Everything you ever wanted to know about caching resolvers but were afraid to ask
Participants:
Andrea Barberio, Petros Gigis, Jerry Lundström, Teemu Rytilahti, Willem Toorop

Goal:
Provide insight into caching resolver capabilities
Capabilities & properties

Basic: IPv6, TCP, TCP over IPv6

Security: DNSSEC validation, Algorithm support, TA’s Root KSK Sentinel, NXdomain rewrite

Privacy: Qname minimization, EDNS Client Subnet
Some msms need just a zone
IPv6, DNSSEC validation, NXdomain rewriting

Some need authoritative perspective
TCP, Qname minimization, EDNS Client subnet

dnsthoughtd
```
$ dig @9.9.9.9 tc.ripe-hackathon6.nlnetlabs.nl AAAA
;; DiG 9.11.0-P2 <<>> @9.9.9.9 tc.ripe-hackathon6.nlnetlabs.nl AAAA
;; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<-- opcode: QUERY, status: NOERROR, id: 61711
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
tc.ripe-hackathon6.nlnetlabs.nl. IN AAAA

;; ANSWER SECTION:
tc.ripe-hackathon6.nlnetlabs.nl. 0 IN AAAA 2620:171:f9:f0::8

;; Query time: 15 msec
;; SERVER: 9.9.9.9#53(9.9.9.9)
;; WHEN: Mon Oct 08 15:10:12 CEST 2018
;; MSG SIZE rcvd: 88
```

```
$ dig -x 2620:171:f9:f0::8 +short
res110.ams.rriidsn.pch.net.
$`
The RIPE Atlas perspective

Host Network

Internet

NLnet Labs

Public Resolver
dnsthoughtd

Willem Toorop

DNSThought @OARC29 6/38
## The RIPE Atlas perspective

<table>
<thead>
<tr>
<th>Internal</th>
<th>Forwarding</th>
<th>External</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>X</td>
<td>X</td>
<td>Y</td>
</tr>
<tr>
<td>X</td>
<td>Y</td>
<td>Z</td>
</tr>
</tbody>
</table>

- **Probe ASN**
- **Resolver ASN**
- **Authoritative ASN**

- X = X
- Z = Z
- Y = Y

---

Willem Toorop

**DNSThought** @OARC29 7/38
Qname minimization

```
willzem@makaak:~$ dig @1.1.1.1 qnamemintest.internet.nl TXT
;;<<>> DiG 9.11.0-P2 <<>> @1.1.1.1 qnamemintest.internet.nl TXT
;(1 server found)
;; global options: +cmd
;; Got answer:
;; >>>HEADER<<- opcode: QUERY, status: NOERROR, id: 33167
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1452
;; QUESTION SECTION:
;qnamemintest.internet.nl. IN TXT

;; ANSWER SECTION:
qnamemintest.internet.nl. 10 IN CNAME a.b.qnamemin-test.internet.nl.
a.b.qnamemin-test.internet.nl. 10 IN TXT "HOORAY - QNAME minimisation is enabled on your resolver :)"

;; Query time: 20 msec
;; SERVER: 1.1.1.1#53(1.1.1.1)
;; WHEN: Mon Oct 08 15:26:41 CEST 2018
;; MSG SIZE rcvd: 157
willzem@makaak:~$
```
Measurements for all probes every hour

<table>
<thead>
<tr>
<th>query</th>
<th>msm ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;prb_id&gt;..&lt;time&gt;.ripe-hackathon6.nlnetlabs.nl AAAA</td>
<td>8310366</td>
</tr>
<tr>
<td>&lt;prb_id&gt;..&lt;time&gt;.tc.ripe-hackathon4.nlnetlabs.nl A</td>
<td>8310360</td>
</tr>
<tr>
<td>&lt;prb_id&gt;..&lt;time&gt;.tc.ripe-hackathon6.nlnetlabs.nl AAAA</td>
<td>8310364</td>
</tr>
<tr>
<td>qnamemintest.internet.nl TXT</td>
<td>8310250</td>
</tr>
<tr>
<td>nxdomain.ripe-hackathon2.nlnetlabs.nl A</td>
<td>8311777</td>
</tr>
<tr>
<td>whoami.akamai.net A</td>
<td>8310245</td>
</tr>
<tr>
<td>o-o.myaddr.l.google.com TXT</td>
<td>8310237</td>
</tr>
<tr>
<td>secure.ripe-hackathon2.nlnetlabs.nl A</td>
<td>8311760</td>
</tr>
<tr>
<td>bogus.ripe-hackathon2.nlnetlabs.nl A</td>
<td>8311763</td>
</tr>
</tbody>
</table>

Thank you Emile Aben! ♥
Per probe | Overview of probe 31568

Overview:
- The probe can connect to a name server
- The probe resolver can perform DNS IPv4 TCP
- The probe resolver can perform DNS IPv6 TCP
- The probe resolver has IPv6 capability
- The probe resolver offers QNAME minimization
- The probe resolver does not deliver edns subnet info

Availability per DNS Resolver

<table>
<thead>
<tr>
<th>Resolver IP</th>
<th>Last Hour</th>
<th>Last 6h</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.87.36.36</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>195.169.124.124</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Capabilities per DNS Resolver

<table>
<thead>
<tr>
<th>resolver IP</th>
<th>resolver net</th>
<th>resolver ASN</th>
<th>edns0 client subnet</th>
<th>IPv6 capability</th>
<th>IPv4 TCP</th>
<th>IPv6 TCP</th>
<th>QNAME minimization</th>
</tr>
</thead>
<tbody>
<tr>
<td>195.169.124.124</td>
<td>195.169.0.0/16</td>
<td>1103</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>192.87.36.36</td>
<td>192.87.0.0/24</td>
<td>1103</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Probe Map of AS v4: 1103 | v6: 1103

View Probe (id: 31568)
Root Canary Project

- Participation with Roland van Rijswijk - Deij
- Measurements started 20 June 2017
More measurements

• Moritz Muller joined too
• Root KSK Sentinel msms since 19 July 2018

query

root-key-sentinel-not-ta-19036.d2a8n3.rootcanary.net A 15283670
root-key-sentinel-not-ta-20326.d2a8n3.rootcanary.net A 15283671

With validating resolvers we have three situations:
1. Key 20326 has not been picked up (yet)
2. Key 20326 is a valid TA, and key 19036 is still a valid TA
3. Key 20326 is a valid TA, and key 19036 is removed
For these situations (1, 2, 3), measurements for:
- (not-ta-19036 is-ta-20326) results in 1: (S S), 2: (S A), 3: (A A)
- (is-ta-19036 is-ta-20326) results in 1: (A S), 2: (A A), 3: (S A)
- (not-ta-19036 not-ta-20326) results in 1: (S A), 2: (S S), 3: (A S)
- (is-ta-19036 not-ta-20326) results in 1: (A A), 2: (A S), 3: (S S)
1½ years of measurements
Internal, Forwarding & External

https://dnsthought.nlnetlabs.nl/#int_fwd_ext

with 19082 resolvers

with 10155 probes

- external (22.4%)
- forwarding (22.7%)
- internal (55.0%)

Willem Toorop
DNSThought @OARC29 13/38
1½ years of measurements
Top 10 ASNs seen @ authoritative

https://dnsthought.nlnetlabs.nl/#top_auth_asns

with 19082 resolvers
have the same ASN as the probe (internal)
https://dnsthought.nlnetlabs.nl/is_internal/#int_fwd_ext

with 10490 resolvers

with 6611 probes

Willem Toorop
DNSThought @OARC29 15/38
Top 10 ASNs seen @ authoritative with 10490 resolvers

- Remaining (80.9%)
- AS3215 (1.8%)
- AS12453 (0.9%)
- AS12322 (3.1%)
- AS31334 (1.0%)
- AS3320 (3.1%)
- AS6830 (3.3%)
- AS6848 (0.8%)
- AS3265 (1.3%)
- AS7922 (3.8%)

https://dnsthought.nlnetlabs.nl/is_internal/#top_auth_asns
Top 10 ASNs seen @ authoritative with 3351 resolvers

- Remaining (24.9%)
- AS42 (6.8%)
- AS13335 (16.3%)
- AS12552 (0.1%)
- AS36692 (5.7%)
- AS15169 (35.3%)
- AS6830 (1.1%)
- AS3356 (1.4%)
- AS3320 (0.2%)
- Remaining

Forwarding

forwarding to a resolver with a different ASN
https://dnsthought.nlnetlabs.nl/is_forwarding/#top_auth_asns

1st April 2018

16 November '17
PCH = Quad9

Willem Toorop
DNSThought @OARC29 17/38
Top 10 ASNs seen @ authoritative with 4266 resolvers

have a ASN different from the probe ASN
https://dnsthought.nlnetlabs.nl/is_external/#top_auth_asns
Internal, Forwarding, External

Diversity
DNSSEC RSA-SHA256 support

With 19135 resolvers

With 10178 probes

https://dnsthought.nlnetlabs.nl/#rsasha256
- 54.1% of probes has validating resolver
- 16.7% of those have a non validating resolver too
- So realistically only 45.1% of probes is protected
validate DNSKEY algorithm RSA-SHA256
https://dnsthought.nlnetlabs.nl/can_rsasha256/#ta_20326

DNSSEC
Root Key Trust Anchor Sentinel

with 9493 resolvers
with 5508 probes
Root Key Trust Anchor Sentinel

DNSSEC

Root KSK sentinel support
https://dnsthought.nlnetlabs.nl/has_ta_19036/#ta_20326

with 902 resolvers

with 709 probes

Willem Toorop
DNSThought @OARC29 23/38
root KSK sentinel support
https://dnsthought.nlnetlabs.nl/has_ta_19036/#top_resolver_asns

Root Key Trust Anchor Sentinel

with 902 resolvers
In 709 probes
validate DNSKEY algorithm RSA-SHA256
https://dnsthought.nlnetlabs.nl/can_rsasha256/#top_auth_asns

DNSSEC
Strange dent in August
with 9493 resolvers
In 5508 probes

Willem Toorop
DNSThought @OARC29 25/38
Strange dent in August

with 897 resolvers

with 650 probes

coming from AS13335
https://dnsthought.nlnetlabs.nl/auth_AS1335/#rsasha256
Strange broken GOST DS in September

DNSSEC

coming from AS13335
https://dnsthought.nlnetlabs.nl/auth_AS13335/#gost

with 897 resolvers

with 650 probes

Willem Toorop
DNSThought @OARC29 27/38
Strange broken GOST DS in September

broken DS algorithm GOST validation support
https://dnsthought.nlnetlabs.nl/broken_gost/#top_auth_asns

with 231 resolvers in 185 probes

DNSSEC

Probes/resolver pairs

Remaining (28.6%)
AS43950 (0.0%)
AS42 (3.9%)
AS13335 (12.1%)
AS6830 (1.7%)
AS3265 (0.0%)
AS1103 (0.9%)
AS15169 (11.7%)
AS4804 (0.9%)
AS1 (40.3%)
The two incidents side by side

with 4304 resolvers in 3025 probes

validate DNSKEY algorithm ED25519
https://dnsthought.nlnetlabs.nl/can_ed25519/#gost
Send an EDNS Client Subnet option

With 4832 (25.3%) resolvers in 3283 (32.3%) probes

https://dnsthought.nlnetlabs.nl/does_ecs/#top_auth_asns
Send an EDNS Client Subnet option

With 498 resolvers in 338 probes

Privacy

coming from AS36692
https://dnsthought.nlnetlabs.nl/auth_AS36692/#ecs_masks
Send an EDNS Client Subnet option

With 4129 resolvers in 2963 probes

Privacy

coming from AS15169
https://dnsthought.nlnetlabs.nl/auth_AS15169/#ecs_masks
do QNAME Minimization
https://dnsthought.nlnetlabs.nl/does_qnamemin/#top_auth_asns

Privacy

QNAME Minimization

With 1624 (8.5%) resolvers in 1140 (11.2%) probes

With 1140 probes

Willem Toorop
DNSThought @OARC29 33/38
do QNAME Minimization
https://dnsthought.nlnetlabs.nl/does_qnamemin/#ecs_masks

Privacy

QNAME Minimization
with 1624 resolvers
with 1140 probes

- Also zero NX domain rewriting
- Also high % DNSSEC validation:
do NX domain rewriting
https://dnsthought.nlnetlabs.nl/does_nxdomain/#int_fwd_ext

Privacy/Security
NX domain rewriting

With 279 (1.5%) resolvers
With 206 (2.0%) probes
do NX domain rewriting
https://dnsthought.nlnetlabs.nl/does_nxdomain/#top_auth_asns

Privacy/Security
NX domain rewriting

Top 10 Probe ASNs == Top 10 Resolver ASNs == Top 10 Authoritative ASNs
do NX domain rewriting
https://dnsthought.nlnetlabs.nl/does_nxdomain/#top_nxhj_asns

Privacy/Security
NX domain rewriting
with 279 resolvers
with 206 probes

- Also only 4.3% DNSSEC validation:
DNSThought

- Public, though rough, interface to data available
  https://dnsthought.nlnetlabs.nl/

- Raw processed data available too
  https://dnsthought.nlnetlabs.nl/raw

- Focus on development of properties over time
  Per probe properties & capabilities with RIPE Atlas Probe Tags
  https://atlas.ripe.net/docs/probe-tags/

- Lots to improve
  - Dynamic (zoomable) plots
  - IPv4 & IPv6 ECS detection
  - Better DS algorithm detection
  - Fragment dropping / Path MTU

Questions
Suggestions