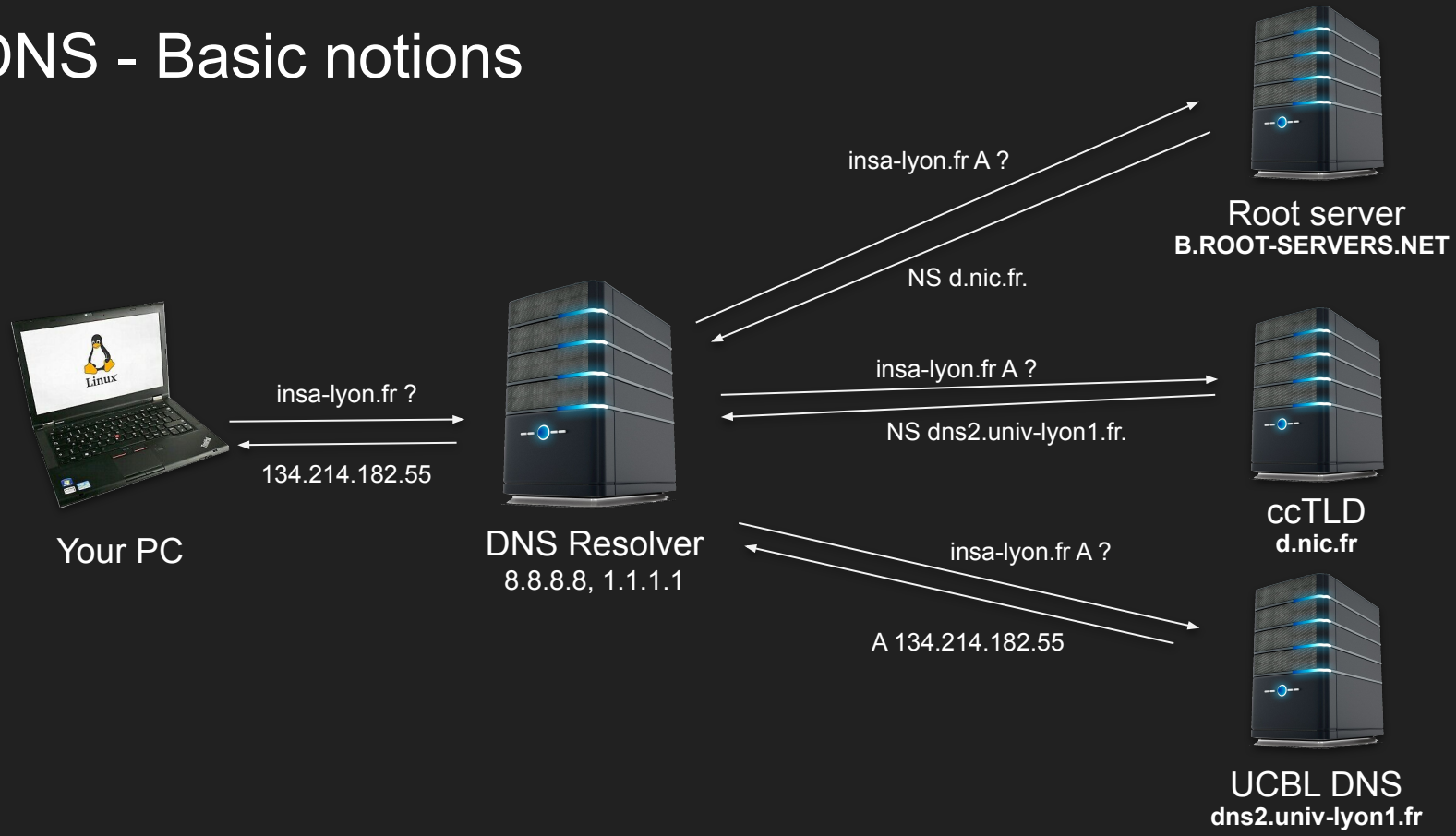
Clouding up the internet

How centralized is DNS traffic becoming ?

Authors : Giovane C. M. Moura, Sebastian Castro, Wes Hardaker, Maarten Wullink, and Cristian Hesselman
Venue : In Proceedings of ACM Internet Measurement Conference (IMC 2020), Virtual Conference.
DOI : https://doi.org/10.1145/3419394.3423625
Conference dates : 27 – 29 October , 2020.

DNS - Basic notions



DNS Record types

A : IPv4 address record

AAAA : IPv6 address record

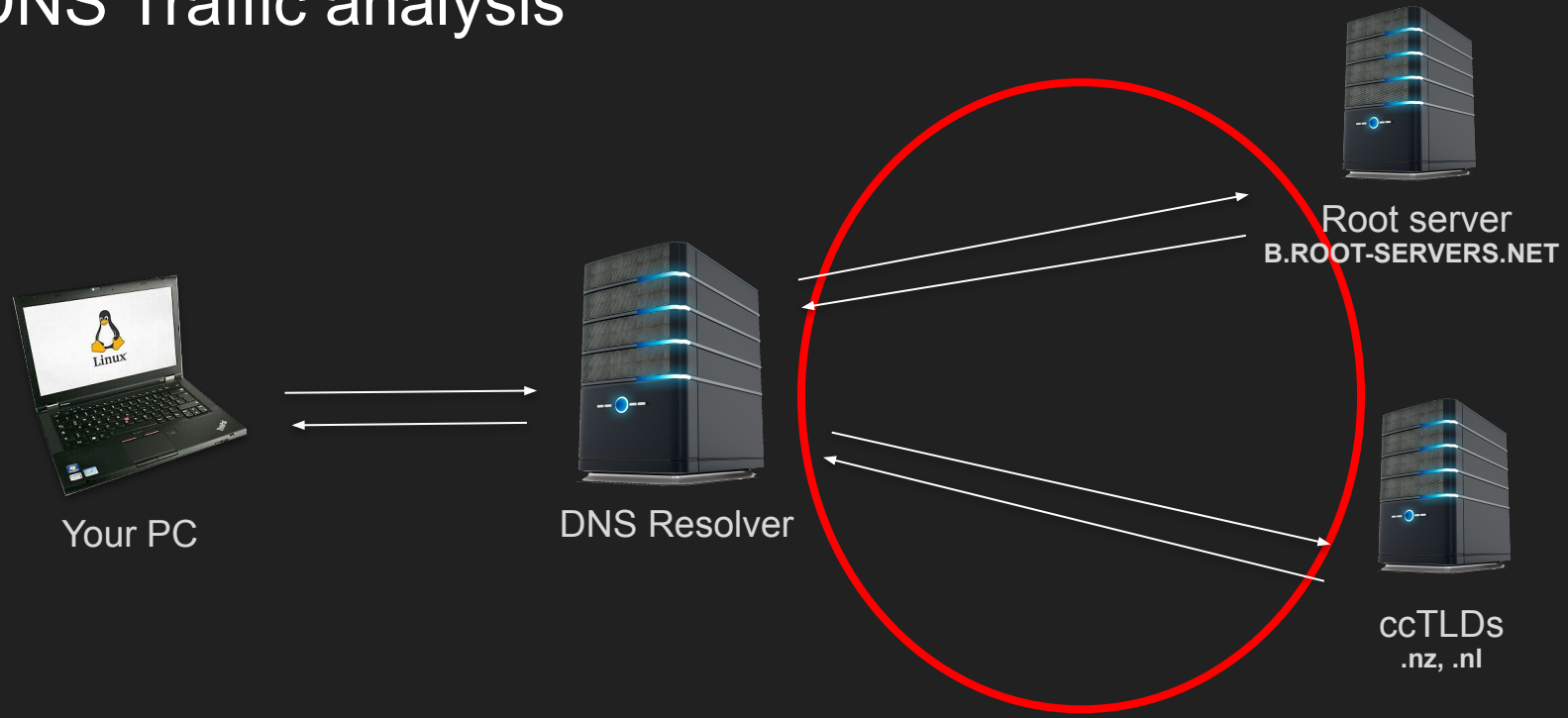
CNAME : Alias

MX : Mail eXchange record

NS : Name Server, gives the address of the subdomain DNS server

DS/DNSKEY : Used for DNSSec (next year in TC ?)

DNS Traffic analysis



Datasets

.nl				
Week	**Queries(total)**	**Queries (valid)**	**Resolvers**	**ASes**
w2018	7.29B	6.53B	2.09M	41276
w2019	10.16B	9.05B	2.18M	42727
w2020	13.75B	11.88B	1.99M	41716
.nz				
Week	**Queries(total)**	**Queries (valid)**	**Resolvers**	**ASes**
w2018	2.95B	2.00B	1.28M	37623
w2019	3.48B	2.81B	1.42M	39601
w2020	4.57B	3.03B	1.31M	38505
B-Root				
Date	**Queries(total)**	**Queries (valid)**	**Resolvers**	**ASes**
2018/04/10	2.68B	0.93B	4.23M	45210
2019/04/09	4.13B	1.43B	4.13M	48154
2020/05/06	6.70B	1.34B	6.01M	51820

Table 3: Evaluated datasets.

- 55.7B request total
- 1 week per year for ccTLDs
- 1 day each year for b-root

NL : 17.1M inhabitants

6M domain names (.nl)

NZ : 4.8 M inhabitants

700k domain names (.nz)

Cloud queries : how concentrated is DNS traffic

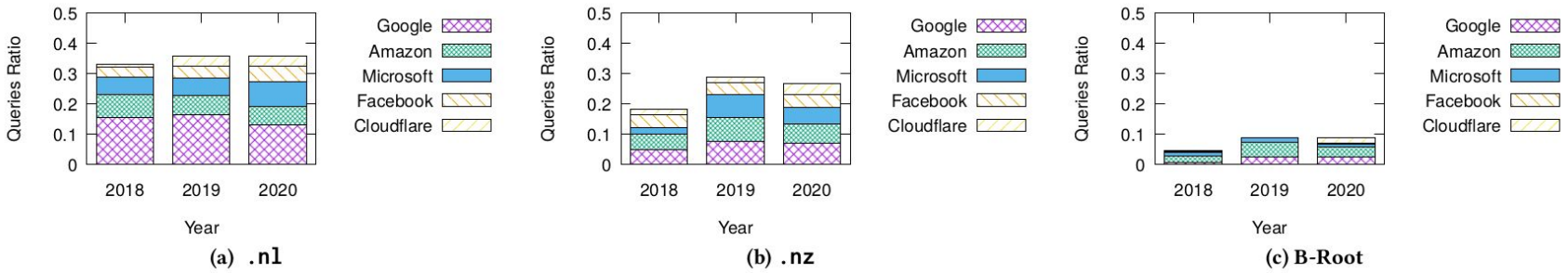
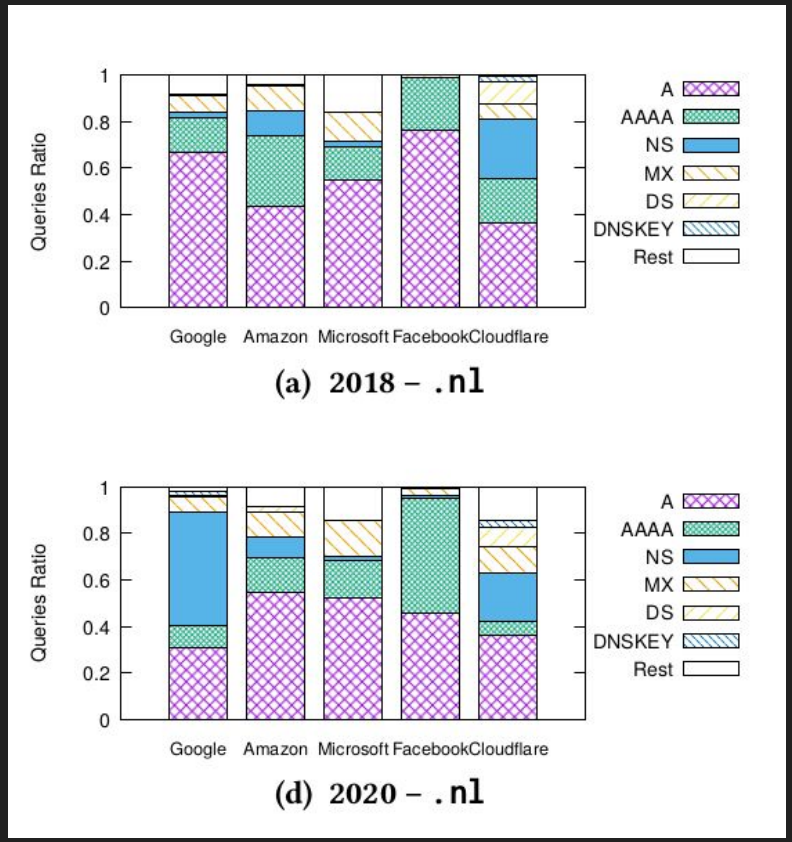


Figure 1: Clouds query ratio per ccTLD and B-Root

- On ccTLDs, ⅓ of the traffic is coming from only 5 providers
- On b-root, it's much less because of junk traffic and the much wider proportion of Resolvers sending Queries to it
- The GAF(A)M(+C) are more and more prevalent in DNS traffic
- Google is less present in .nz than .nl
    - Marker of the popularity of certain services in the country

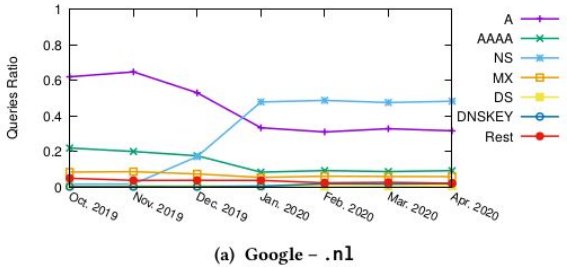
Type of DNS requests

- A (IPv4) record is the most popular one
- At Facebook, AAAA (IPv6) usage increases
- Same trends for .nz
- No DNSSec for Microsoft :’(

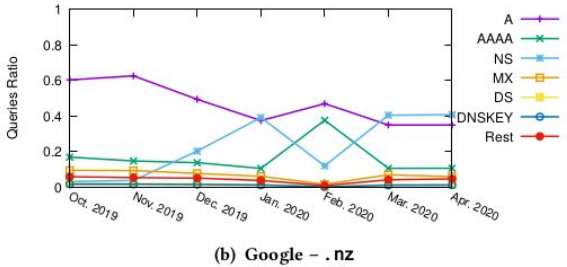


Google DNS traffic queries type

- Why so much NS requests at Google ?
  - Qname minimization optimisation to improve privacy
  - We can determine when it was deployed
  - It’s a great improvement in privacy
- Why the peak in AAAA request in feb ?
  - It’s a misconfiguration on 2 .nz domains which caused cyclic requests
  - Caused Google to issue millions of A & AAAA requests



(a) Google – .nl



(b) Google – .nz

Figure 3: Queries distribution per month for Google.

Proportion of junk traffic

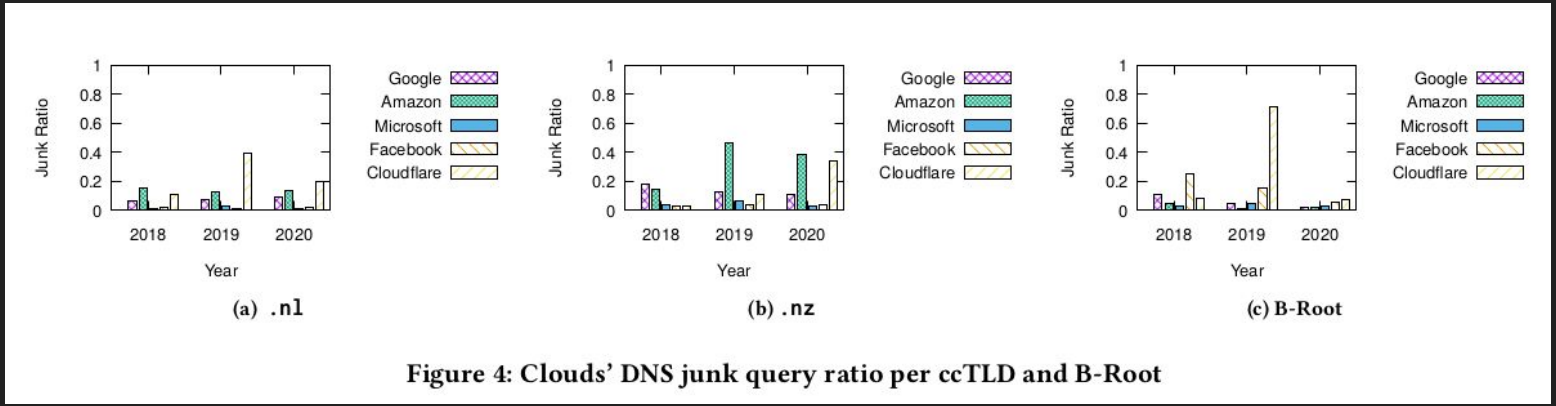
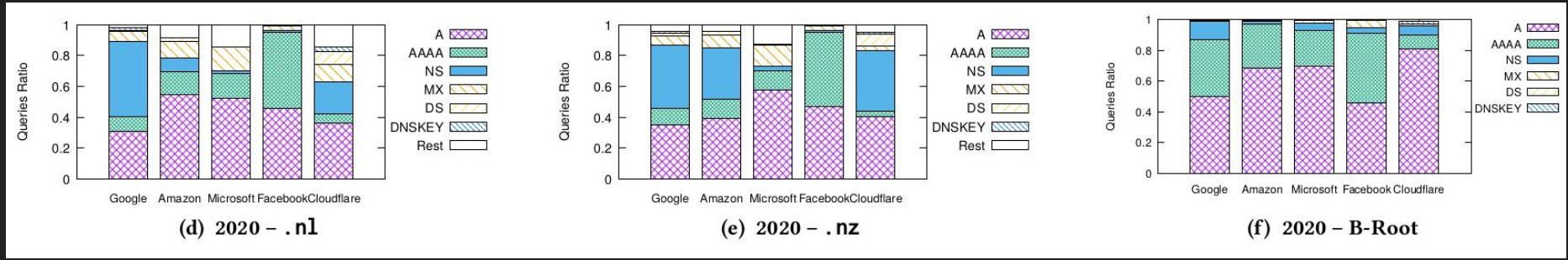


Figure 4: Clouds' DNS junk query ratio per ccTLD and B-Root

- Junk : non RCODE 0, bad queries (errors)
- B-root has the most junk traffic (80% of junk queries overall from all resolvers)
- Because of Chromium which issues bad queries (auto generating non existing TLD names)
- Decreases overall because of NSEC aggressive caching

Adoption of new technologies

DNSSec IPv6 DNS over TCP



- DNSSEC : verify the answers with cryptographically signed answers : uses DNS record types DS and DNSKEY
- Only Microsoft doesn’t validate DNSSEC queries
- More DS than DNSKey for Cloudflare
- Still very low usage in proportion

Adoption of new technologies

DNSSec **IPv6** DNS over TCP

		.nl		.nz	
	Year	IPv4	IPv6	IPv4	IPv6
Google	2018	0.66	0.34	0.61	0.39
	2019	0.49	0.51	0.54	0.46
	2020	0.52	0.48	054	0.46
Amazon	2018	1	0	1	0
	2019	0.98	0.02	0.97	0.03
	2020	0.97	0.03	0.96	0.04
Microsoft	2018	1	0	1	0
	2019	1	0	1	0
	2020	1	0	1	0
Facebook	2018	0.52	0.48	0.51	0.49
	2019	0.24	0.76	0.19	0.81
	2020	0.24	0.76	0.17	0.83
Cloudflare	2018	0.54	0.46	0.54	0.46
	2019	0.57	0.43	0.56	0.44
	2020	0.51	0.49	0.49	0.51

IPv4 and IPv6 queries proportion

- IPv6 Adoption
  - 50/50 : Google and Cloudflare
  - More IPv6 : Facebook
    - Seeks performance
  - Less IPv6 : Microsoft and Amazon
    - Small numbers of Resolvers are IPv6

	.nl	.nz
Amazon	38317	34645
IPv4	37640 (98.2%)	33908 (97.9%)
IPv6	677 (1.8%)	737 (2.1%)
Microsoft	14494	10206
IPv4	14069 (97.0%)	9738 (95.4%)
IPv6	425 (3.0%)	468 (4.6%)

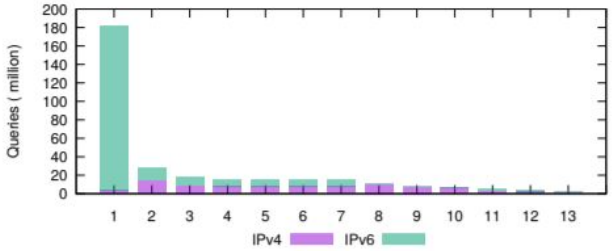
Table 3: Amazon and Microsoft resolvers (Week 2020)

Adoption of new technologies

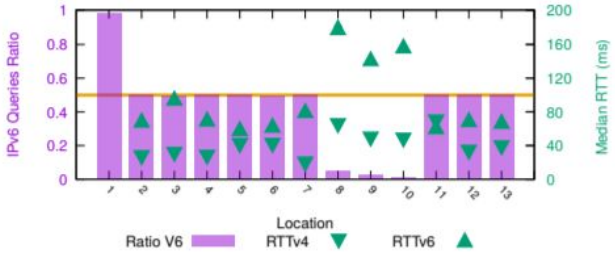
DNSSec **IPv6** DNS over TCP

Why so much IPv6 for Facebook ?

- Location 1, mostly UDP, uses IPv6
- Other locations use one or the other depending on latency



(a) Facebook Location vs Queries to .nl's Server A (w2020).

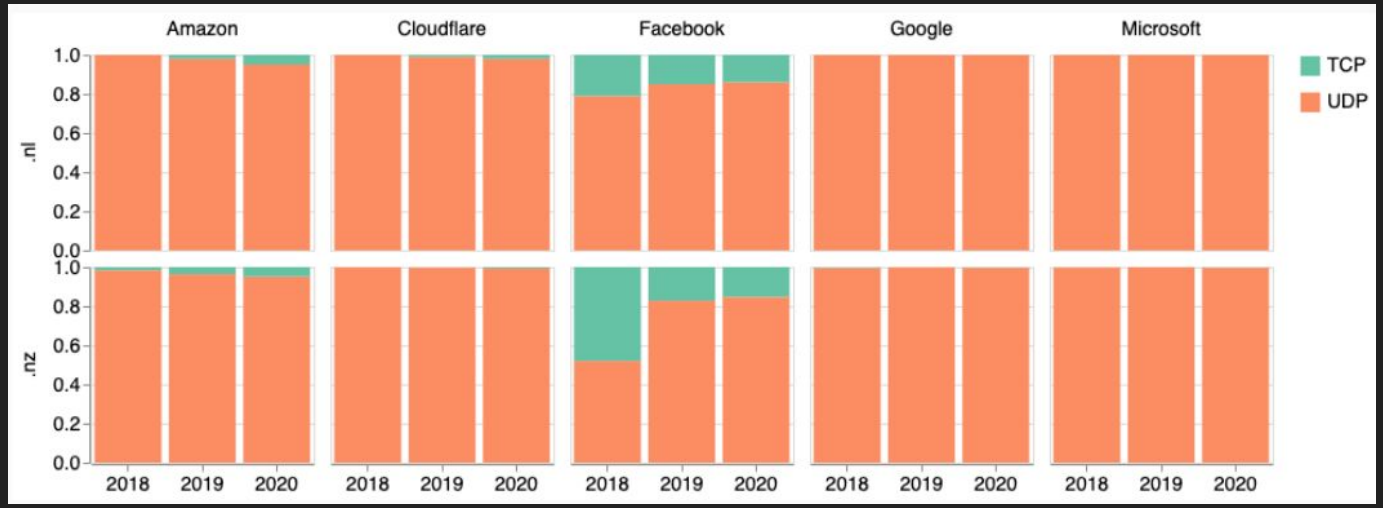


(b) Ratio queries IPv6 and RTT to Server A of .nl in w2020.

Figure 5: Facebook Resolver's location and IPv4 and IPv6 usage when querying .nl's Server A (w2020) .

Adoption of new technologies

DNSSec IPv6 **DNS over TCP**



- TCP has to be supported by the DNS server, but it’s not widely used
- We can’t use UDP for DNS when the answer is too long : it truncates it
  - Request is issued again using TCP
- Facebook had more answers truncated, thus more DNS over TCP requests

Related work / Conclusion

- These DNS analysis have already been done, but not broken down by Cloud provider
- We can measure exactly when Google has deployed Qmin, which has never been done
- These analysis by CP have not been conducted on root DNS servers yet
- We take the side of authoritative servers and not users, which gives another perspective

- Pros of concentration :
  - Deployment of security or privacy features from one CP benefits to a large number of users at once
- Cons of concentration :
  - “single point of failure” => one incident can affect many users at once