Passive analysis of DNS server reachability
14th CENTR R&D workshop

Maciej Andziński • maciej.andzinski@nic.cz • 29.05.2019
### .CZ DNS servers

- 4 NS, all anycasted

<table>
<thead>
<tr>
<th>Domain</th>
<th>TTL</th>
<th>Record Type</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>cz.</td>
<td>3600</td>
<td>NS</td>
<td>a.ns.nic.cz.</td>
</tr>
<tr>
<td>cz.</td>
<td>3600</td>
<td>NS</td>
<td>b.ns.nic.cz.</td>
</tr>
<tr>
<td>cz.</td>
<td>3600</td>
<td>NS</td>
<td>c.ns.nic.cz.</td>
</tr>
<tr>
<td>cz.</td>
<td>3600</td>
<td>NS</td>
<td>d.ns.nic.cz.</td>
</tr>
<tr>
<td>a.ns.nic.cz.</td>
<td>3600</td>
<td>A</td>
<td>194.0.12.1</td>
</tr>
<tr>
<td>a.ns.nic.cz.</td>
<td>3600</td>
<td>AAAA</td>
<td>2001:678:f::1</td>
</tr>
<tr>
<td>b.ns.nic.cz.</td>
<td>3600</td>
<td>A</td>
<td>194.0.13.1</td>
</tr>
<tr>
<td>b.ns.nic.cz.</td>
<td>3600</td>
<td>AAAA</td>
<td>2001:678:10::1</td>
</tr>
<tr>
<td>d.ns.nic.cz.</td>
<td>3600</td>
<td>A</td>
<td>193.29.206.1</td>
</tr>
<tr>
<td>d.ns.nic.cz.</td>
<td>3600</td>
<td>AAAA</td>
<td>2001:678:1::1</td>
</tr>
</tbody>
</table>
Location of .CZ DNS servers

- **Asia**
  - [JP] Tokyo

- **Europe**
  - [AT] Vienna
  - [CZ] Undisclosed location, 2x Prague
  - [DE] Frankfurt
  - [SE] Stockholm
  - [UK] London

- **North America**
  - [US] California, Virginia

- **South America**
  - [BR] Sao Paulo
  - [CL] Santiago de Chile

**12 locations**

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

this is easy

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 15,659,160,884 in the first two weeks of May 2019
  - UDP 15,638,098,643 queries (99.87%)
  - TCP: 21,062,241 queries (0.13%)
Our concept: passive analysis

- We capture DNS traffic that hits .CZ DNS servers
- There was \textbf{15,659,160,884} in the first two weeks of May 2019
  - UDP \textbf{15,638,098,643} queries (99.87%)  
  - TCP: \textbf{21,062,241} queries (0.13%)  
    ~ 17 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
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

<table>
<thead>
<tr>
<th>client_ip</th>
<th>client_cc</th>
<th>client_asn</th>
<th>server</th>
<th>queries</th>
<th>tcp</th>
<th>median_rtt</th>
</tr>
</thead>
<tbody>
<tr>
<td>217.31.193.164</td>
<td>CZ</td>
<td>25192</td>
<td>[Europe] AT, Vienna</td>
<td>37123</td>
<td>0</td>
<td>NA</td>
</tr>
<tr>
<td>217.31.193.164</td>
<td>CZ</td>
<td>25192</td>
<td>[Europe] CZ, Undisclosed</td>
<td>5171434</td>
<td>57</td>
<td>12.7 ms</td>
</tr>
<tr>
<td>217.31.193.164</td>
<td>CZ</td>
<td>25192</td>
<td>[Europe] CZ, Praha – CECOLO</td>
<td>2579707</td>
<td>6</td>
<td>11.9 ms</td>
</tr>
<tr>
<td>217.31.193.164</td>
<td>CZ</td>
<td>25192</td>
<td>[Europe] CZ, Praha – CRA</td>
<td>27065563</td>
<td>220</td>
<td>11.5 ms</td>
</tr>
<tr>
<td>217.31.193.164</td>
<td>CZ</td>
<td>25192</td>
<td>[Europe] UK, London</td>
<td>8416765</td>
<td>88</td>
<td>43.4 ms</td>
</tr>
</tbody>
</table>

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)

<table>
<thead>
<tr>
<th>client_ip</th>
<th>client_cc</th>
<th>client_asn</th>
<th>server</th>
<th>queries</th>
<th>median_rtt</th>
<th>weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>217.31.193.164</td>
<td>CZ</td>
<td>25192</td>
<td>[Europe] AT, Vienna</td>
<td>37123</td>
<td>NA</td>
<td>0.000858</td>
</tr>
<tr>
<td>217.31.193.164</td>
<td>CZ</td>
<td>25192</td>
<td>[Europe] CZ, Undisclosed</td>
<td>5171434</td>
<td>12.7 ms</td>
<td>0.120</td>
</tr>
<tr>
<td>217.31.193.164</td>
<td>CZ</td>
<td>25192</td>
<td>[Europe] CZ, Praha – CECOLO</td>
<td>2579707</td>
<td>11.9 ms</td>
<td>0.0596</td>
</tr>
<tr>
<td>217.31.193.164</td>
<td>CZ</td>
<td>25192</td>
<td>[Europe] CZ, Praha – CRA</td>
<td>27065563</td>
<td>11.5 ms</td>
<td>0.625</td>
</tr>
<tr>
<td>217.31.193.164</td>
<td>CZ</td>
<td>25192</td>
<td>[Europe] UK, London</td>
<td>8416765</td>
<td>43.4 ms</td>
<td>0.195</td>
</tr>
</tbody>
</table>

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

Evaluated RTT for 217.31.193.164 = 17.9 ms
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
Results

Number of queries vs evaluated RTT for top 50 countries by query number
For DNS traffic captured on 1-14 May 2019
Results

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

<table>
<thead>
<tr>
<th>Source of DNS queries</th>
<th>ipv4</th>
<th>ipv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Czechia (29.44%)</td>
<td>8ms</td>
<td></td>
</tr>
<tr>
<td>Russia (3.15%)</td>
<td></td>
<td>44ms</td>
</tr>
<tr>
<td>Slovakia (2.06%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Poland (0.81%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ukraine (0.33%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Romania (0.22%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hungary (0.22%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bulgaria (0.13%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Belarus (0.07%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Moldova (0.03%)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Queries (UDP+TCP) over server distribution (within each country)

- 10.0%
- 20.0%
- 30.0%
- 40.0%

Evaluated RTT

- <10 ms
- 10-30 ms
- 30-75 ms
- 75-150 ms
- 150-300 ms
- >300 ms

Location of .CZ server

CZ Domain Registry

CZ.nic

CZ Domain Registry
Results

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

Location of .CZ server

Queries (UDP+TCP) over server distribution (within each country)
- 10.0%
- 20.0%
- 30.0%
- 40.0%

Evaluating RTT
- <10 ms
- 10-30 ms
- 30-75 ms
- 75-150 ms
- 150-300 ms
- 300-1000 ms
- NA
Results

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

Queries (UDP+TCP) over server distribution (within each country)

- 10.0%
- 20.0%
- 30.0%
- 40.0%

Evaluated RTT

- <10 ms
- 10-30 ms
- 30-75 ms
- 75-150 ms
- 150-300 ms
- NA

Location of .CZ server

Source of DNS queries

- Italy (0.65%) 49ms
- Spain (0.30%) 55ms
- Portugal (0.14%) 59ms
- Greece (0.11%) 63ms
- Croatia (0.08%) 16ms
- Serbia (0.06%) 20ms
- Slovenia (0.06%) 16ms
- Macedonia (0.04%) 38ms
- Bosnia & Herzegovina (0.02%) 32ms
- Albania (0.01%) 40ms

Europe Southern Europe (1.48% 47ms)
Results

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

Source of DNS queries:
- Singapore (2.50% 212ms)
- Indonesia (0.51% 170ms)
- Thailand (0.22% 204ms)
- Vietnam (0.21% 192ms)
- Malaysia (0.07% 181ms)
- Philippines (0.07% 168ms)
- Cambodia (0.02% 218ms)
- Brunei (0.01% 224ms)
- Myanmar (0.01% 243ms)

Queries (UDP+TCP) over server distribution (within each country):
- 10.0%
- 20.0%
- 30.0%
- 40.0%

Evaluated RTT:
- 30-75 ms
- 75-150 ms
- 150-300 ms
- 300-1000 ms

Location of .cz server:

South-Eastern Asia (3.63% 220ms)
Results

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

<table>
<thead>
<tr>
<th>Source of DNS queries</th>
<th>ipv4</th>
<th>ipv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brazil (1.67% 130ms)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chile (0.31% 100ms)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Argentina (0.16% 122ms)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Colombia (0.07% 153ms)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peru (0.04% 126ms)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ecuador (0.03% 188ms)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Uruguay (0.02% 109ms)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Venezuela (0.02% 162ms)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Evaluated RTT:
- <10 ms
- 10-30 ms
- 30-75 ms
- 75-150 ms
- 150-300 ms
- 300-1000 ms
- NA

Location of .CZ server

Queries (UDP+TCP) over server distribution (within each country):
- 20.0%
- 40.0%
- 60.0%
Results

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

Location of .CZ server

Queries (UDP+TCP) over server distribution (within each country)

- 10.0%
- 20.0%
- 30.0%

Evaluated RTT

- 75-150 ms
- 150-300 ms
- 300-1000 ms
- NA
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 occurrence in DNS
- GeoIP accuracy / updates