Passive analysis of DNS server reachability

IT19 conference

Maciej Andziński • maciej.andzinski@nic.cz • 14.11.2019

CZ.NIC | CZ DOMAIN REGISTRY

.CZ DNS servers

- 4 NS, anycast cloud

```
cz.                 3600 IN   NS   a.ns.nic.cz.
cz.                 3600 IN   NS   b.ns.nic.cz.
cz.                 3600 IN   NS   c.ns.nic.cz.
cz.                 3600 IN   NS   d.ns.nic.cz.

a.ns.nic.cz.        3600 IN   A    194.0.12.1
a.ns.nic.cz.        3600 IN   AAAA 2001:678:f::1
b.ns.nic.cz.        3600 IN   A    194.0.13.1
b.ns.nic.cz.        3600 IN   AAAA 2001:678:10::1
d.ns.nic.cz.        3600 IN   A    193.29.206.1
d.ns.nic.cz.        3600 IN   AAAA 2001:678:1::1
```

Location of .CZ DNS servers

- **Asia**
  - [JP] Tokyo
- **Europe**
  - [AT] Vienna
  - [CZ] Undisclosed location, 2x Prague
  - [DE] Frankfurt
  - [IT] Milan
  - [SE] Stockholm
  - [UK] London
- **North America**
  - [US] California, Virginia
- **South America**
  - [BR] Sao Paulo
  - [CL] Santiago de Chile

13 locations

10 countries

4 continents

Motivation

- Help to answer the question:

  What is the best location for our DNS servers?

Motivation

- Help to answer the question:

  What is the best location for our DNS servers?

  - Who sends queries to our servers and

    how log does it take for a query to reach our server?

Motivation

- Help to answer the question:

  What is the best location for our DNS servers?

  this is easy

  - Who sends queries to our servers and
    how log does it take for a query to reach our server?

  this is challenging

Challenge

- How to measure the latency between a DNS client and a DNS server?
  - A typical solution: active measurements
    - PING from DNS server to DNS client
    - PING to DNS server from a probe (e.g. RIPE Atlas)

Our concept: passive analysis

- We capture DNS traffic that hits .CZ DNS servers
- There was **17,464,111,432** in the first two weeks of October 2019
  - UDP **17,418,571,042** queries **(99.74%)**
  - TCP: **45,540,390** queries **(0.26%)**

CZ DOMAIN REGISTRY

Our concept: passive analysis

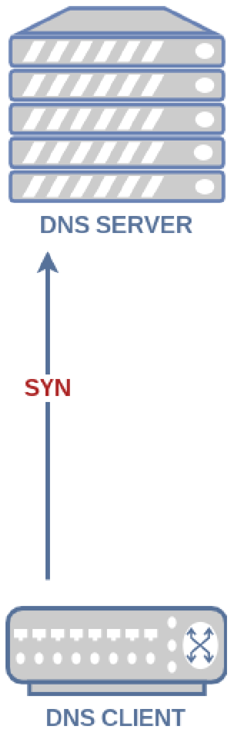
- We capture DNS traffic that hits .CZ DNS servers
- There was **17,464,111,432** in the first two weeks of October 2019
  - UDP **17,418,571,042** queries **(99.74%)**
  - TCP: **45,540,390** queries **(0.26%)**

~ 38 TCP connections per second

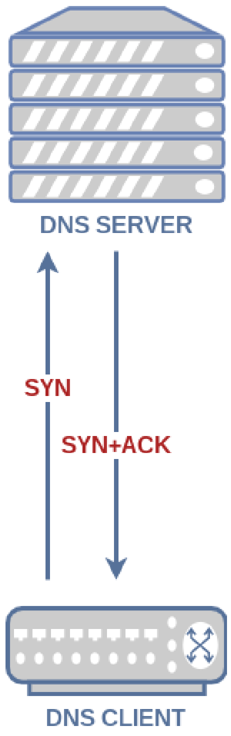
- Let‘s use TCP data to evaluate the latency between a DNS client and a DNS server!

TCP handshake

TCP handshake

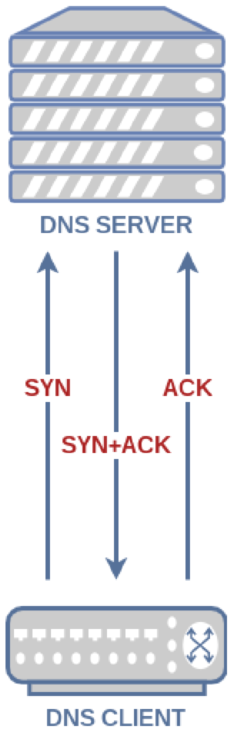


TCP handshake

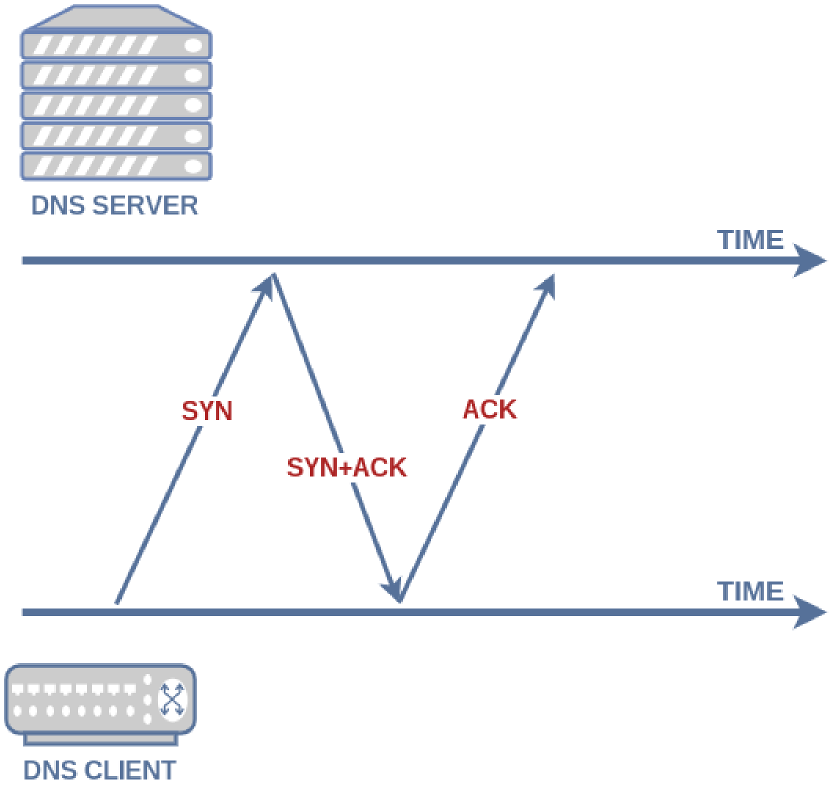


CZ DOMAIN REGISTRY

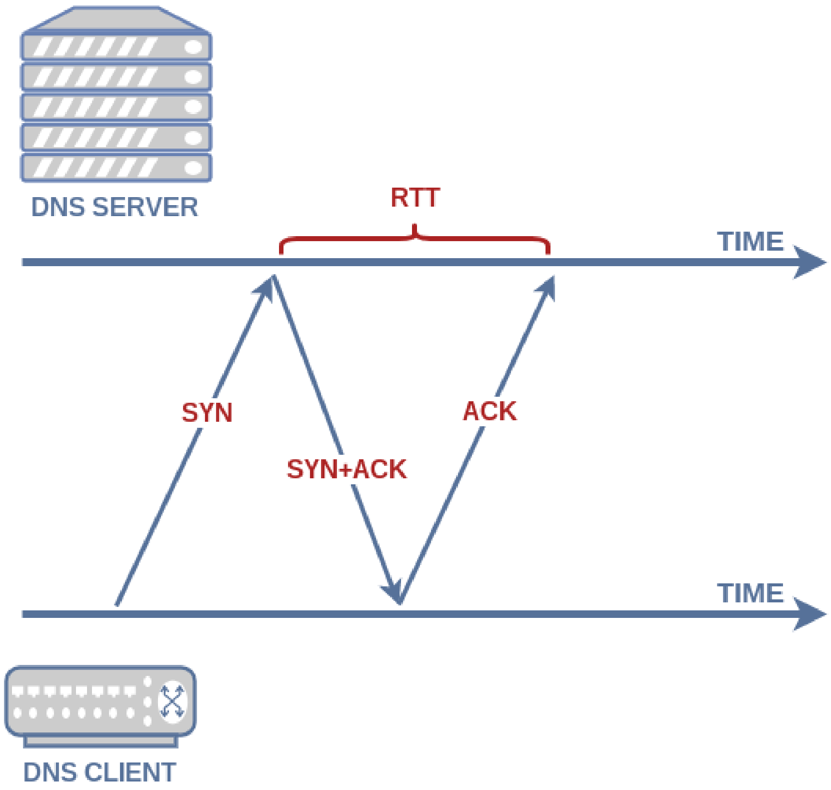
TCP handshake



RTT of a TCP handshake



RTT of a TCP handshake



Our concept

1) 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

Our concept

2)Evaluate RTT for each client, network, country, …

(**Evaluated RTT** = *weighted mean* of RTT for all servers)

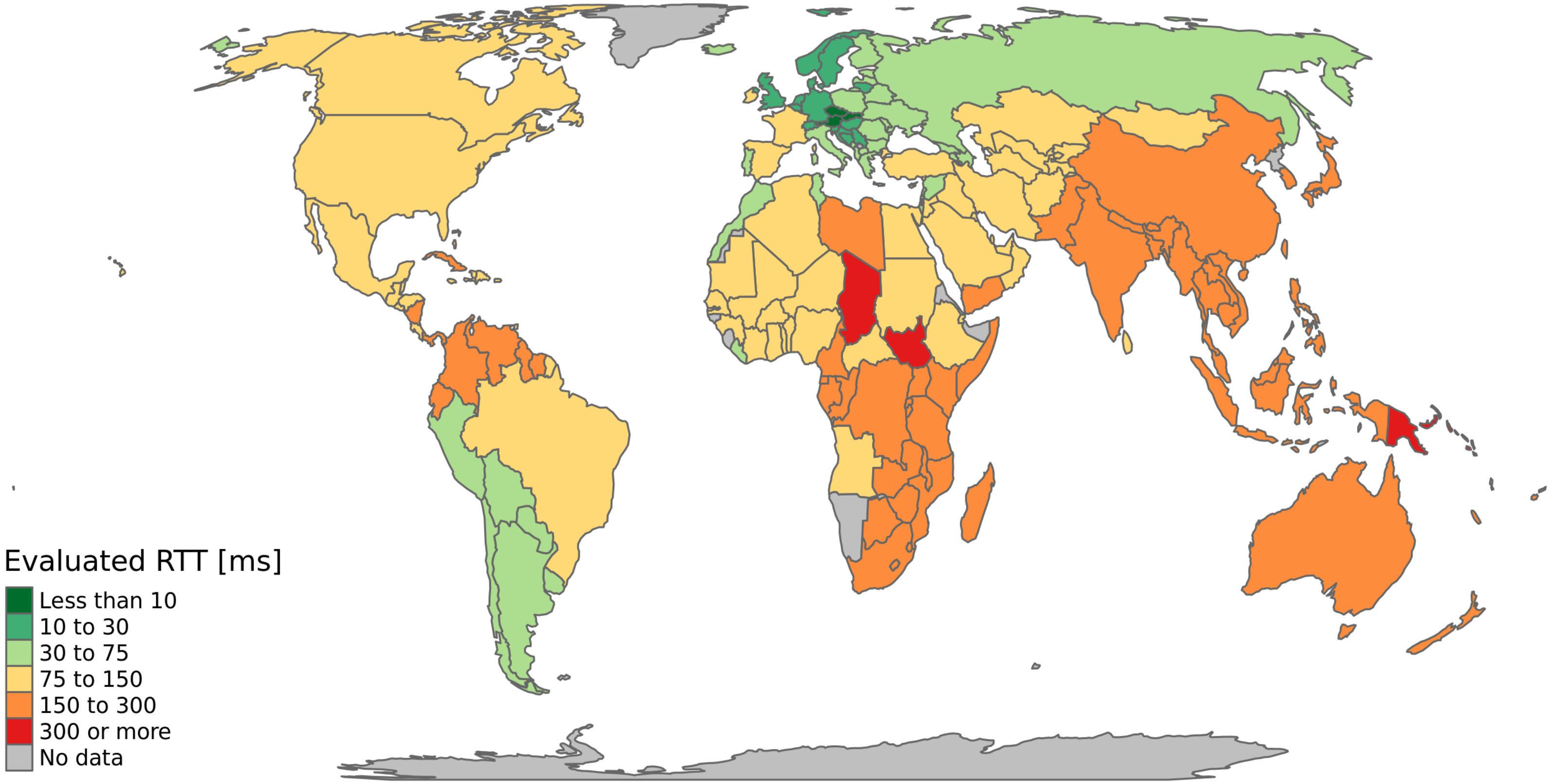
client_ip	client_cc	client_asn	server	queries	**median_rtt**	**weight**
217.31.193.164	CZ	25192	[Europe] AT, Vienna	37123	**NA**	**0.000858**
217.31.193.164	CZ	25192	[Europe] CZ, Undisclosed	5171434	**12.7 ms**	**0.120**
217.31.193.164	CZ	25192	[Europe] CZ, Praha – CECOLO	2579707	**11.9 ms**	**0.0596**
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**

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

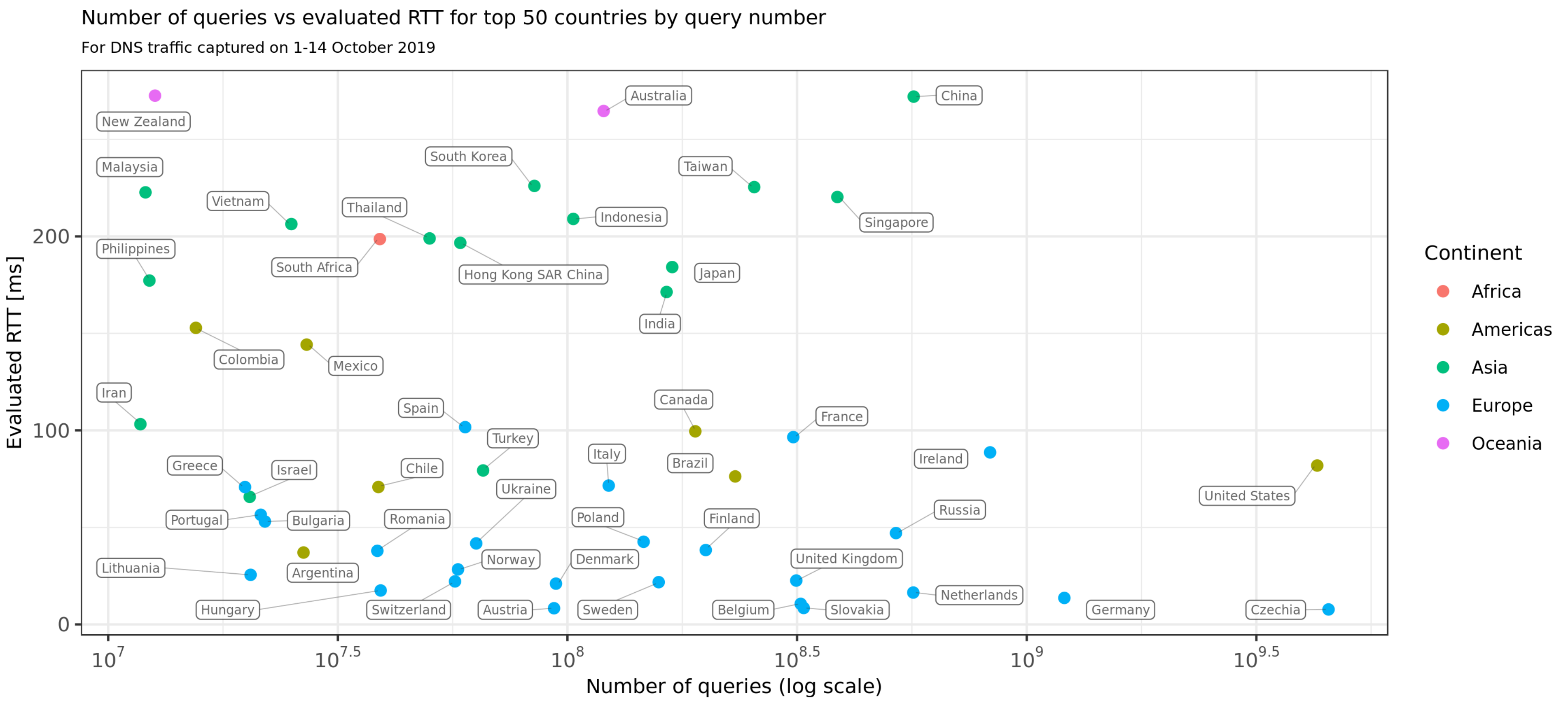
Evaluated RTT for 217.31.193.164 = **17.9 ms**

CZ.NIC CZ DOMAIN REGISTRY

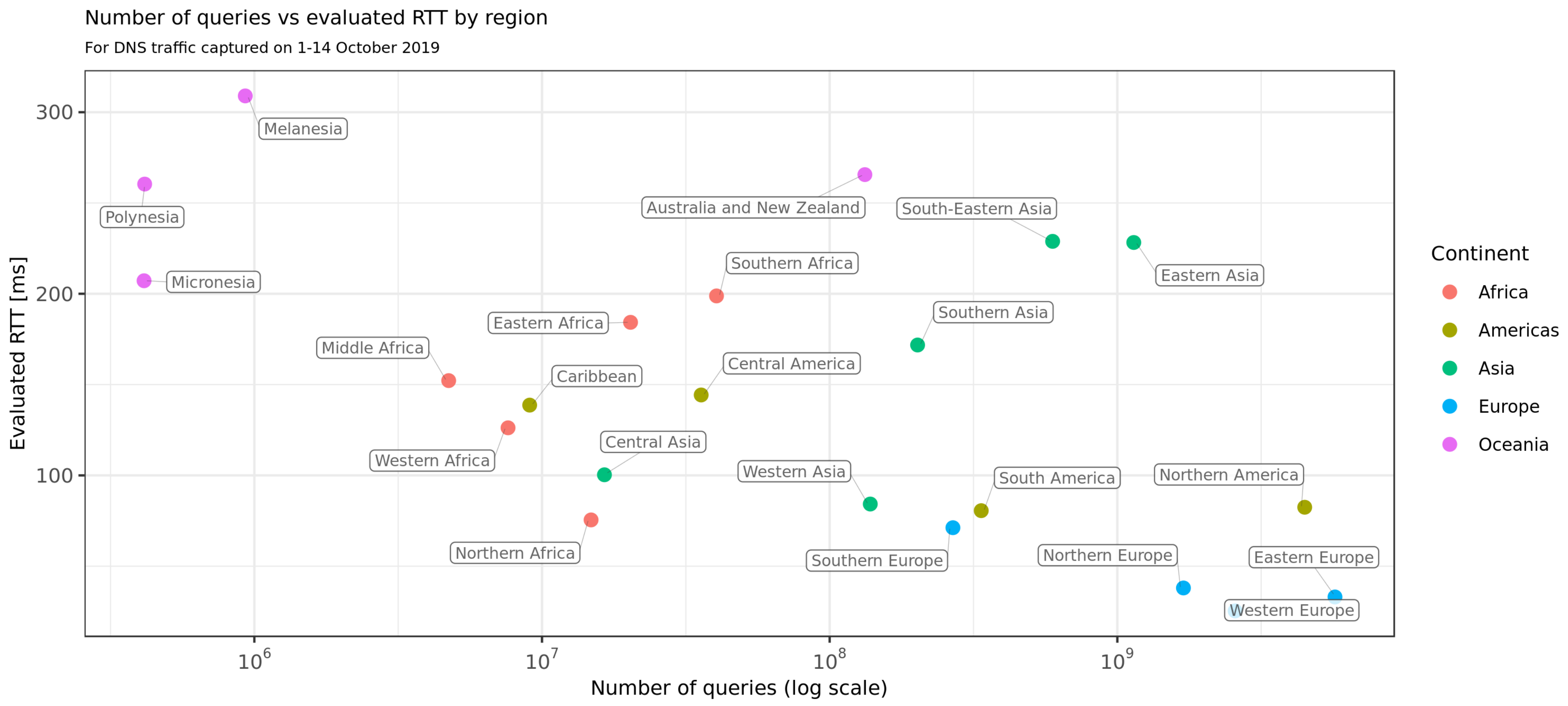
Results


Evaluated RTT [ms]
Less than 10
10 to 30
30 to 75
75 to 150
150 to 300
300 or more
No data

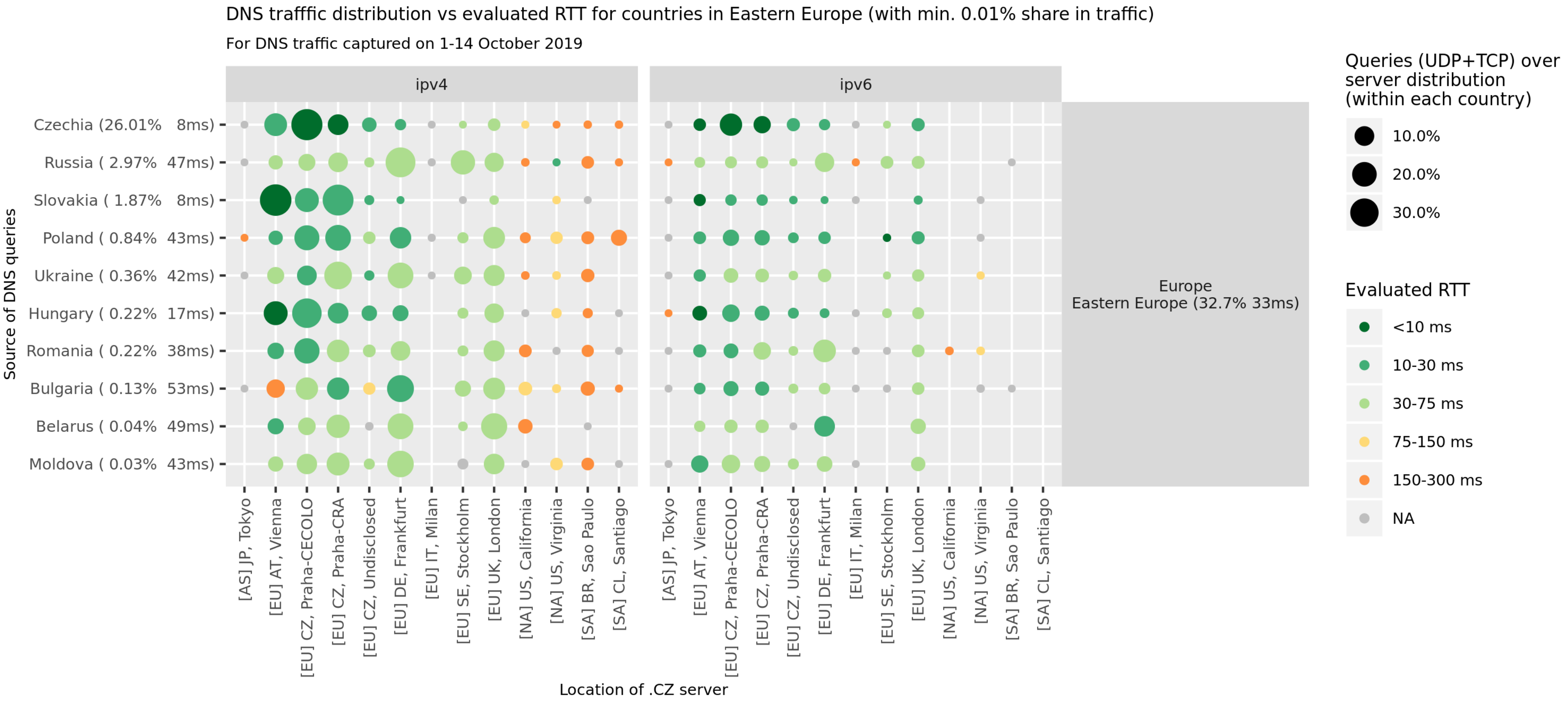
Results


Number of queries vs evaluated RTT for top 50 countries by query number
For DNS traffic captured on 1-14 October 2019
Evaluated RTT [ms]
Number of queries (log scale)
0
100
200
10^7
$10^{7.5}$
10^8
$10^{8.5}$
10^9
$10^{9.5}$
Continent
Africa
Americas
Asia
Europe
Oceania
New Zealand
Australia
China
Malaysia
South Korea
Taiwan
Vietnam
Thailand
Indonesia
Singapore
Philippines
South Africa
Hong Kong SAR China
Japan
India
Colombia
Mexico
Iran
Spain
Canada
France
Turkey
Italy
Brazil
Ireland
Greece
Israel
Chile
Ukraine
United States
Portugal
Bulgaria
Romania
Poland
Finland
Russia
Lithuania
Argentina
Norway
Denmark
United Kingdom
Netherlands
Hungary
Switzerland
Austria
Sweden
Belgium
Slovakia
Germany
Czechia

Results

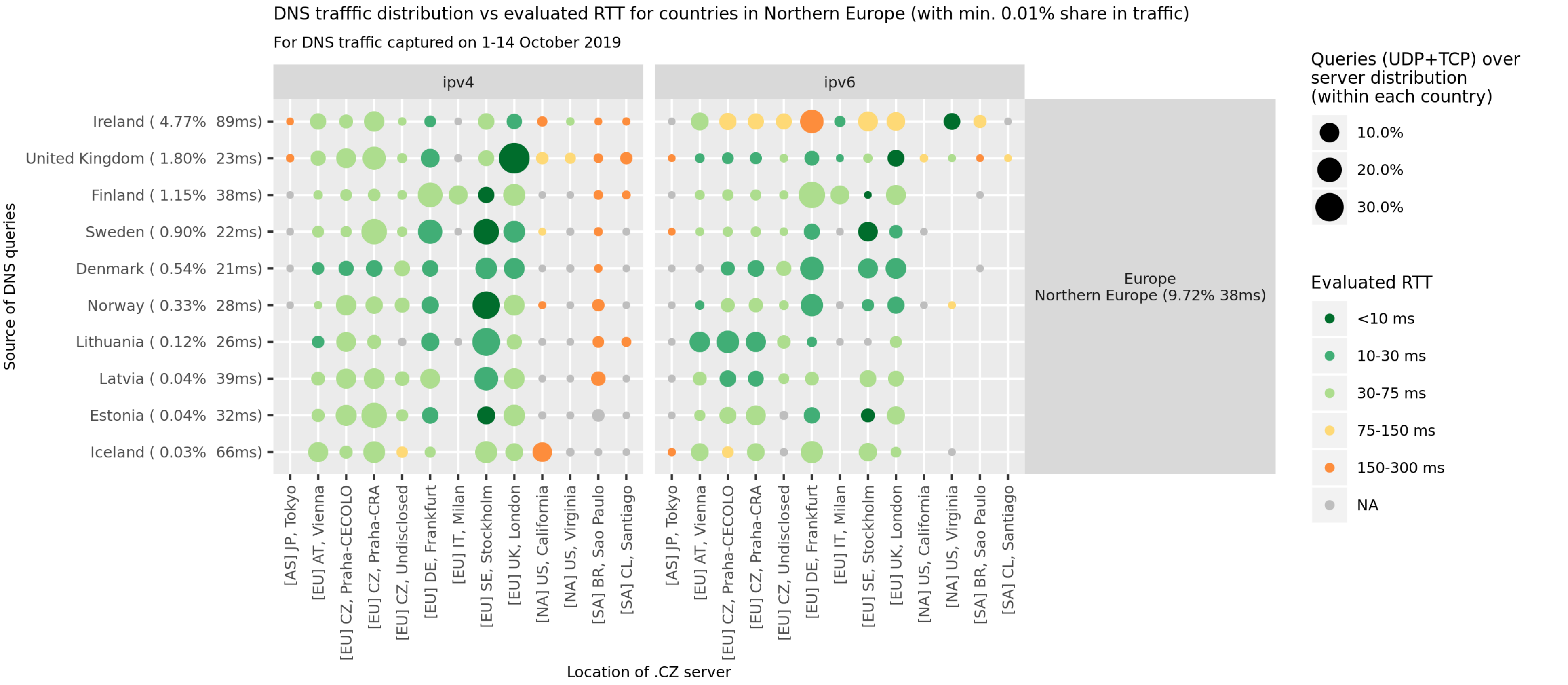

Number of queries vs evaluated RTT by region
For DNS traffic captured on 1-14 October 2019
Evaluated RTT [ms]
300
200
100
Number of queries (log scale)
10^6
10^7
10^8
10^9
Melanesia
Polynesia
Micronesia
Australia and New Zealand
South-Eastern Asia
Eastern Asia
Southern Africa
Eastern Africa
Southern Asia
Middle Africa
Caribbean
Central America
Western Africa
Central Asia
Western Asia
South America
Northern America
Northern Africa
Southern Europe
Northern Europe
Eastern Europe
Western Europe
Continent
Africa
Americas
Asia
Europe
Oceania

Results



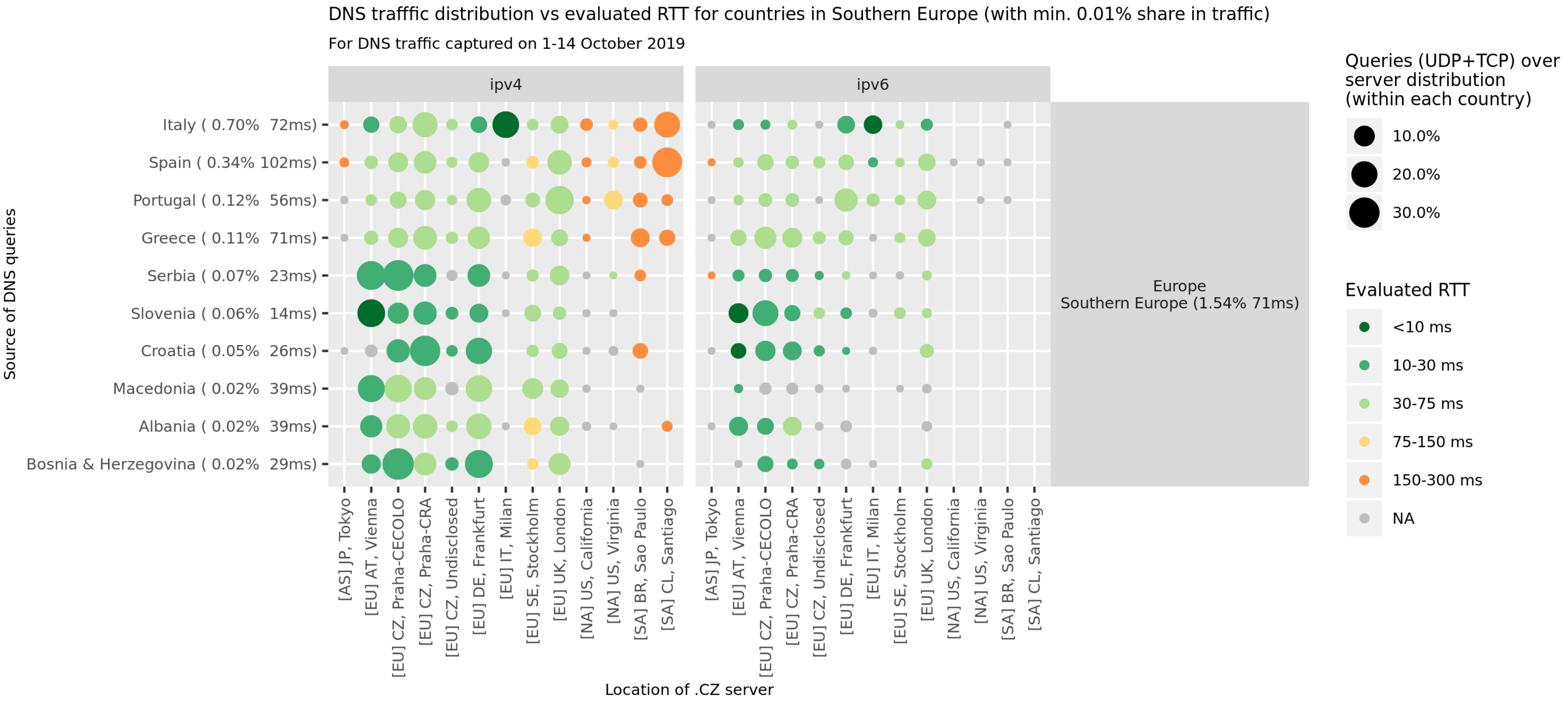
CZ DOMAIN REGISTRY

Results



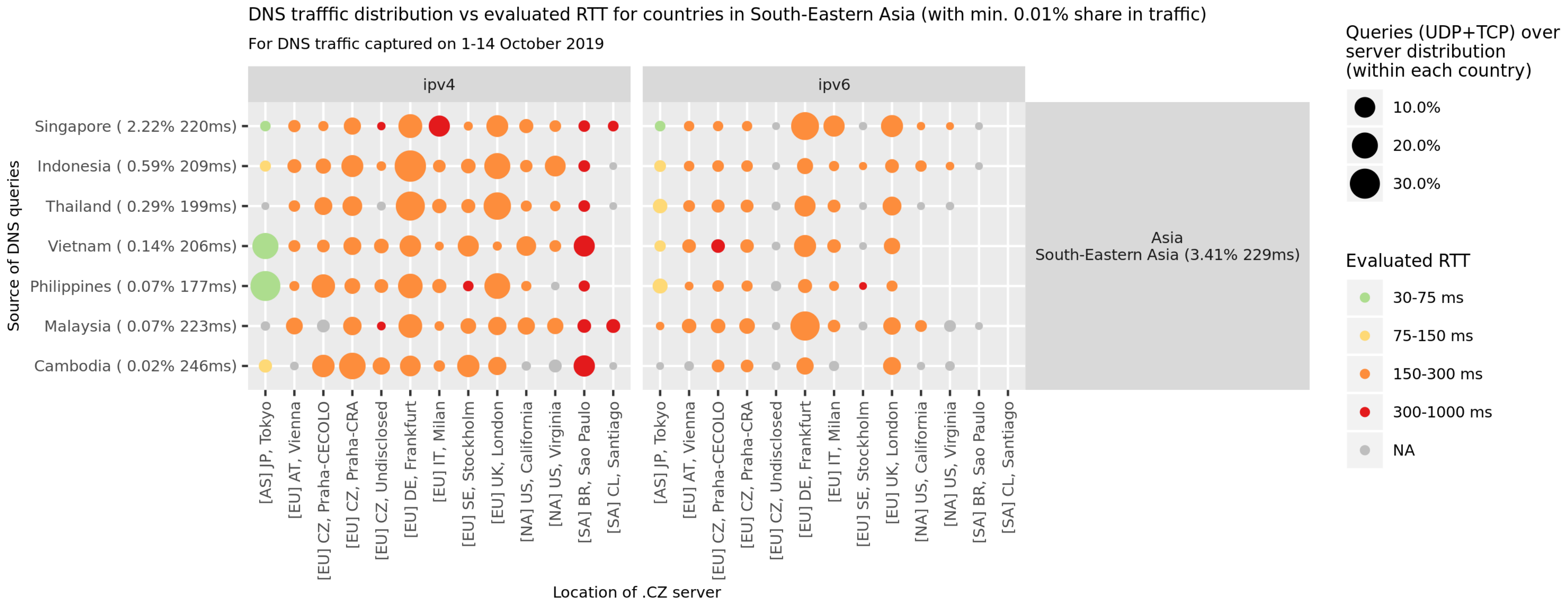
CZ.NIC CZ DOMAIN REGISTRY

Results

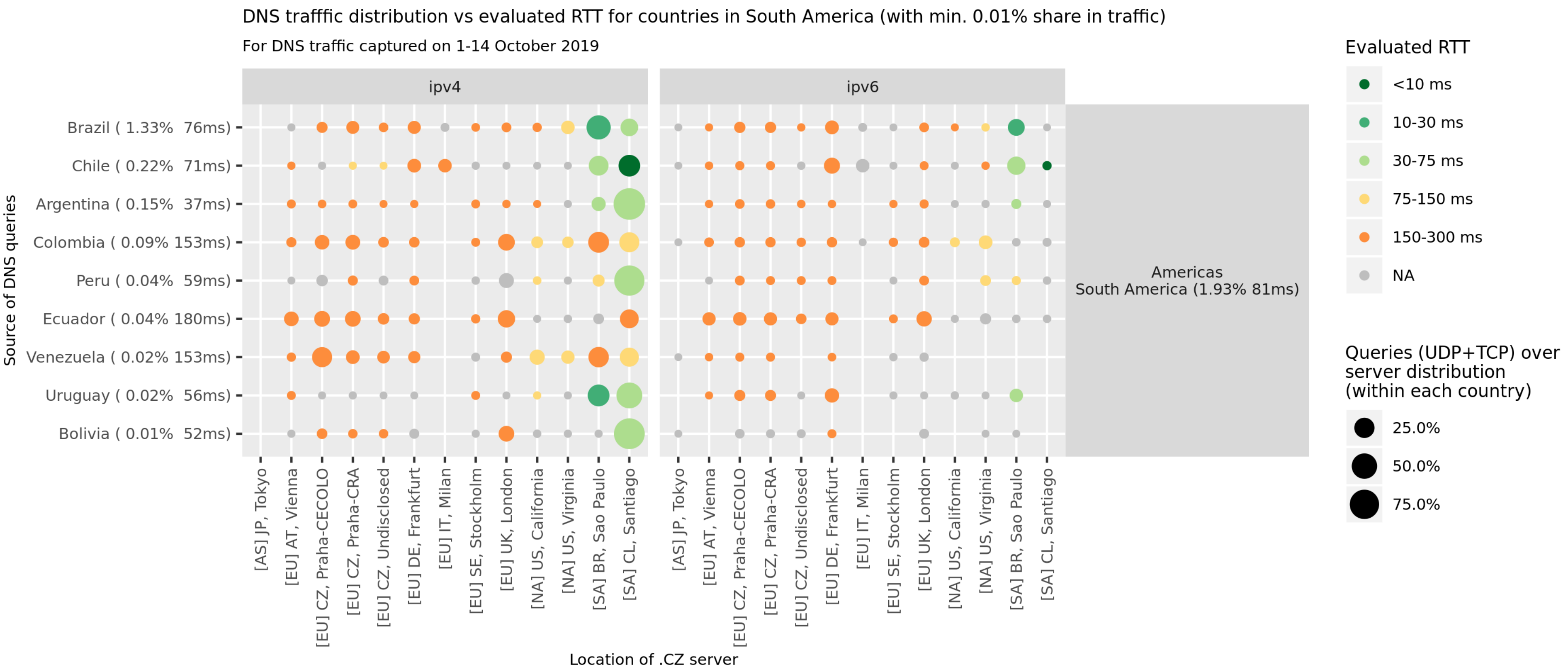


CZ DOMAIN REGISTRY

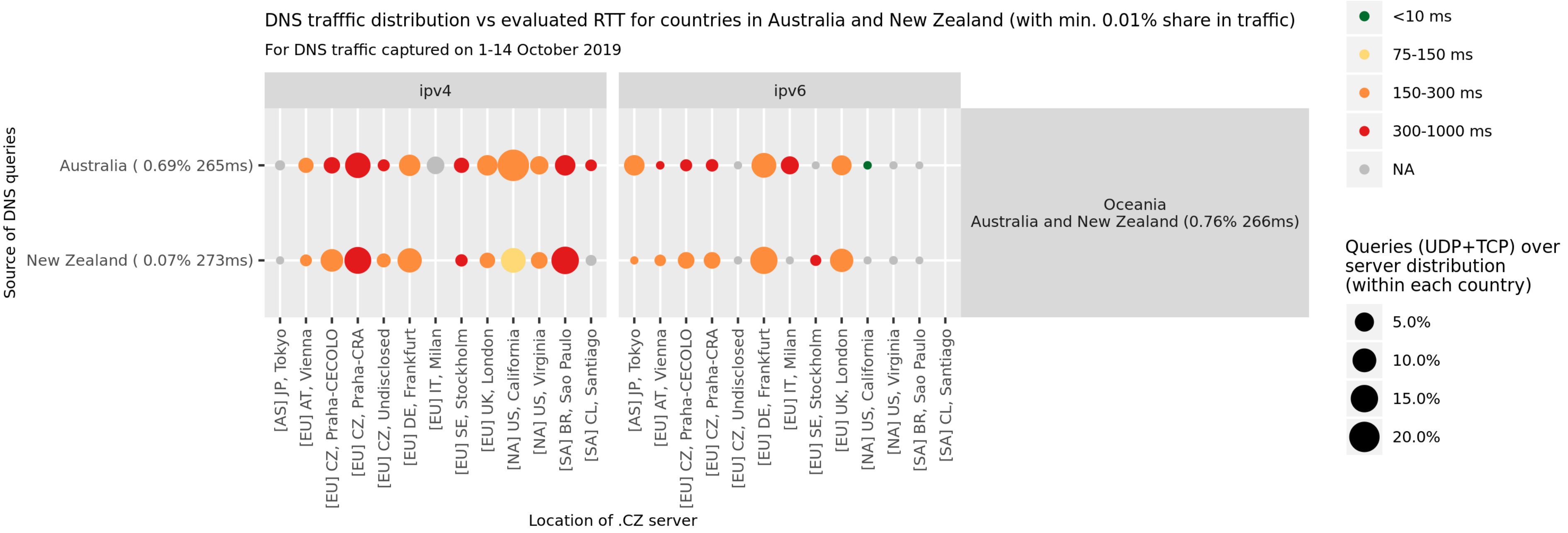
Results


DNS trafffic distribution vs evaluated RTT for countries in South-Eastern Asia (with min. 0.01% share in traffic)
For DNS traffic captured on 1-14 October 2019
ipv4
ipv6
Singapore (2.22% 220ms)
Indonesia (0.59% 209ms)
Thailand (0.29% 199ms)
Vietnam (0.14% 206ms)
Philippines (0.07% 177ms)
Malaysia (0.07% 223ms)
Cambodia (0.02% 246ms)
Source of DNS queries
Asia
South-Eastern Asia (3.41% 229ms)
[AS] JP, Tokyo
[EU] AT, Vienna
[EU] CZ, Praha-CECOLO
[EU] CZ, Praha-CRA
[EU] CZ, Undisclosed
[EU] DE, Frankfurt
[EU] IT, Milan
[EU] SE, Stockholm
[EU] UK, London
[NA] US, California
[NA] US, Virginia
[SA] BR, Sao Paulo
[SA] CL, Santiago
Location of .CZ server
Queries (UDP+TCP) over server distribution (within each country)
10.0%
20.0%
30.0%
Evaluated RTT
30-75 ms
75-150 ms
150-300 ms
300-1000 ms
NA

Results

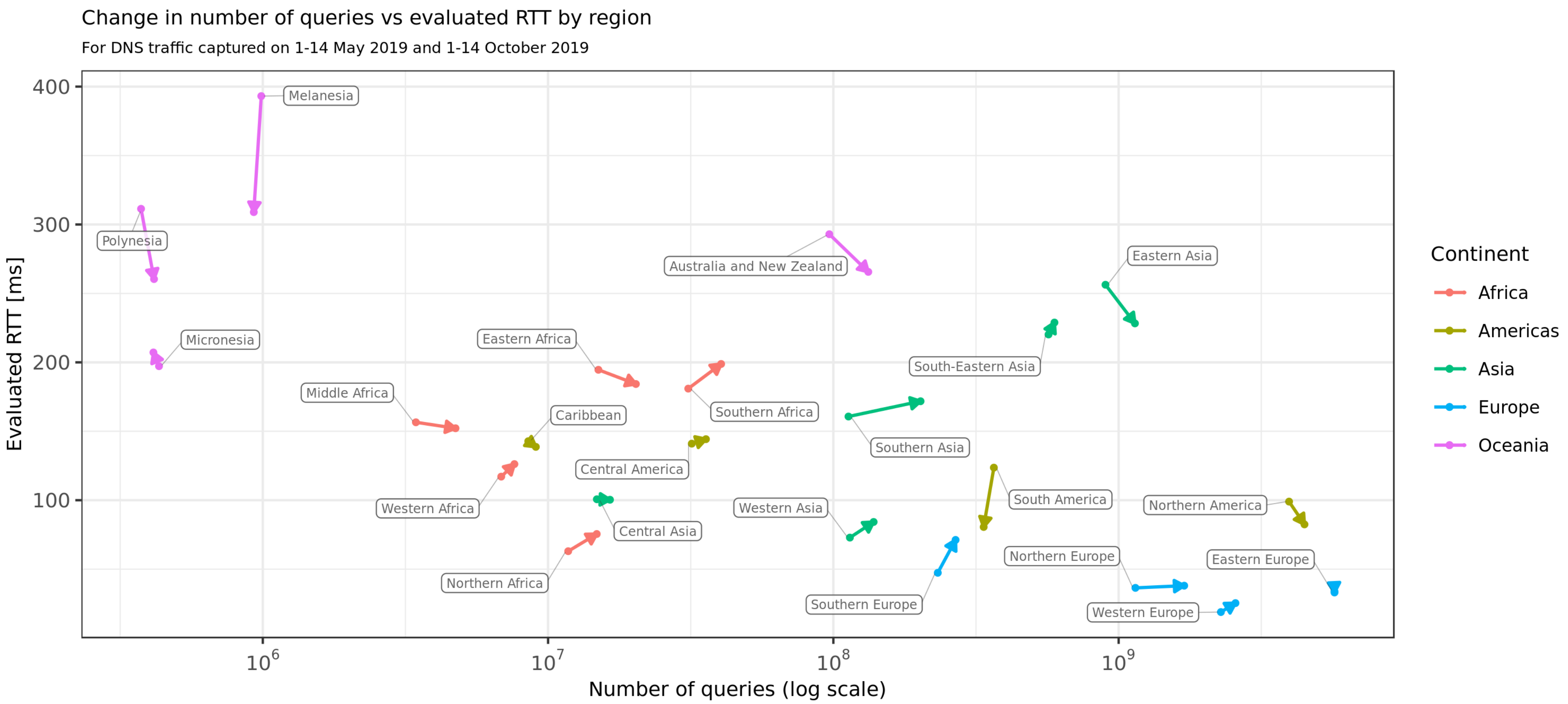

DNS trafffic distribution vs evaluated RTT for countries in South America (with min. 0.01% share in traffic)
For DNS traffic captured on 1-14 October 2019
ipv4
ipv6
Brazil (1.33% 76ms)
Chile (0.22% 71ms)
Argentina (0.15% 37ms)
Colombia (0.09% 153ms)
Peru (0.04% 59ms)
Ecuador (0.04% 180ms)
Venezuela (0.02% 153ms)
Uruguay (0.02% 56ms)
Bolivia (0.01% 52ms)
Source of DNS queries
[AS] JP, Tokyo
[EU] AT, Vienna
[EU] CZ, Praha-CECOLO
[EU] CZ, Praha-CRA
[EU] CZ, Undisclosed
[EU] DE, Frankfurt
[EU] IT, Milan
[EU] SE, Stockholm
[EU] UK, London
[NA] US, California
[NA] US, Virginia
[SA] BR, Sao Paulo
[SA] CL, Santiago
Location of .CZ server
Americas
South America (1.93% 81ms)
Evaluated RTT
<10 ms
10-30 ms
30-75 ms
75-150 ms
150-300 ms
NA
Queries (UDP+TCP) over server distribution (within each country)
25.0%
50.0%
75.0%

Results



CZ DOMAIN REGISTRY

Results – May 2019 vs October 2019



CZ.NIC | CZ DOMAIN REGISTRY

Conclusion (on results)

- Geography matters
- Peering matters
- More than 1 server in a region needed to provide good RTT
  - Fewer NS → better?
- RTT: excellent in Czech Republic and very good in Europe (most of the traffic), but poor in some remote areas
  - A server down under may be a good idea

Conclusion (on method)

(-) Drawbacks

- Much traffic needed
- Sometimes difficult to measure RTT of TCP handshake (retransmissions, broken handshakes, lost packets)

(+) Advantages

- Delivers RTT for actual origin of a DNS query
- Relatively easy to deploy

(?) Other remarks

- Considerations on TCP occurence in DNS
- GeoIP accuracy / updates

Thank You

Maciej Andziński • maciej.andzinski@nic.cz

CZ DOMAIN REGISTRY