

How does CZ DNS anycast work?

upgrade & analysis

Zdeněk Brůna • zdenek.bruna@nic.cz • 28.05.2019

Basics for .CZ DNS anycast

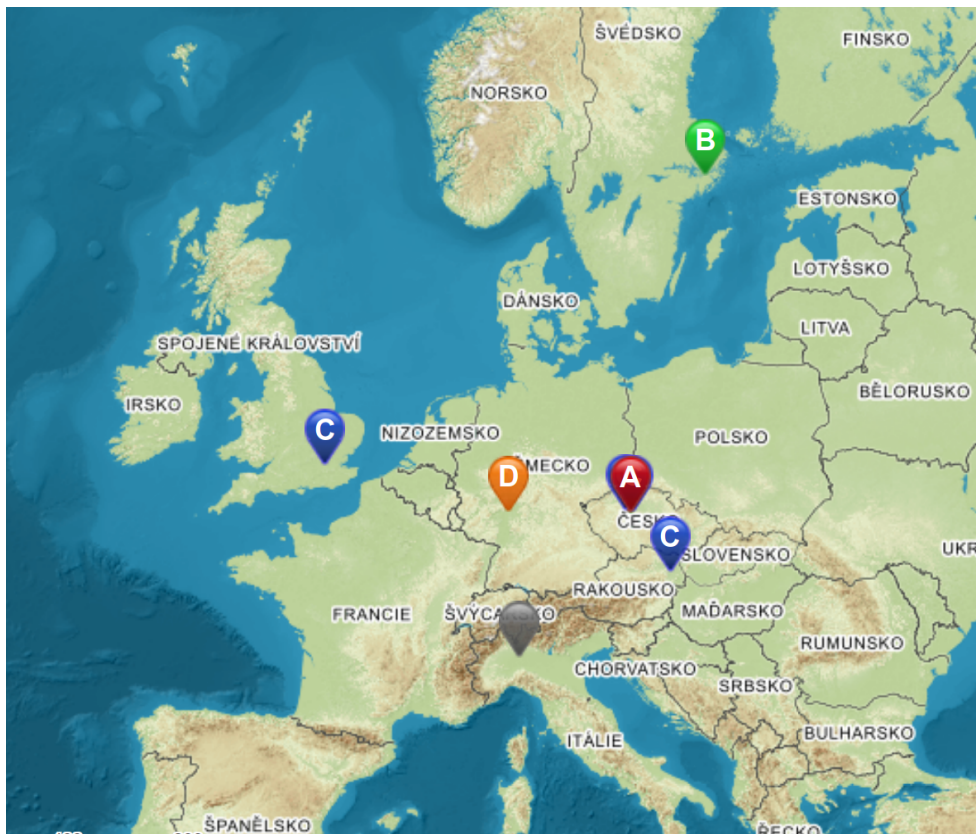
- more servers with one IP address
- BGP routes requests to nearest location
- load balancing, latency reduction
- automated traffic redirection during outages
- optimal distribution of DNS servers



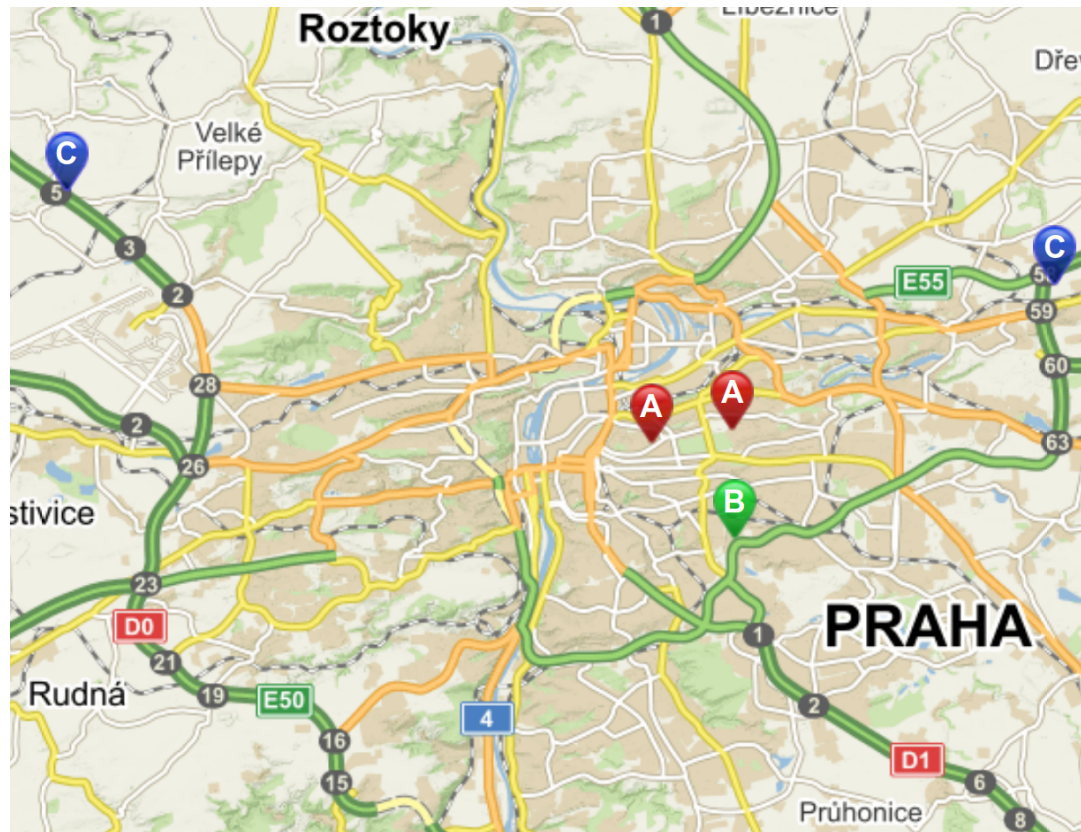
Basics for .CZ DNS anycast



Basics for .CZ DNS anycast



Basics for .CZ DNS anycast



Basics for .CZ DNS anycast

- **Asia**

- [JP] Tokyo

- **Europe**

- [AT] Vienna
- [CZ] 5 x Prague, 1 x Undisclosed location
- [DE] 2 x Frankfurt
- [SE] Stockholm
- [UK] London
- [IT] Milan

- **North America**

- [US] California, Virginia

- **South America**

- [BR] Sao Paulo
- [CL] Santiago de Chile

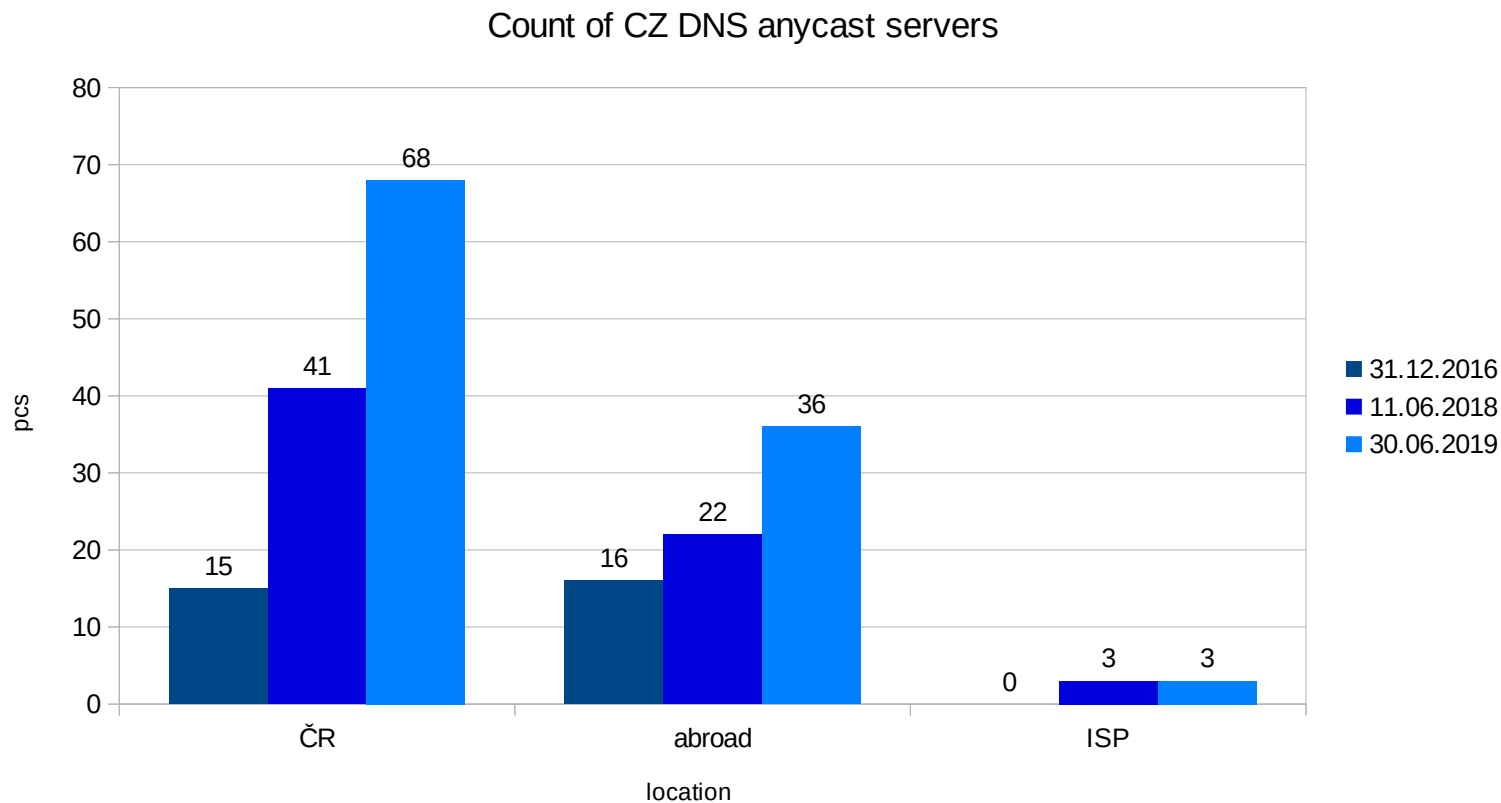
17 locations

10 countries

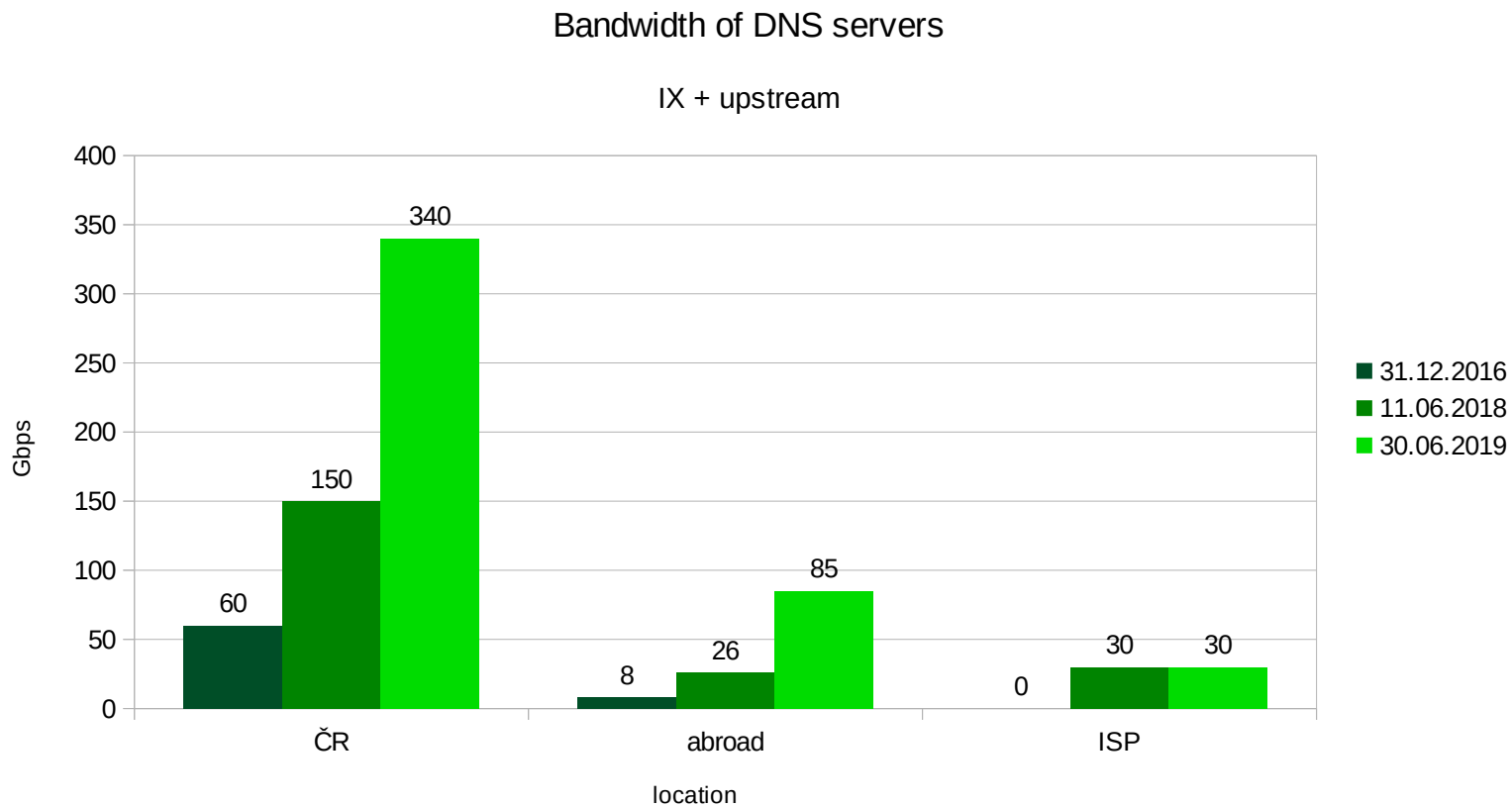
4 continents



Upgrade results



Upgrade results



Upgrade results

- performance limits
- ~ 20 000 000 -> 200 000 000 QPS
- ~ 60+ -> 400+ Gbps



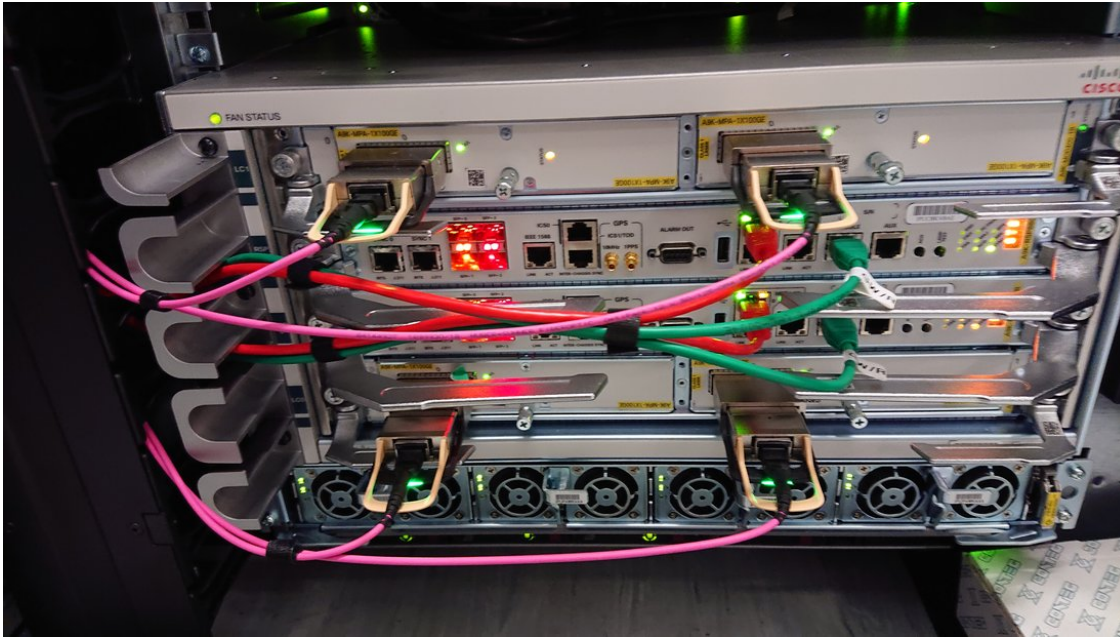
Upgrade results

1. 100 Gbps DNS stack



Upgrade results

2. 100 Gbps DNS stack

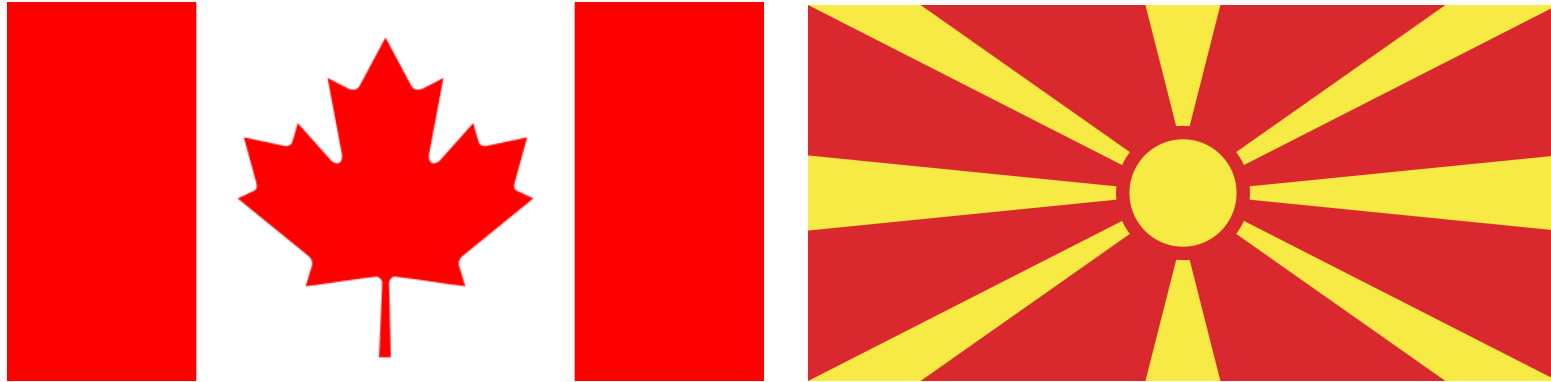


Performance is not the only one

- diversity
 - HW vendors
 - SW
 - OS (Ubuntu / Debian / OpenBSD)
 - BGP (BIRD / BGPD / QUAGGA)
 - DNS (KNOT / BIND / NSD)
- locations
 - geographical
 - different networks (**ISP**)



Sharing of the DNS infrastructure



Where to put another DNS servers?



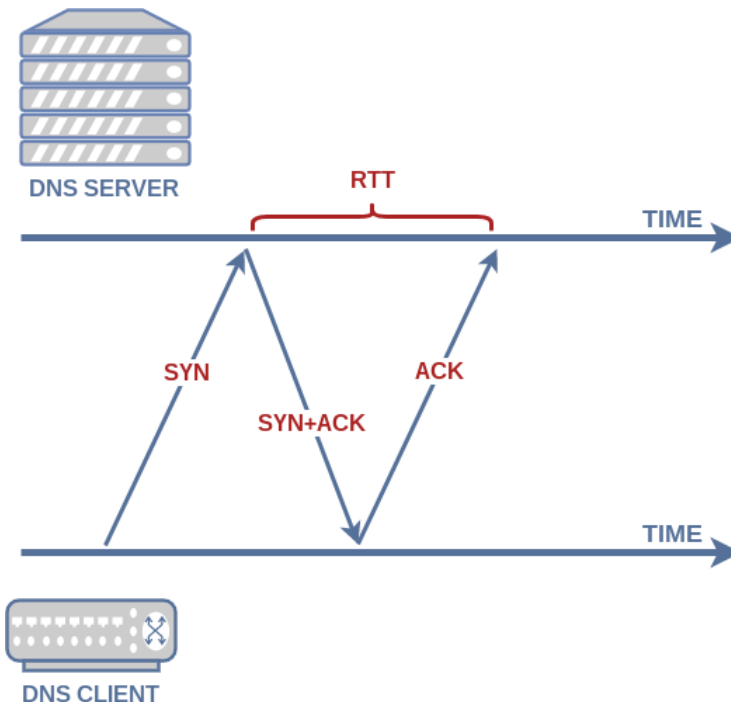
Where to put another DNS servers?

- Who sends queries to our servers?
- How long does it take for a query to reach our server?
 - typically active measurement (PING – DNS server vs. client or probe)
 - we used ADAM (Advanced DNS Analysis and Monitoring) and passive analysis
 - captured DNS traffic from .CZ DNS anycast (1.-14.5.2019)
 - ~15,65 billion+ queries
 - UDP 99.87% ~ 15,63 billion queries
 - **TCP: 0.13% ~ 21 million queries**



Where to put another DNS servers?

- median RTT of a TCP handshake for each pair (client + server)
- evaluated RTT for each:
 - client
 - network
 - country
 - ...



Where to put another DNS servers?

For each pair (client, server) compute median RTT of a TCP handshake

client_ip	client_cc	client_asn	server	queries	tcp	median_rtt
217.31.193.164	CZ	25192	[Europe] AT, Vienna	37123	0	NA
217.31.193.164	CZ	25192	[Europe] CZ, Undisclosed	5171434	57	12.7 ms
217.31.193.164	CZ	25192	[Europe] CZ, Praha – CECOLO	2579707	6	11.9 ms
217.31.193.164	CZ	25192	[Europe] CZ, Praha - CRA	27065563	220	11.5 ms
217.31.193.164	CZ	25192	[Europe] UK, London	8416765	88	43.4 ms

Total number of
DNS queries
(UDP+TCP)

Number of
captured TCP
sessions



Where to put another DNS servers?

Evaluated RTT = weighted mean of RTT for all servers

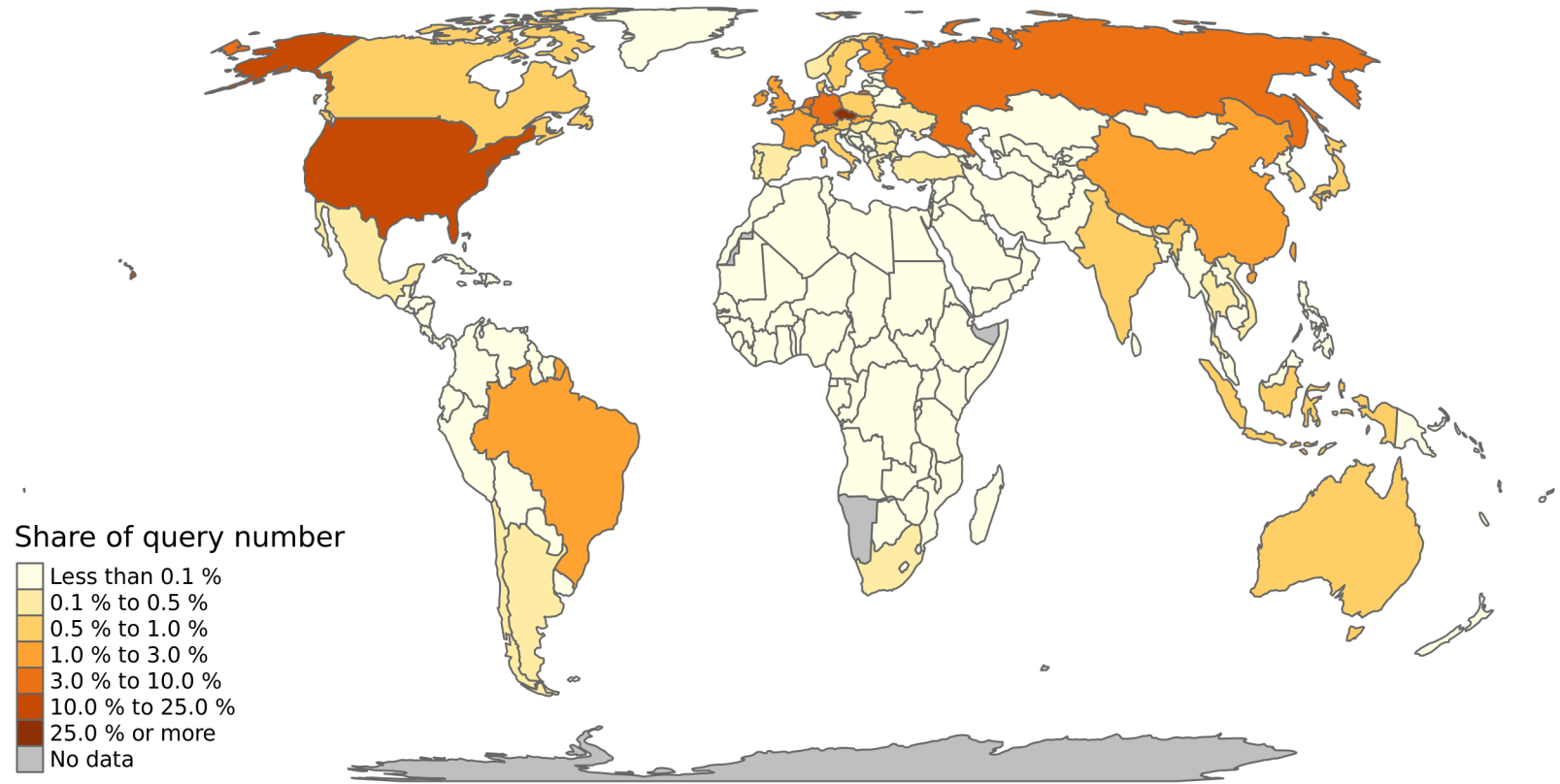
client_ip	client_cc	client_asn	server	queries	median_rtt	weight
217.31.193.164	CZ	25192	[Europe] AT, Vienna	37123	NA	0.000858
217.31.193.164	CZ	25192	[Europe] CZ, Undisclosed	5171434	12.7 ms	0.120
217.31.193.164	CZ	25192	[Europe] CZ, Praha – CECOLO	2579707	11.9 ms	0.0596
217.31.193.164	CZ	25192	[Europe] CZ, Praha - CRA	27065563	11.5 ms	0.625
217.31.193.164	CZ	25192	[Europe] UK, London	8416765	43.4 ms	0.195

$$RTT = \sum_{i=1}^n \text{Norm}(w_i) \cdot RTT_i \quad \text{for } RTT_i \neq NA$$

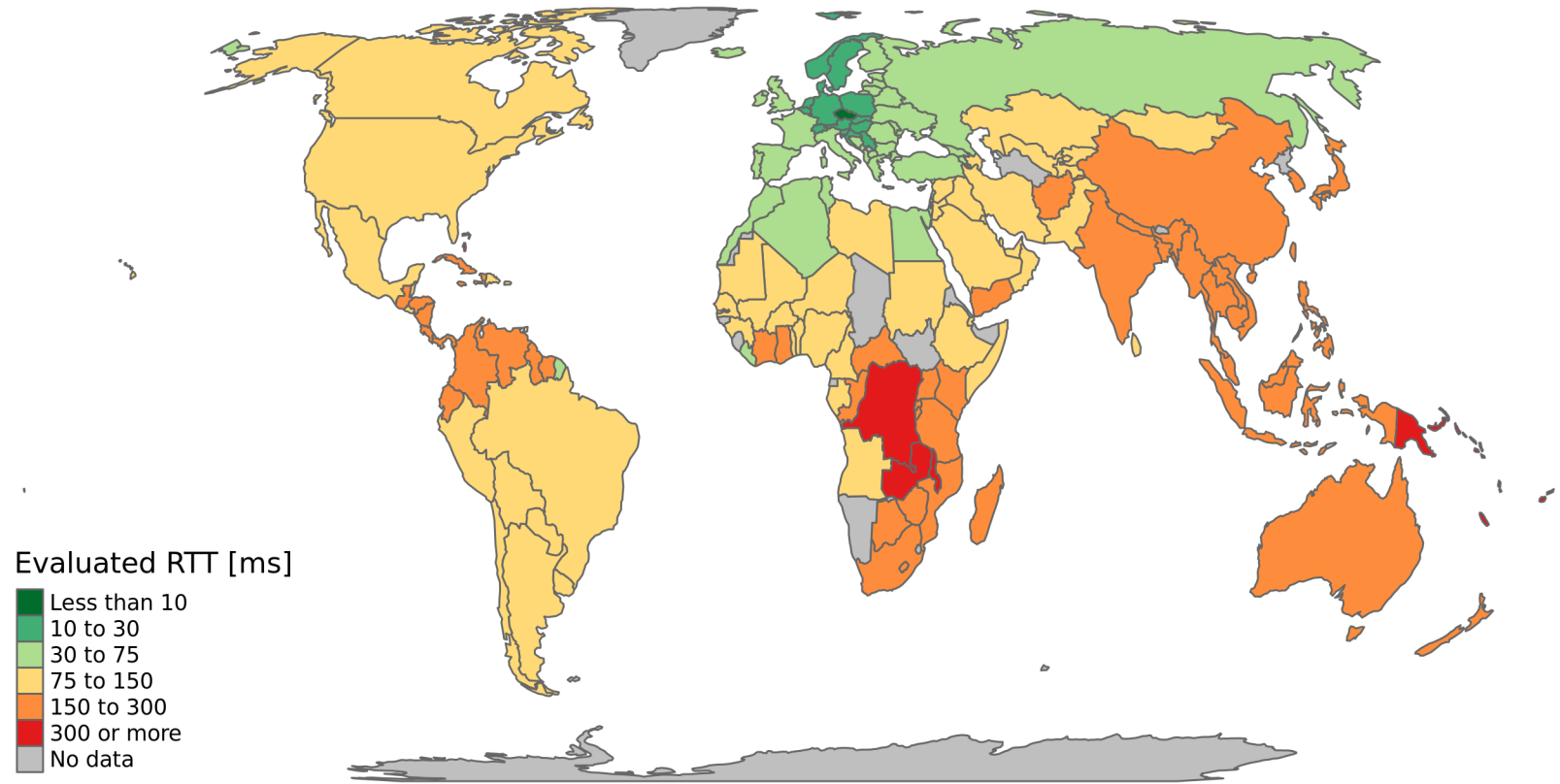
Evaluated RTT for 217.31.193.164 = 17.9 ms



Where to put another DNS servers?



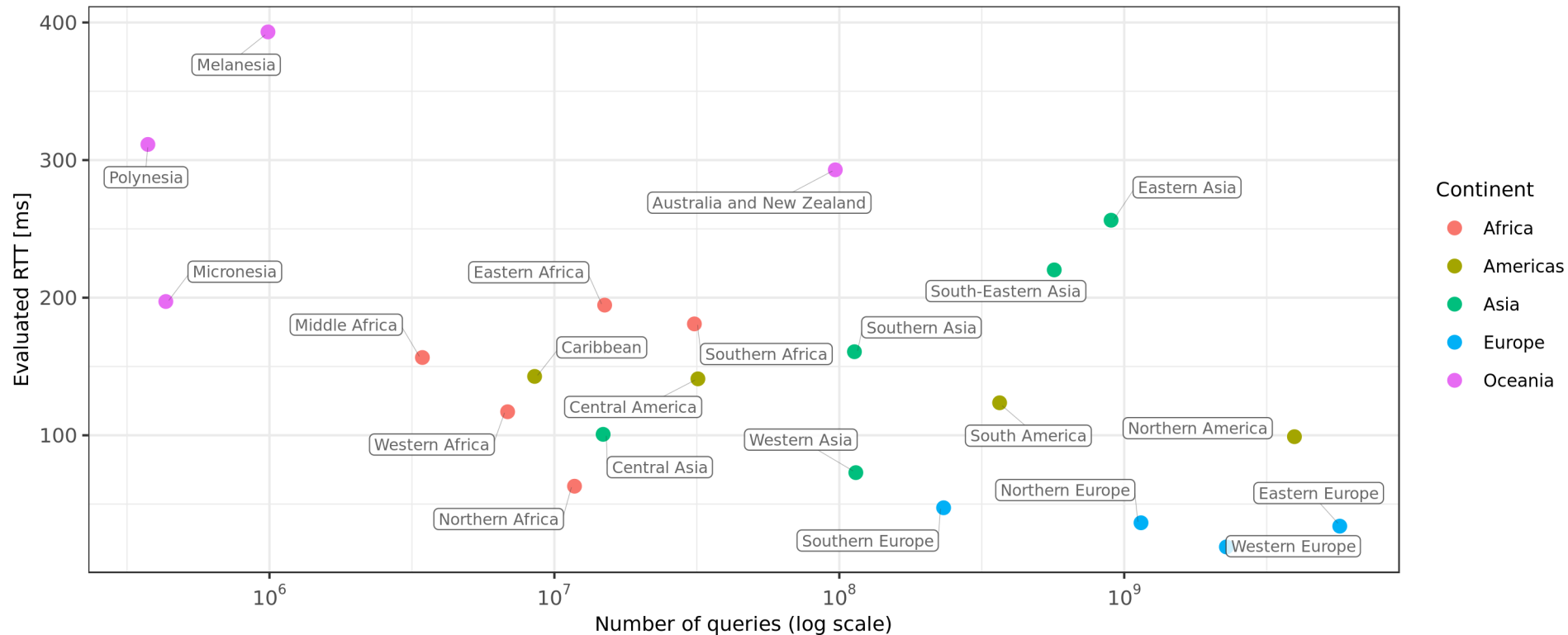
Where to put another DNS servers?



Where to put another DNS servers?

Number of queries vs evaluated RTT by region

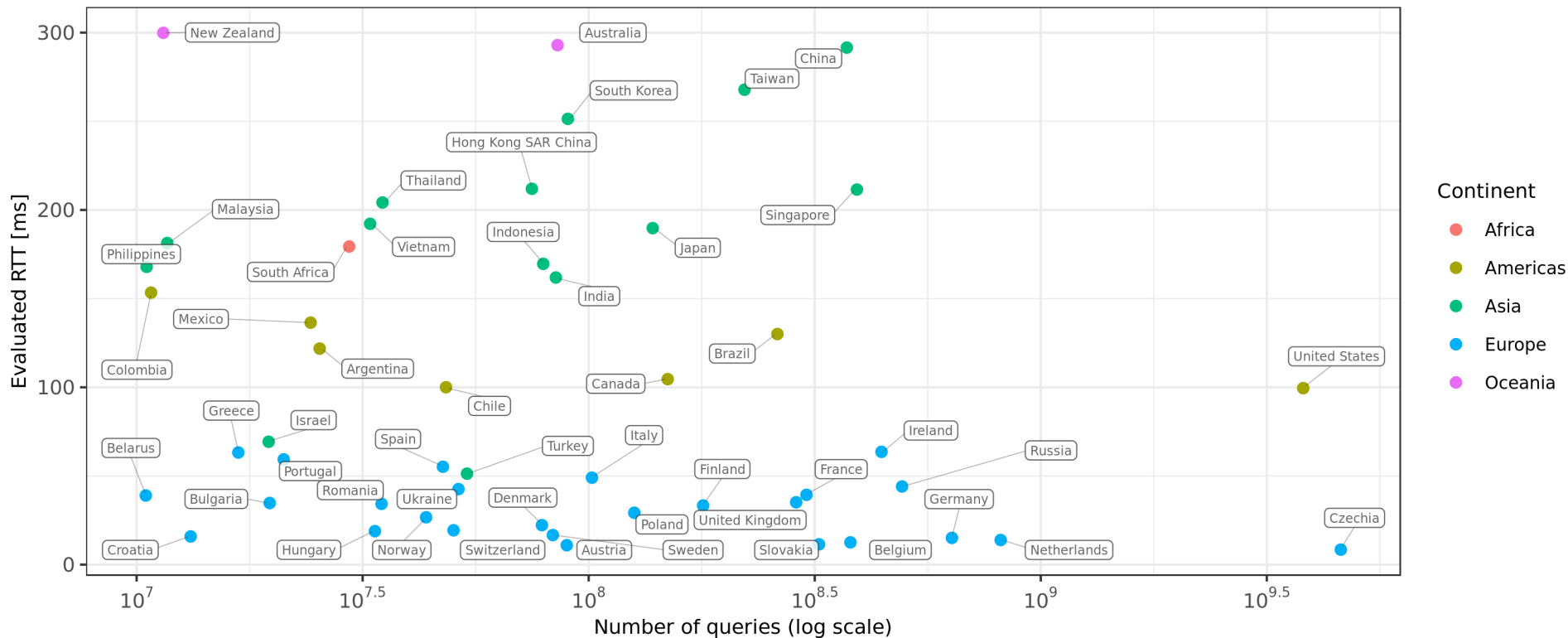
For DNS traffic captured on 1-14 May 2019



Where to put another DNS servers?

Number of queries vs evaluated RTT for top 50 countries by query number

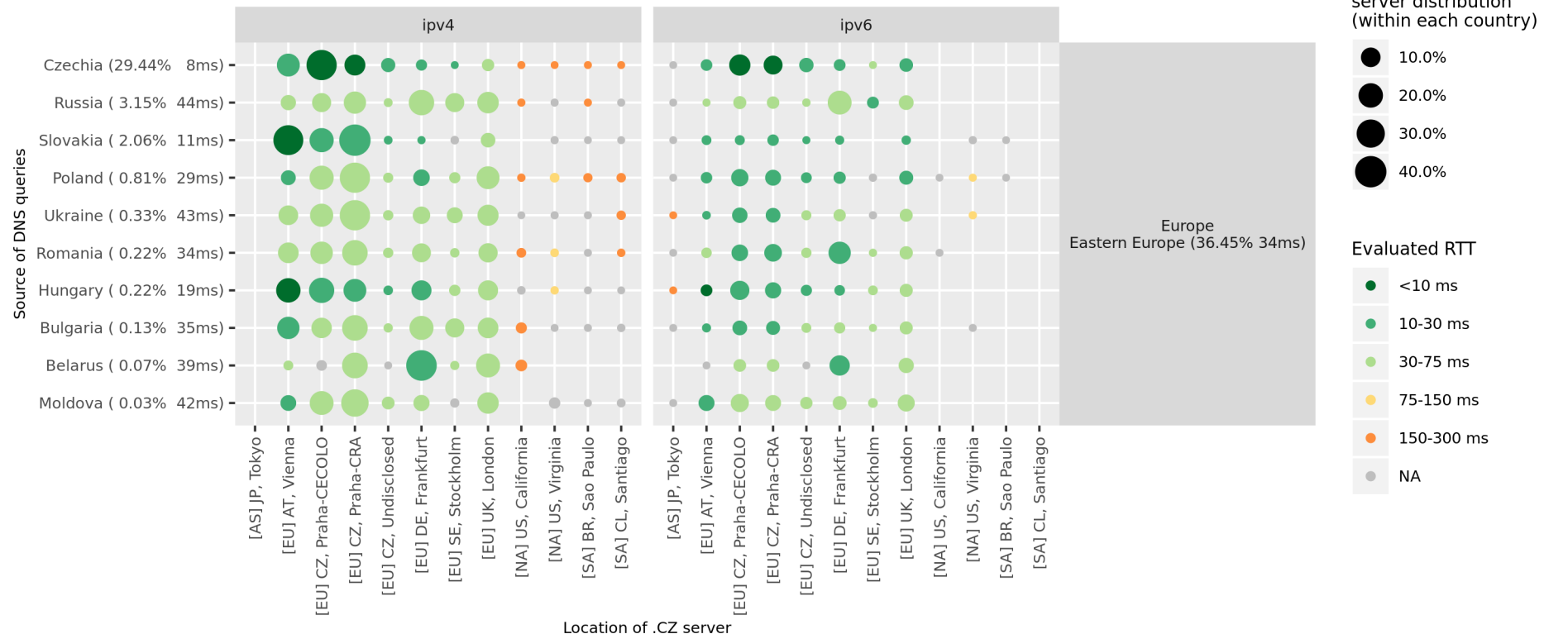
For DNS traffic captured on 1-14 May 2019



Where to put another DNS servers?

DNS traffic distribution vs evaluated RTT for countries in Eastern Europe (with min. 0.01% share in traffic)

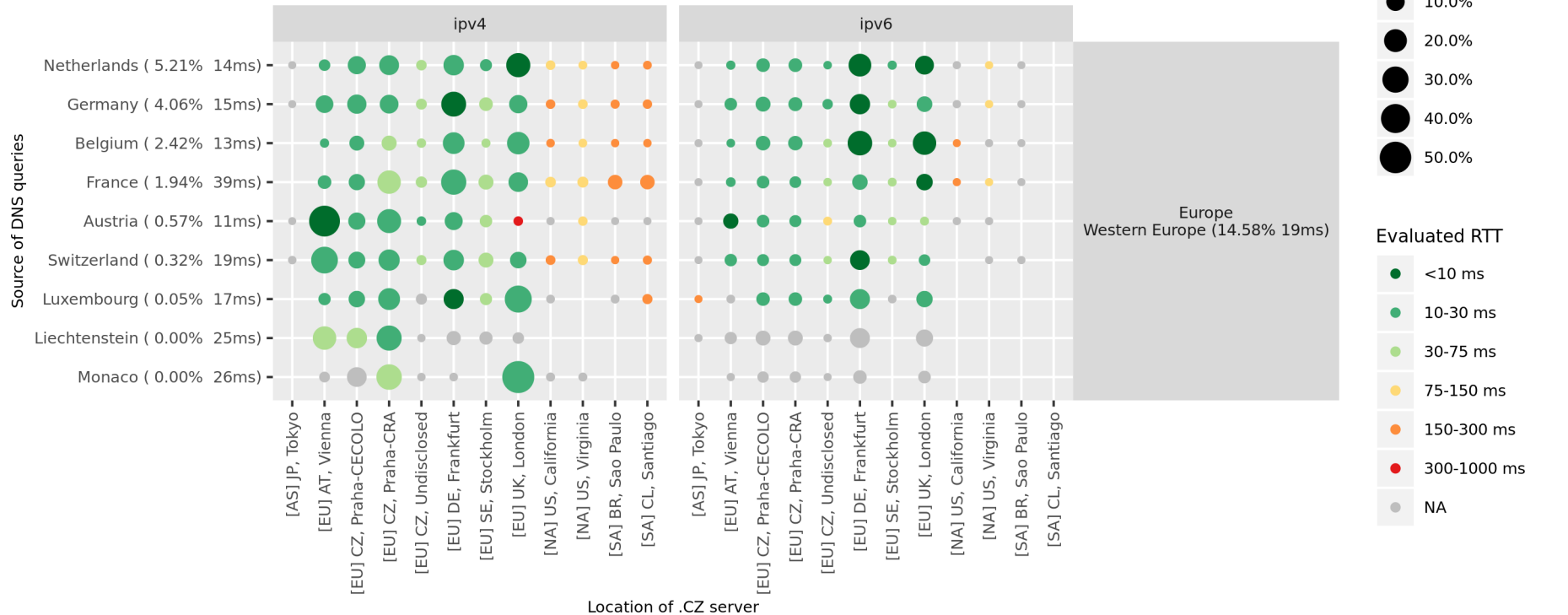
For DNS traffic captured on 1-14 May 2019



Where to put another DNS servers?

DNS traffic distribution vs evaluated RTT for countries in Western Europe

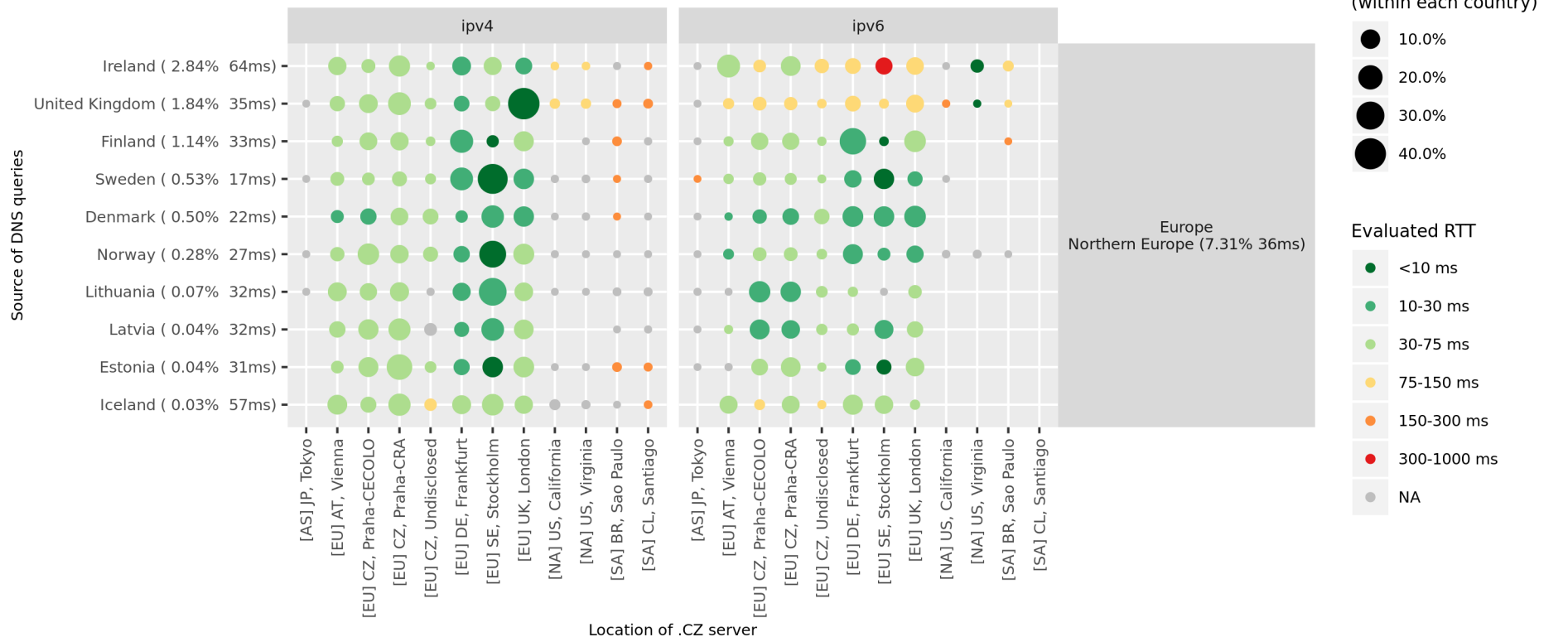
For DNS traffic captured on 1-14 May 2019



Where to put another DNS servers?

DNS traffic distribution vs evaluated RTT for countries in Northern Europe (with min. 0.01% share in traffic)

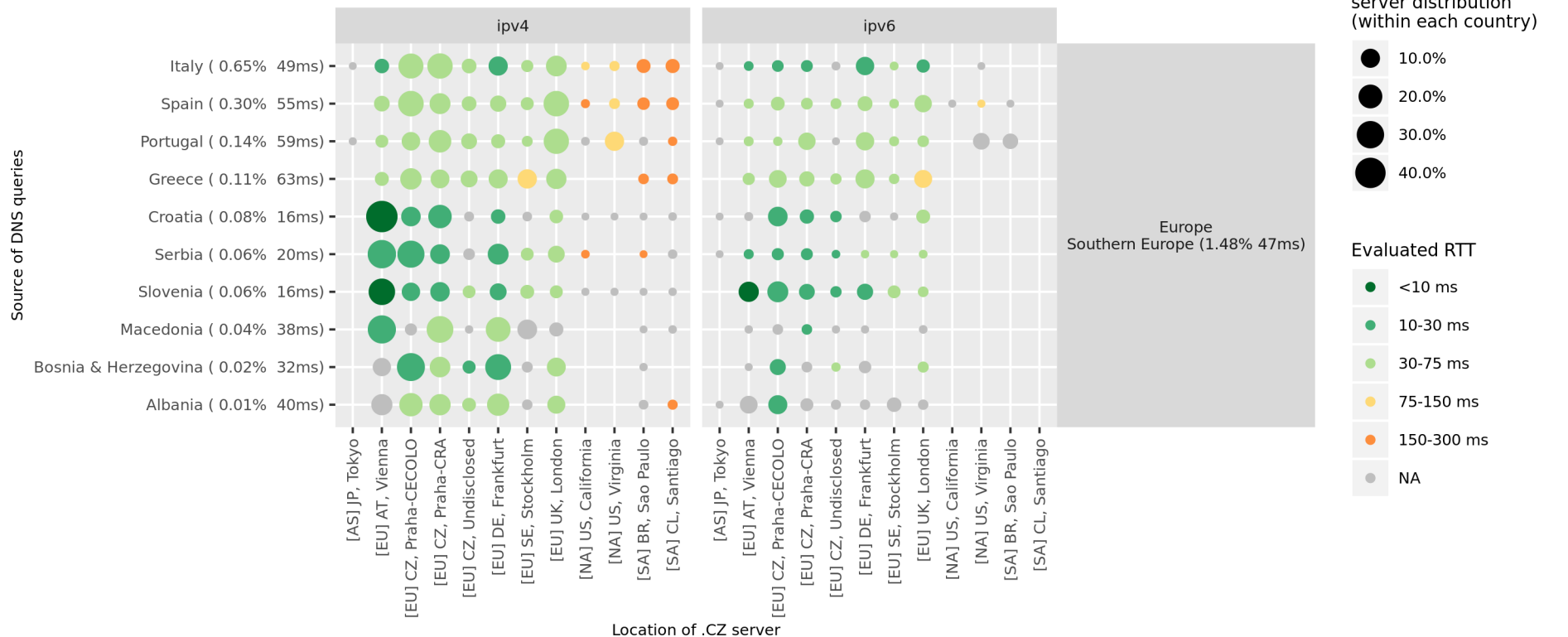
For DNS traffic captured on 1-14 May 2019



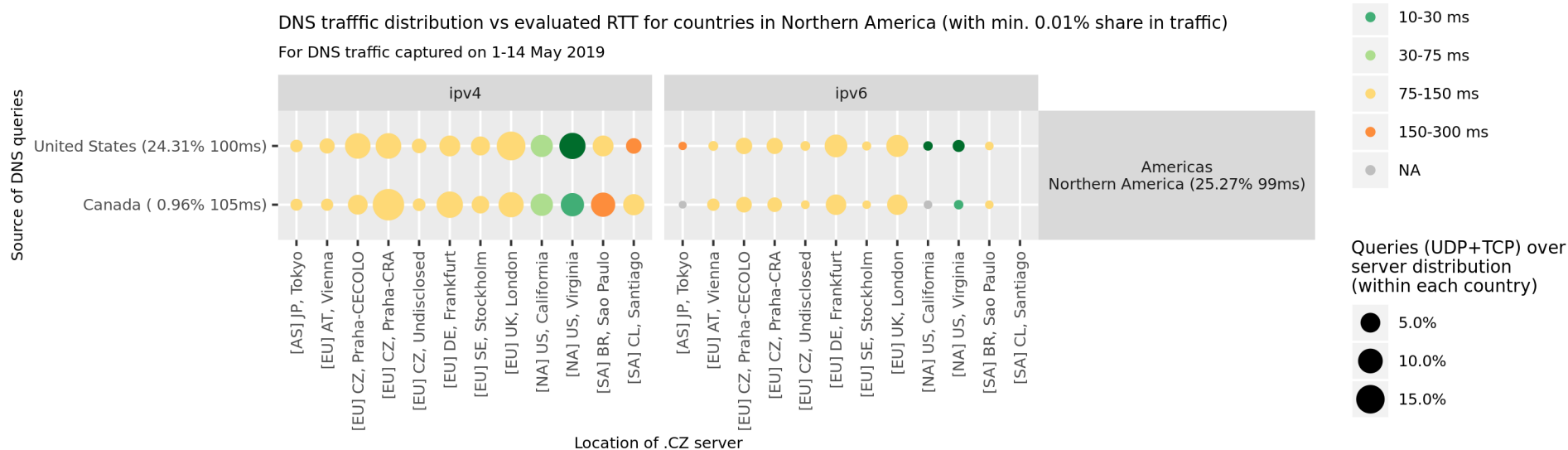
Where to put another DNS servers?

DNS traffic distribution vs evaluated RTT for countries in Southern Europe (with min. 0.01% share in traffic)

For DNS traffic captured on 1-14 May 2019



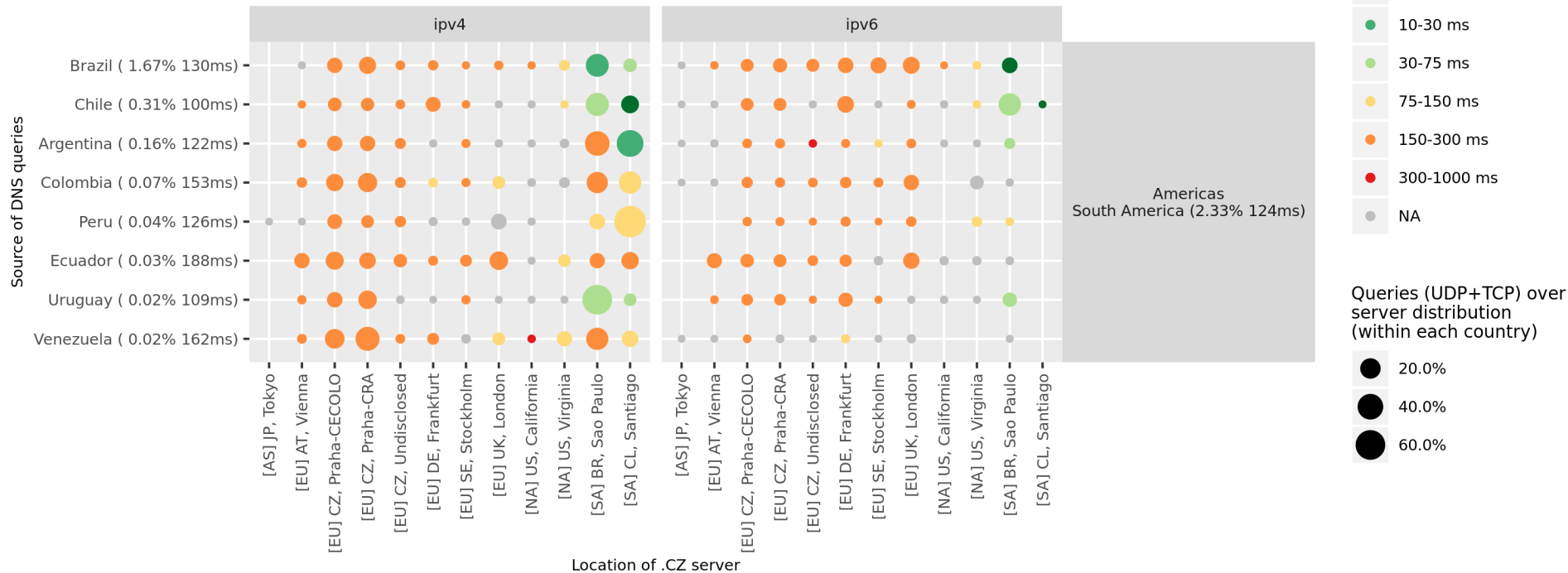
Where to put another DNS servers?



Where to put another DNS servers?

DNS traffic distribution vs evaluated RTT for countries in South America (with min. 0.01% share in traffic)

For DNS traffic captured on 1-14 May 2019



Where to put another DNS servers?

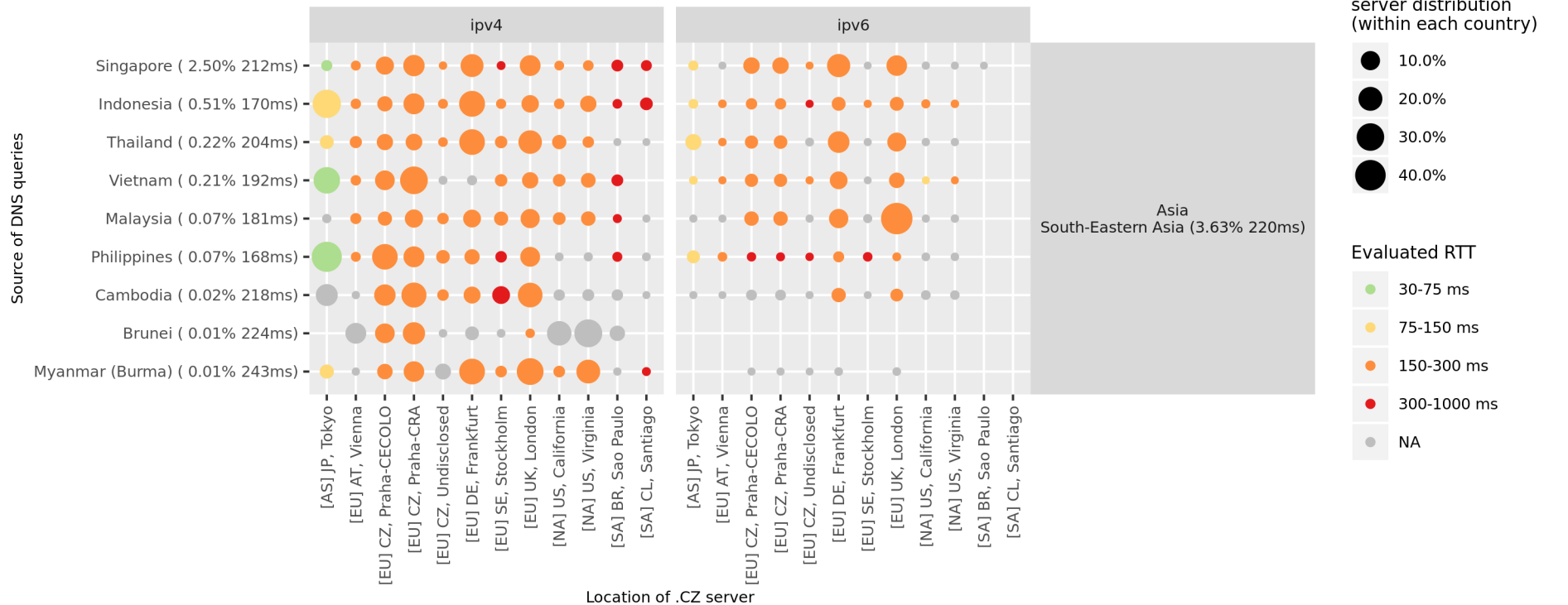
DNS traffic distribution vs evaluated RTT for countries in Eastern Asia (with min. 0.01% share in traffic)
For DNS traffic captured on 1-14 May 2019



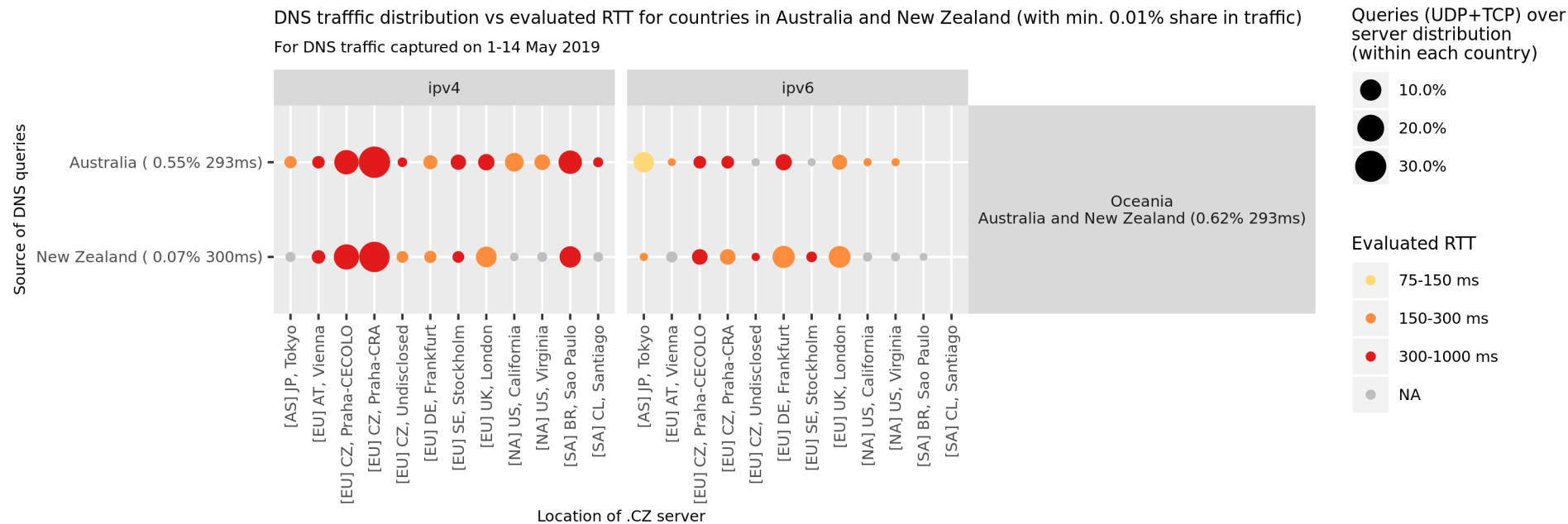
Where to put another DNS servers?

DNS traffic distribution vs evaluated RTT for countries in South-Eastern Asia (with min. 0.01% share in traffic)

For DNS traffic captured on 1-14 May 2019



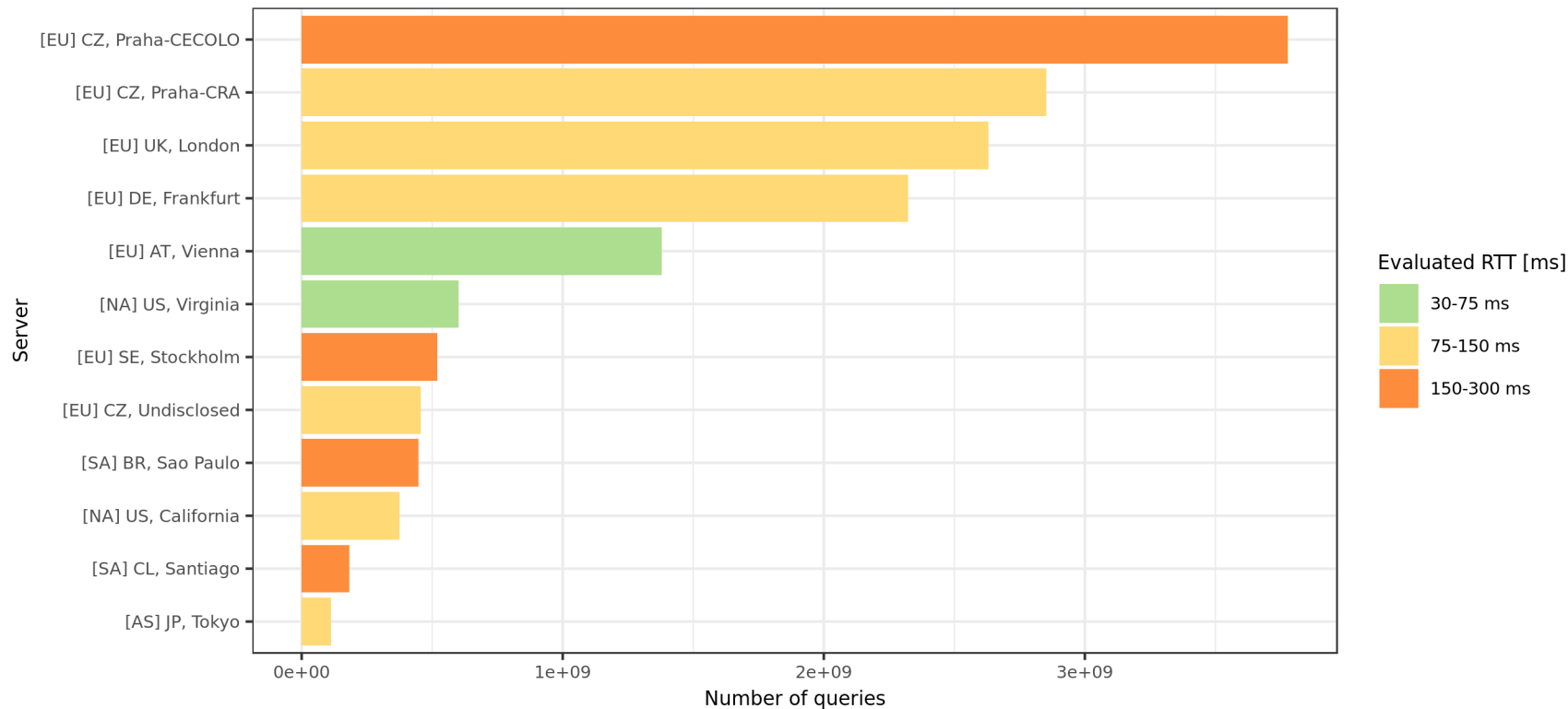
Where to put another DNS servers?



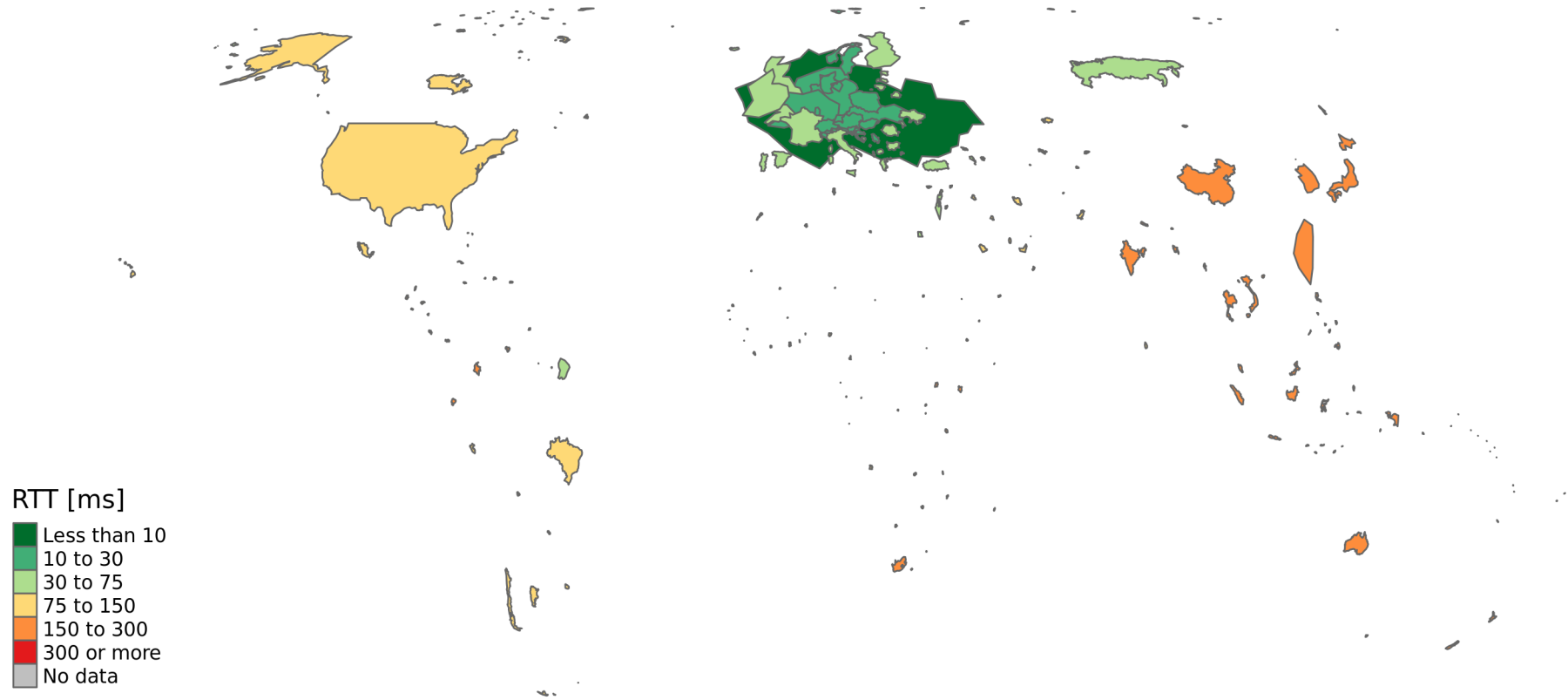
Where to put another DNS servers?

Query distribution over DNS servers

For DNS traffic captured on 1-14 May 2019



Where to put another DNS servers?



Where to put another DNS servers?

- Geography & peering matters
- RTT: excellent in Czech Republic and very good in Europe (most of the traffic), but poor in some remote areas
- New servers required:
 - Eastern, South-Eastern Asia
 - Australia & New Zealand
- Some tweaking required:
 - Northern, South America



New ODVR

- open DNSSEC validating resolvers (<https://www.nic.cz/odvr/>)
- 2 anycast nodes (KNOT resolver 4.0)
- separated from .CZ DNS anycast
- new IP addresses
 - 193.17.47.1, 2001:148f:ffff:1
 - 185.43.135.1, 2001:148f:fffe:1

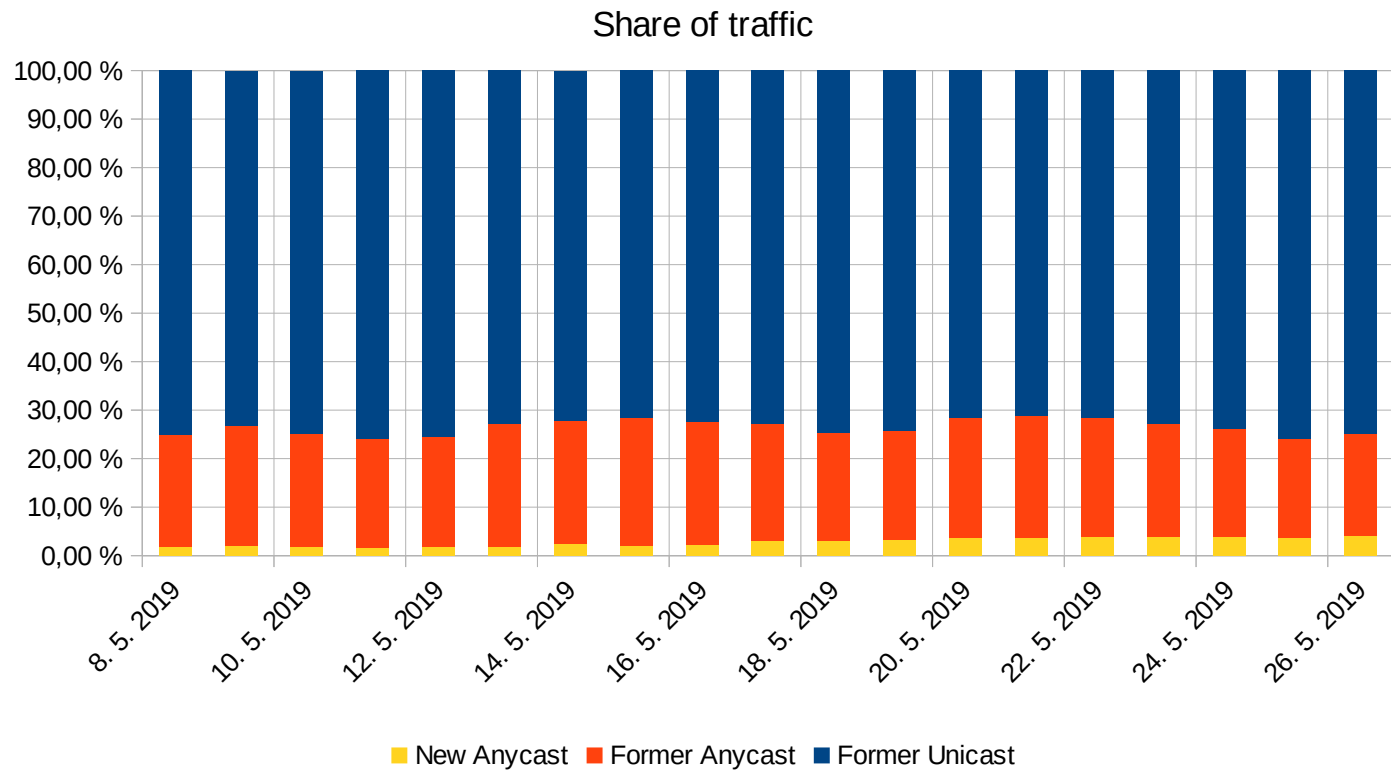


New ODVR

- former ODVR
 - **193.29.206.206 / 2001:678:1::206** & 217.31.204.130 / 2001:1488:800:400::130
 - to be switched off (~1% of the total ODVR traffic)
 - active communication:
 - <https://blog.nic.cz/2019/04/30/spoustime-nove-odvr/>
 - <https://blog.nic.cz/2019/05/20/na-odvr-podporujeme-take-dns-over-https/>
 - tech@nix.cz announcement
 - new ODVR in further TurrisOS
 - contacting significant ISPs



New ODVR



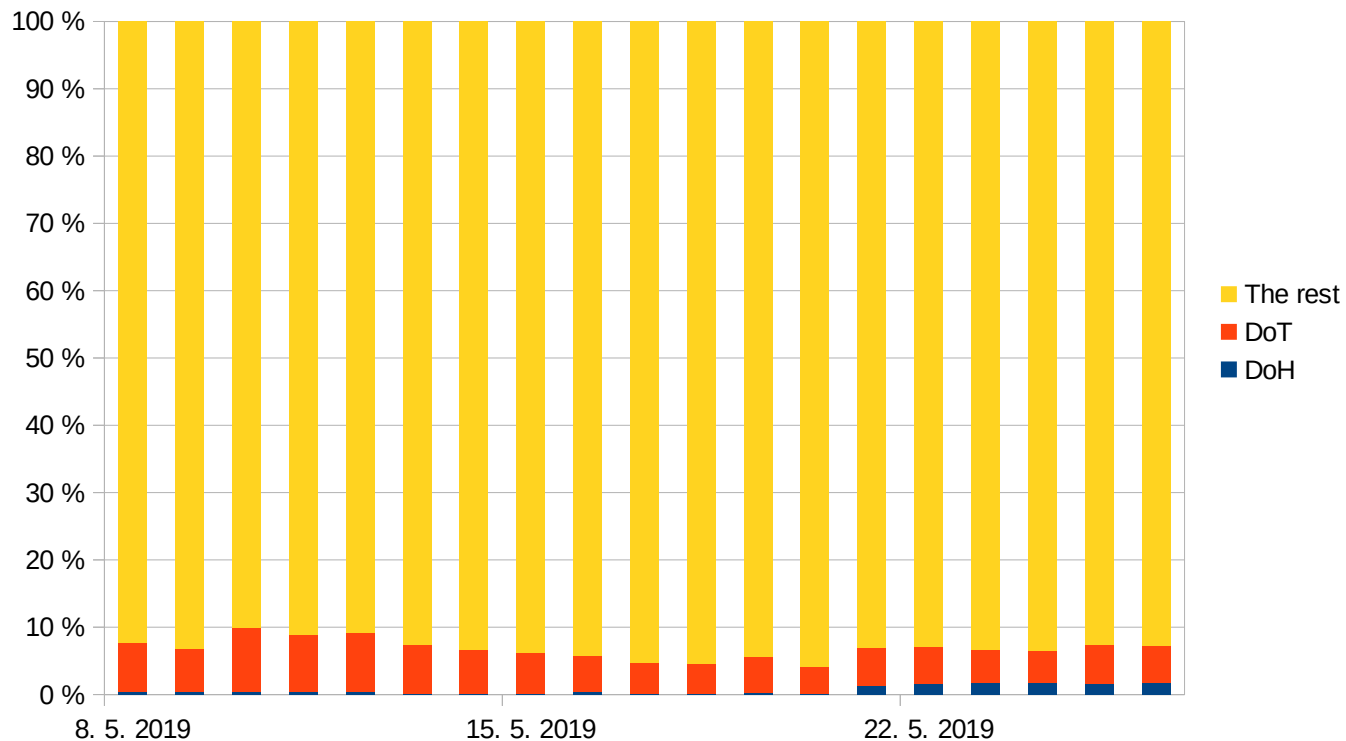
New ODVR

- support for encrypted DNS
 - **DNS over TLS (DoT)**
 - odvr.nic.cz (standard port TCP/853)
 - from 30.4.2019
 - **DNS over HTTPS (DoH)**
 - <https://odvr.nic.cz/doh>
 - supported by Firefox 62+, Chrome 66+
 - from 21.5.2019



New ODVR

Types of traffic at new ODVR

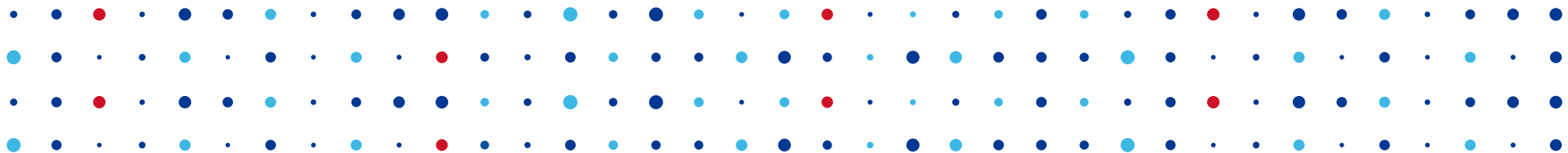


Strengthening of the team

- <https://prace.nic.cz>
 - network & DNS specialist

2001:1488:ffff::456





Thanks for your attention

Zdeněk Brůna • zdenek.bruna@nic.cz

