosek, T.V.Doan, S.Huber, V.Bajpai

<https://doi.org/10.1145/3544912.3544918>

PAM'21

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

T.V.Doan, I.Tsareva, V.Bajpai

[https://doi.org/10.1007/978-3-030-72582-2\\_12](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

M.Kosek, T.V.Doan, M.Grandeath, V.Bajpai

[https://doi.org/10.1007/978-3-030-98785-5\\_24](https://doi.org/10.1007/978-3-030-98785-5_24)

Preamble

Web Consolidation

Landing Pages

Web Content

Ads and Trackers

TLS 1.3

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

Recap