

TNO innovation for life

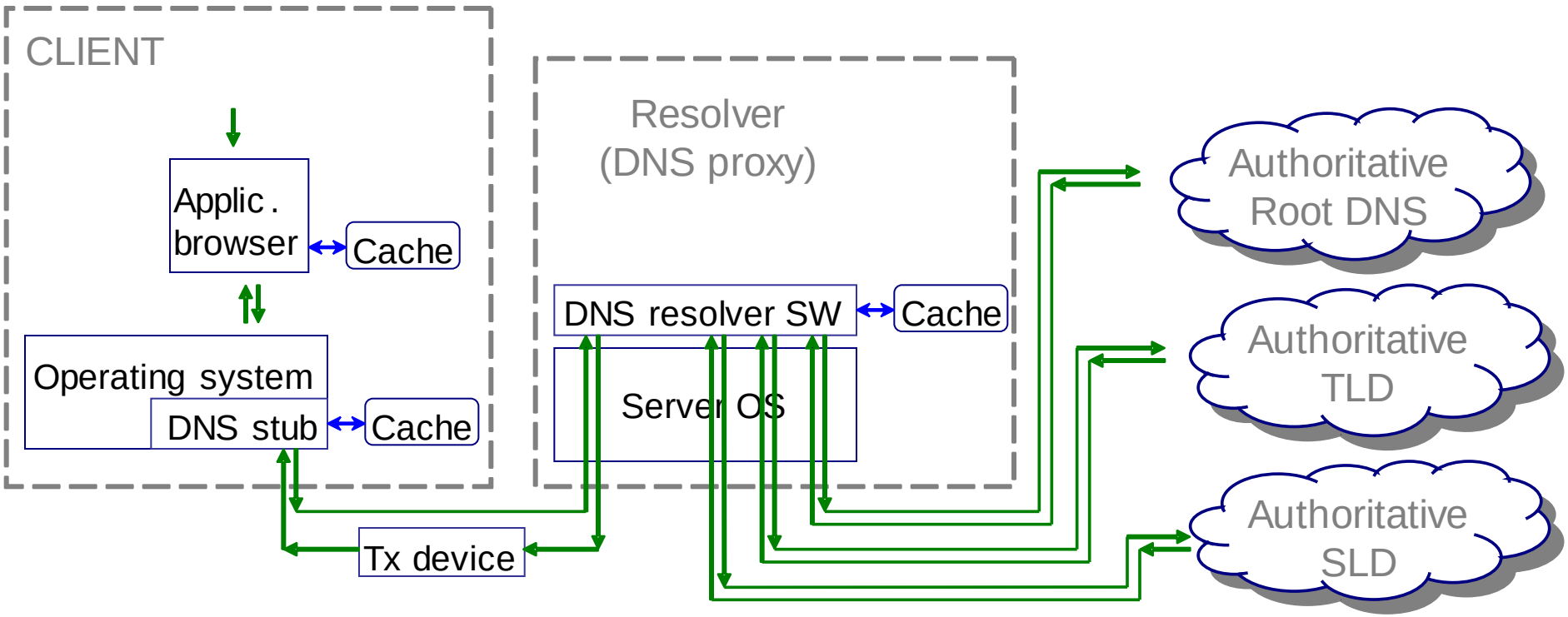
powered by SIDN

assisted by LaQuSo Laboratory for Quality Software

DNS(SEC) Client analysis

Sander Degen @ RIPE 2011 Amsterdam

‘Overview’ DNS traffic analysis



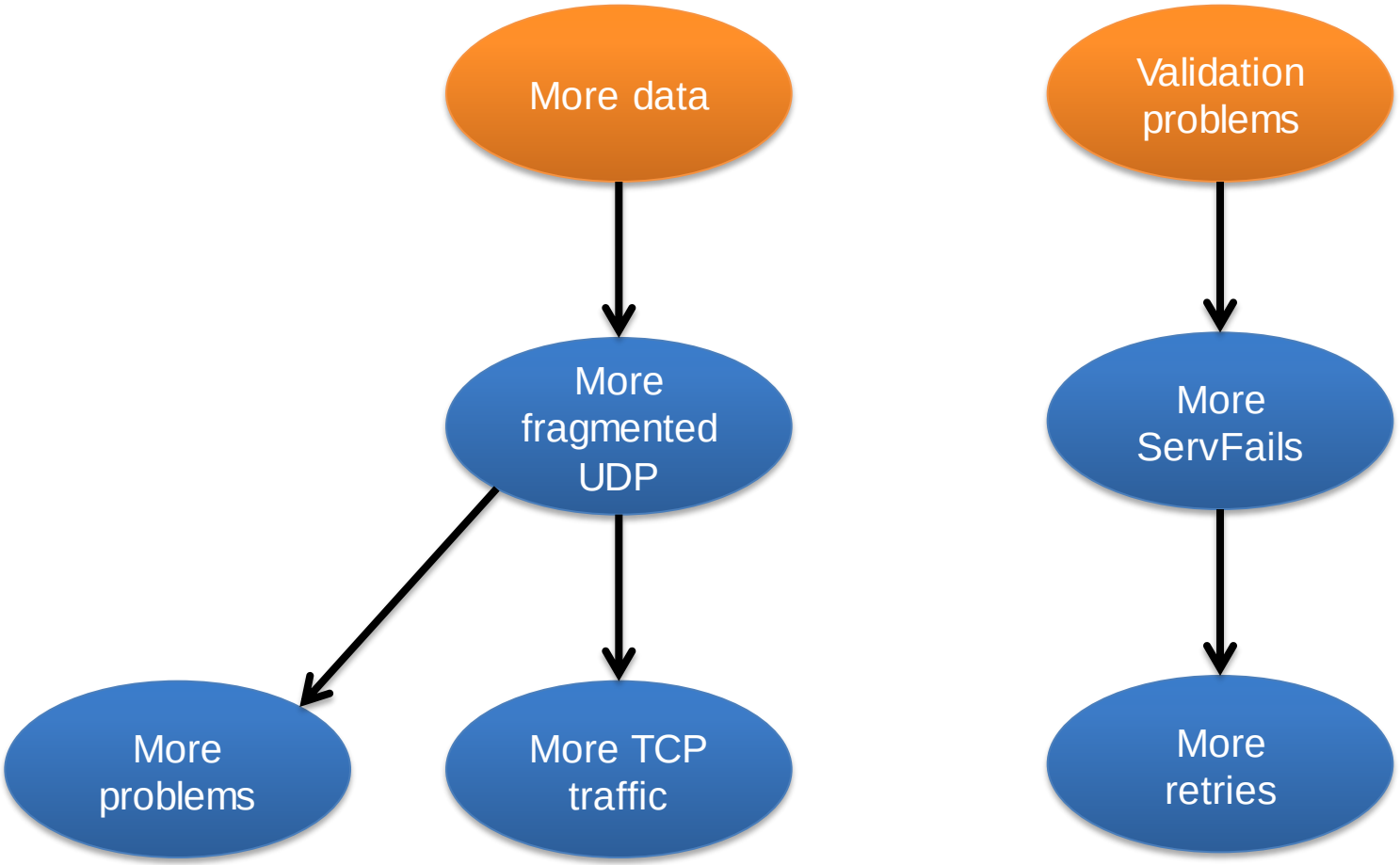
- Focus of DNS analysis has been on resolver and authoritative ⇔ bulk data analysis



TNO innovation for life

SIDN

DNSSEC changes the traffic characteristics





TNO innovation for life

SIDN

Key question:

How will DNSSEC affect client querying?

- ServFail
- >512 byte responses
- NxDomain
- No reply
- Valid response
- Recursion refused
- Partial response



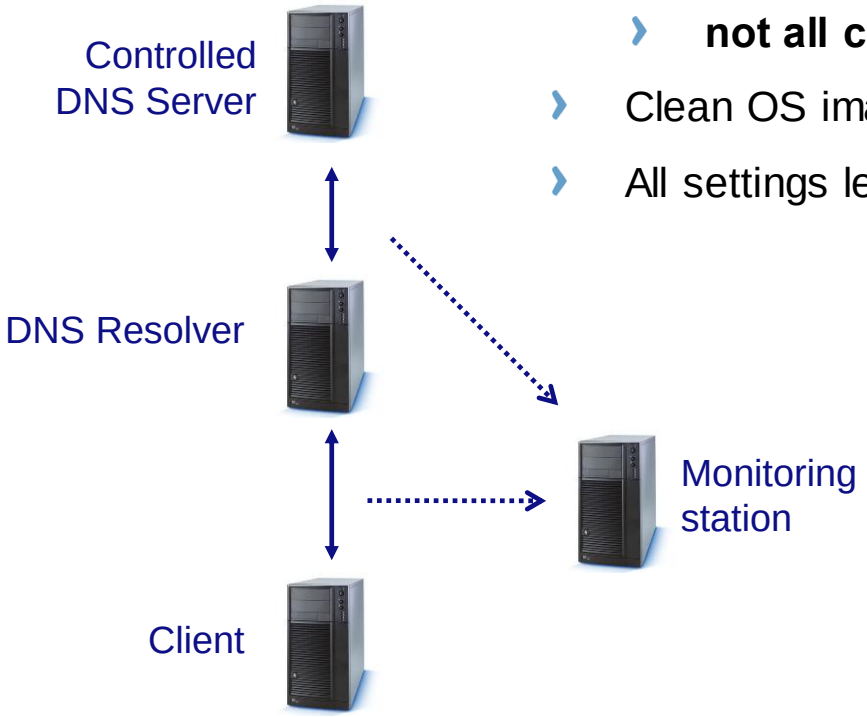
TNO innovation for life

SIDN

The Experiment

Experimental set-up

- Configure OS / browser on client machine
  - **OS: Windows XP, Windows 7, Ubuntu 10.4, Mac OSX**
  - **Browsers: IE, Firefox, Chrome, Safari**
  - **not all combinations, but quite some …**
- Clean OS image
- All settings left on defaults





TNO innovation for life

SIDN

Test execution

- Execute test run
  - query each URLs with predefined response (ldns tool)
    - **Valid, Valid (>512 Bytes), NXdomain, Partial, ServFail, No reply, Truncated, Recursion refused**
  - query via ping (=> OS only) and via browser (=> browser & OS)
  - repeat query once to check impact of caching

➢ Observe the number of repeated queries and delays



TNO innovation for life

SIDN

Browsers **Windows** Resolver *Auth*

Valid








TNO innovation for life

SIDN

Browsers **Windows** Resolver *Auth*

Truncated






TNO innovation for life

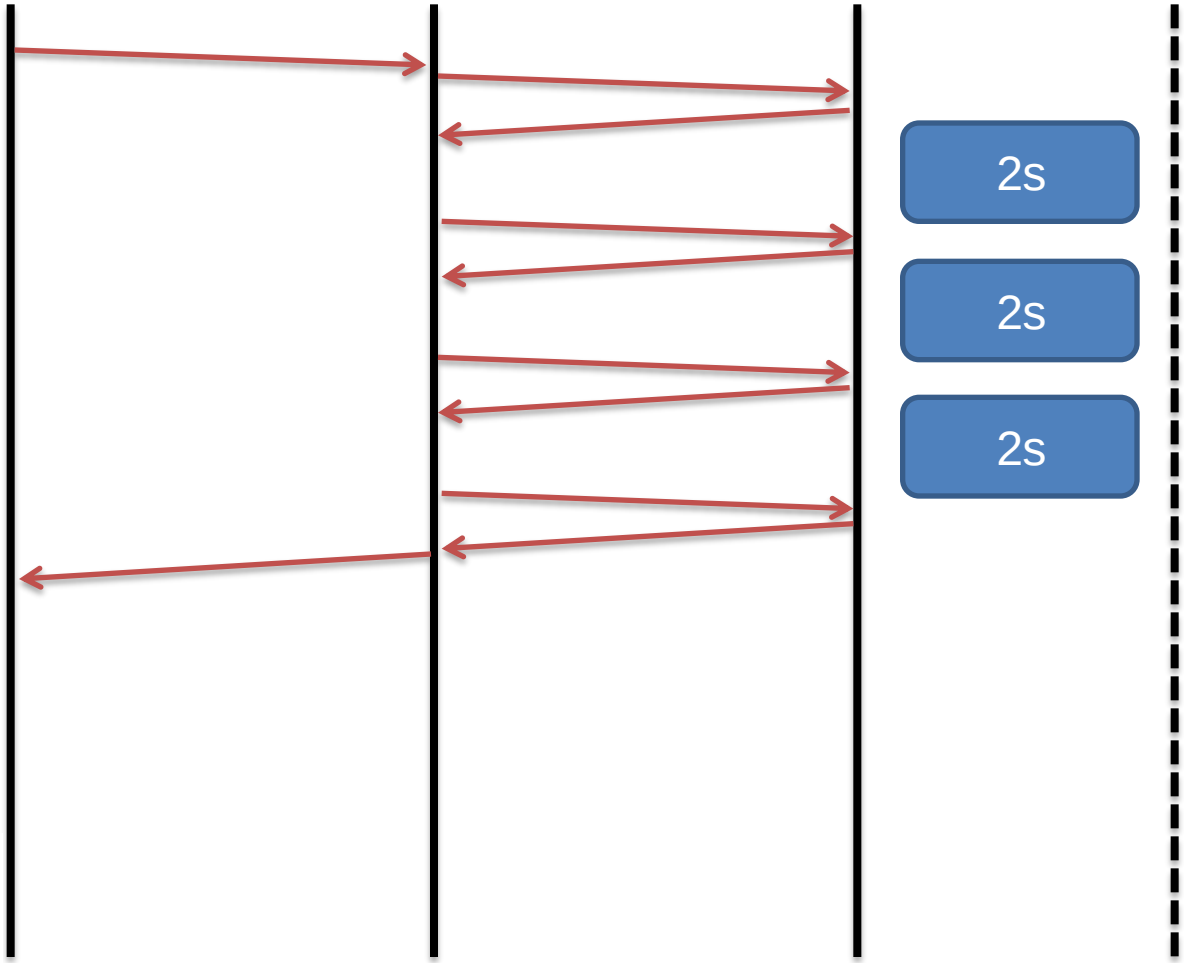
SIDN

Browsers **Windows** Resolver *Auth*

No response





2s

2s

2s



TNO innovation for life

SIDN

Browsers **Windows** Resolver *Auth*

ServFail
Partial
Refused
NxDomain








TNO innovation for life

SIDN

Safari **MacOS X** Resolver *Auth*

Valid

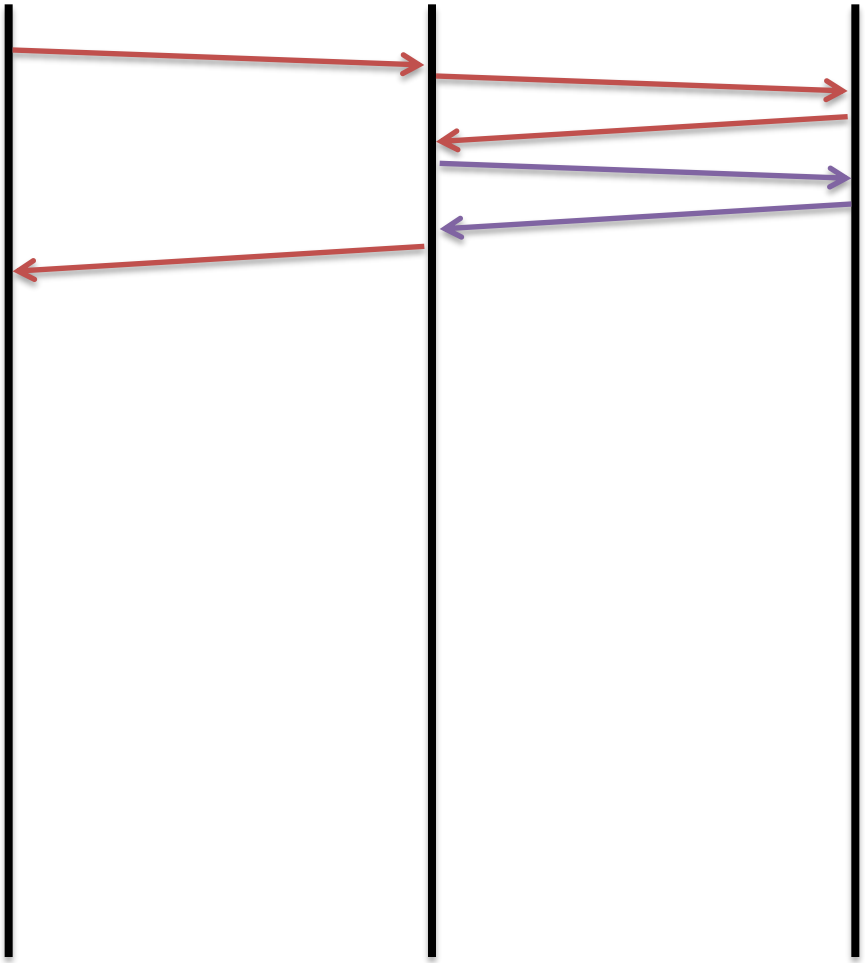


TNO innovation for life

SIDN

Safari **MacOS X** Resolver *Auth*

Truncated





TNO innovation for life

SIDN

Safari **MacOS X** Resolver *Auth*

NxDomain / Partial

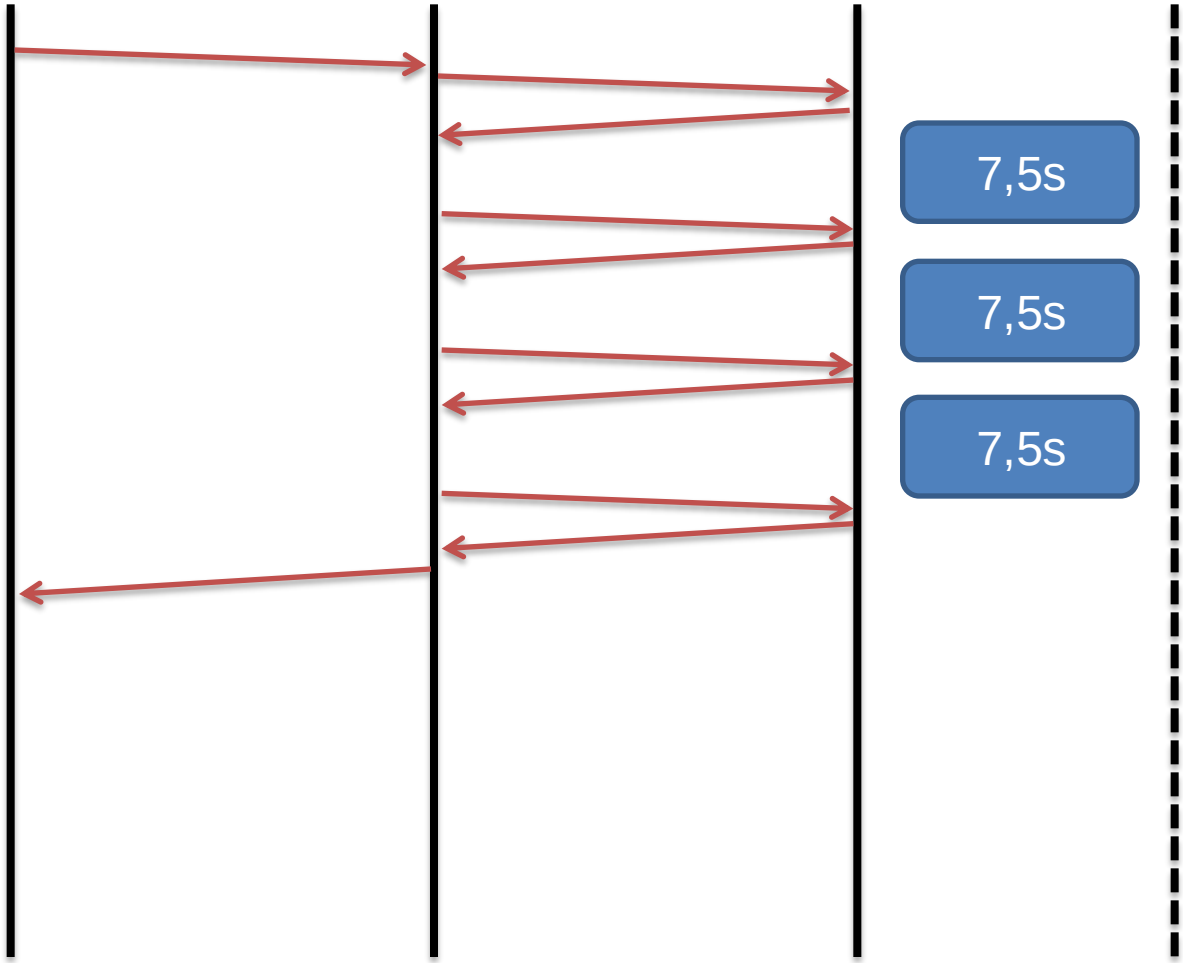


TNO innovation for life

SIDN

Safari **MacOS X** Resolver *Auth*

ServFail
No response
Refused



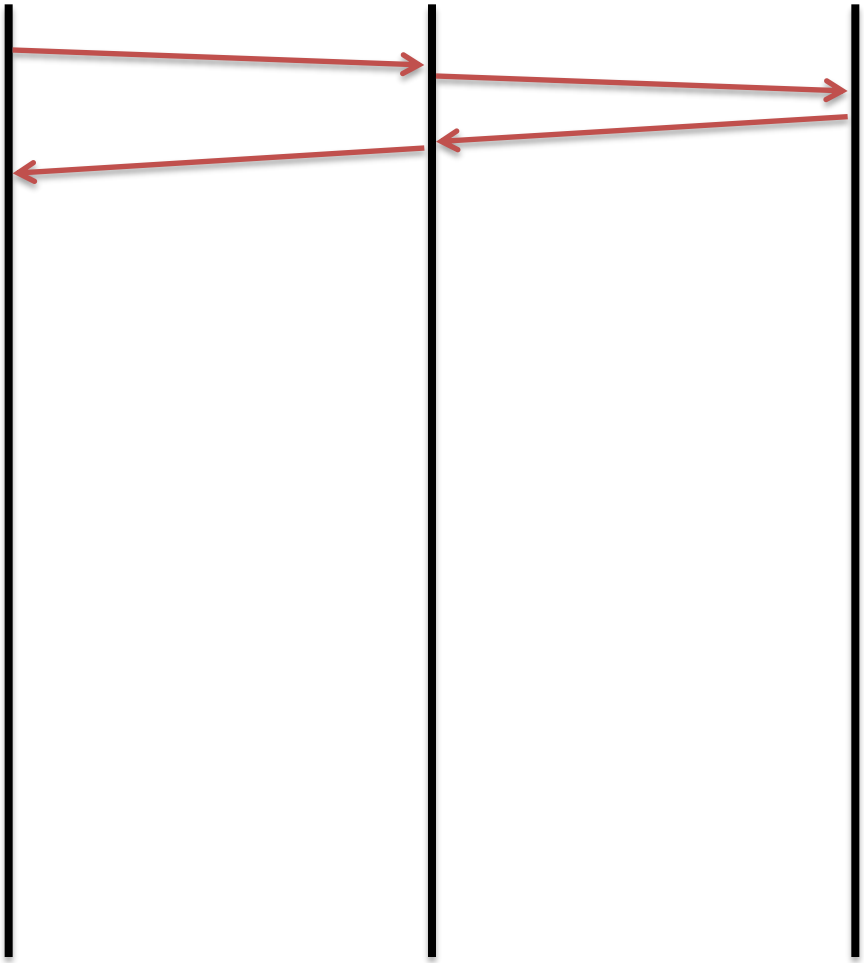


TNO innovation for life

SIDN

Firefox **Linux** Resolver *Auth*

Valid



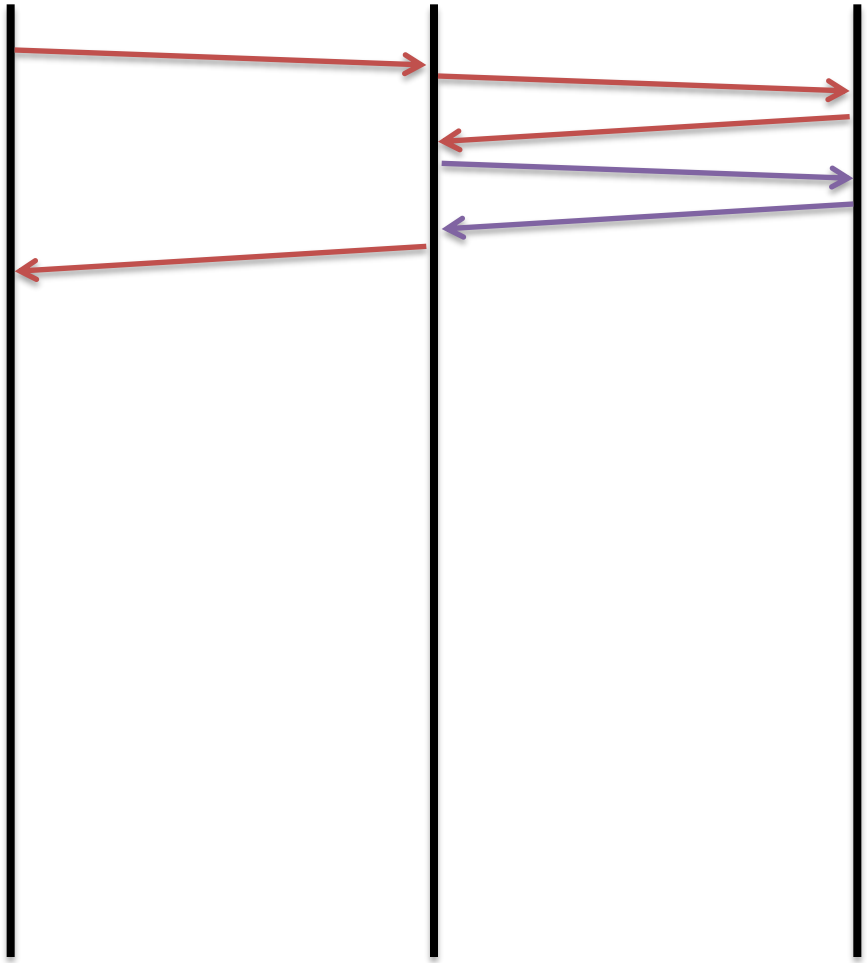


TNO innovation for life

SIDN

Firefox **Linux** Resolver *Auth*

Truncated





TNO innovation for life

SIDN

Firefox **Linux** Resolver *Auth*

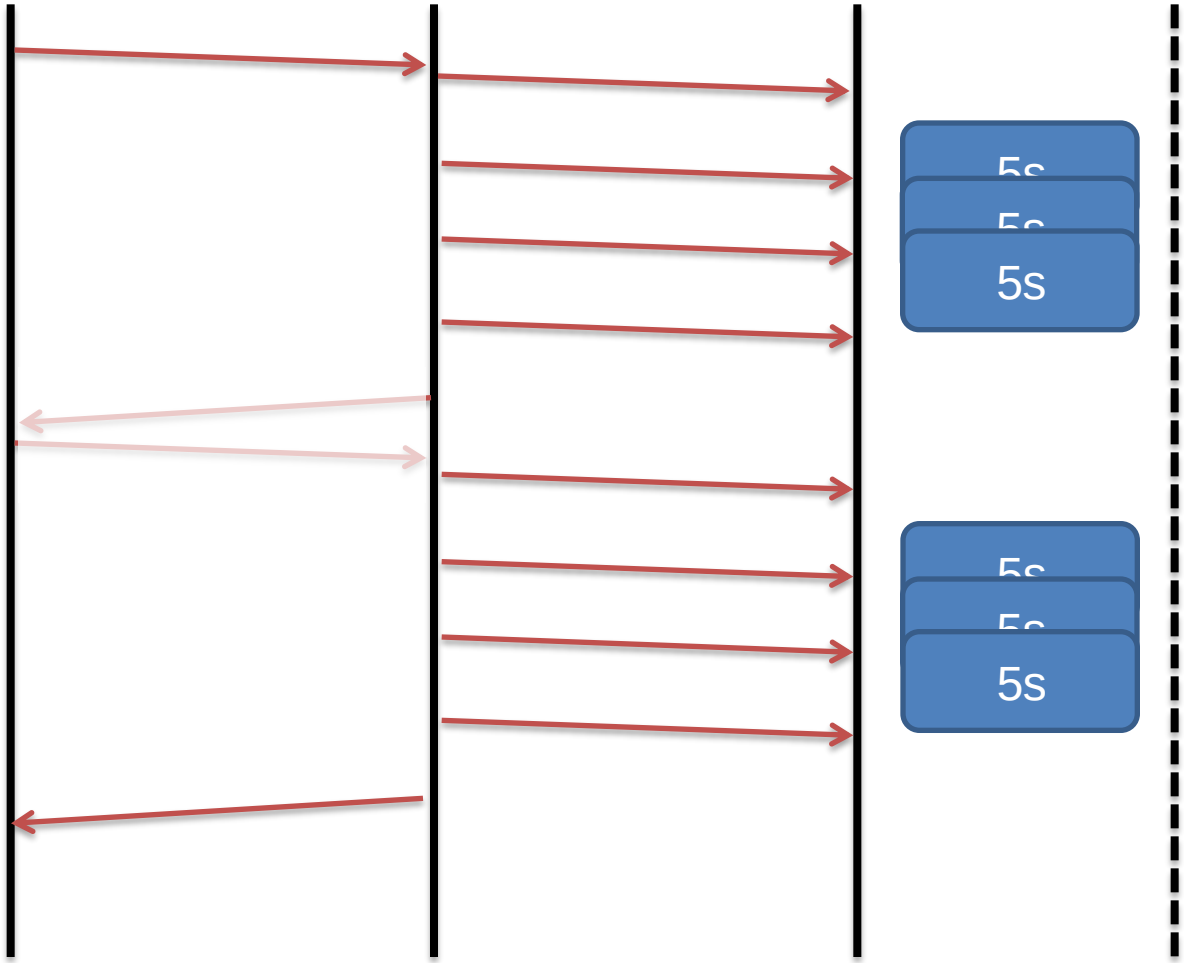
NxDomain / Partial



TNO innovation for life

SIDN

No response





TNO innovation for life

SIDN

Firefox **Linux** Resolver *Auth*

ServFail
Refused



TNO innovation for life

SIDN

x2 with secondary NS

x2 with IPv6

No caching in Ubuntu

ServFails: never cached

ServFails / Refused & Firefox + Ubuntu = :'(

Can become an issue with DNSSEC

Screenshot for ServFail on Firefox + Ubuntu

```
15:26:38.694678 IP 10.0.3.2.56600 > 10.0.2.1.53: 7000+ AAAA? servfail.dnslab.nl. (36)
15:26:38.704409 IP 10.0.2.1.53 > 10.0.3.2.56600: 7000 ServFail 0/0/0 (36)
15:26:38.704779 IP 10.0.3.2.46832 > 10.0.2.1.53: 7000+ AAAA? servfail.dnslab.nl. (36)
15:26:38.711533 IP 10.0.2.1.53 > 10.0.3.2.46832: 7000 ServFail 0/0/0 (36)
15:26:38.712139 IP 10.0.3.2.34859 > 10.0.2.1.53: 751+ AAAA? servfail.dnslab.nl. (36)
15:26:38.720254 IP 10.0.2.1.53 > 10.0.3.2.34859: 751 ServFail 0/0/0 (36)
15:26:38.722147 IP 10.0.3.2.60413 > 10.0.2.1.53: 751+ AAAA? servfail.dnslab.nl. (36)
15:26:38.732281 IP 10.0.2.1.53 > 10.0.3.2.60413: 751 ServFail 0/0/0 (36)
15:26:38.732819 IP 10.0.3.2.53267 > 10.0.2.1.53: 62476+ A? servfail.dnslab.nl. (36)
15:26:38.741631 IP 10.0.2.1.53 > 10.0.3.2.53267: 62476 ServFail 0/0/0 (36)
15:26:38.742221 IP 10.0.3.2.55543 > 10.0.2.1.53: 62476+ A? servfail.dnslab.nl. (36)
15:26:38.750843 IP 10.0.2.1.53 > 10.0.3.2.55543: 62476 ServFail 0/0/0 (36)
15:26:38.750843 IP 10.0.3.2.55146 > 10.0.2.1.53: 40336+ A? servfail.dnslab.nl. (36)
15:26:38.757800 IP 10.0.2.1.53 > 10.0.3.2.55146: 40336 ServFail 0/0/0 (36)
15:26:38.758084 IP 10.0.3.2.55095 > 10.0.2.1.53: 40336+ A? servfail.dnslab.nl. (36)
15:26:38.768255 IP 10.0.2.1.53 > 10.0.3.2.55095: 40336 ServFail 0/0/0 (36)
15:26:38.769784 IP 10.0.3.2.33077 > 10.0.2.1.53: 38673+ AAAA? servfail.dnslab.nl. (36)
15:26:38.776757 IP 10.0.2.1.53 > 10.0.3.2.33077: 38673 ServFail 0/0/0 (36)
15:26:38.776971 IP 10.0.3.2.52085 > 10.0.2.1.53: 38673+ AAAA? servfail.dnslab.nl. (36)
15:26:38.787268 IP 10.0.2.1.53 > 10.0.3.2.52085: 38673 ServFail 0/0/0 (36)
15:26:38.787583 IP 10.0.3.2.60192 > 10.0.2.1.53: 55536+ AAAA? servfail.dnslab.nl. (36)
15:26:38.797645 IP 10.0.2.1.53 > 10.0.3.2.60192: 55536 ServFail 0/0/0 (36)
15:26:38.797985 IP 10.0.3.2.46728 > 10.0.2.1.53: 55536+ AAAA? servfail.dnslab.nl. (36)
15:26:38.803552 IP 10.0.2.1.53 > 10.0.3.2.46728: 55536 ServFail 0/0/0 (36)
15:26:38.803796 IP 10.0.3.2.60114 > 10.0.2.1.53: 40195+ A? servfail.dnslab.nl. (36)
15:26:38.810014 IP 10.0.2.1.53 > 10.0.3.2.60114: 40195 ServFail 0/0/0 (36)
15:26:38.810456 IP 10.0.3.2.35270 > 10.0.2.1.53: 40195+ A? servfail.dnslab.nl. (36)
15:26:38.823206 IP 10.0.2.1.53 > 10.0.3.2.35270: 40195 ServFail 0/0/0 (36)
15:26:38.823551 IP 10.0.3.2.57144 > 10.0.2.1.53: 50408+ A? servfail.dnslab.nl. (36)
15:26:38.829749 IP 10.0.2.1.53 > 10.0.3.2.57144: 50408 ServFail 0/0/0 (36)
15:26:38.829961 IP 10.0.3.2.35860 > 10.0.2.1.53: 50408+ A? servfail.dnslab.nl. (36)
15:26:38.836833 IP 10.0.2.1.53 > 10.0.3.2.35860: 50408 ServFail 0/0/0 (36)
```

↔ example: servfail response

3 immediate retries in case of servfail response

and IPv4?

OS sends servfail to FireFox;

Firefox(?) makes OS retry

16 queries in 0.14 seconds


Reality



TNO innovation for life

SIDN

Real-life data

- Provided by Dutch ISP (>1 million DNS packets)
- Analysed by graduate student Yakup Koc
- Confirms ServFail ‘spam’ from Linux clients
  - 8x A, 8x AAAA, 8x MX
  - Identified through TTL



TNO innovation for life

SIDN

Resolvers

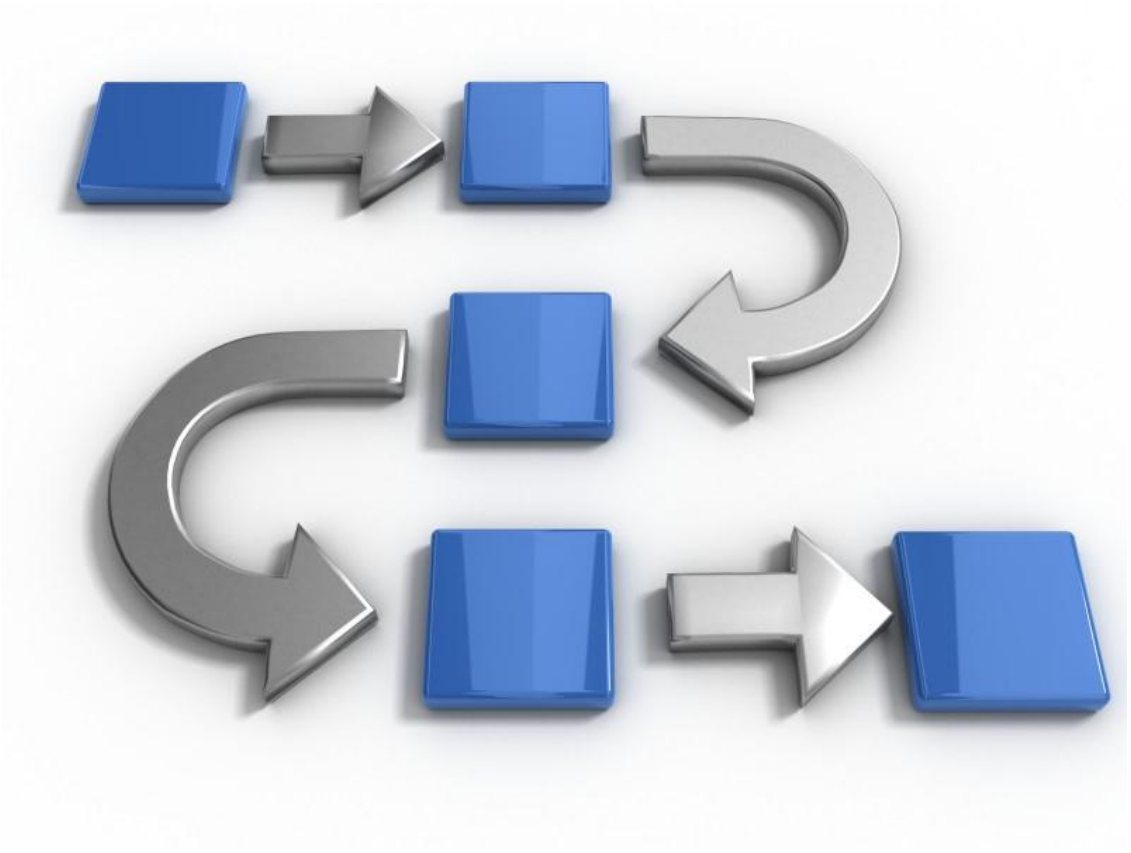
- BIND9:
  - ServFail: 1 request elicits 2 queries, answer is not cached
  - Timeout: 1 request elicits 7 queries, but answer is cached
  - RecRef: 1 request elicits 1 query, answer is not cached
- Unbound:
  - ServFail: 1 request elicits 5 queries, but answer is cached (~7 seconds)
  - Timeout: 1 request elicits 7 queries, but answer is cached
  - RecRef: 1 request elicits 5 queries, but answer is cached (~7 seconds)



TNO innovation for life

SIDN

Past, present and future





TNO innovation for life

SIDN

What now?

Already done:

- Analysis of glibc source code by LaQuSo
- Analysis of impact of servfail behaviour

In progress:

- A DNS health monitor study

Planned:

- Behaviour of **mobile** clients (smartphones etc)



TNO innovation for life

SIDN

Questions?

Contact info:
Mail: Sander.Degen@TNO.nl
Phone: 06-10 96 87 96