“DNS Flag day”

A tale of five ccTLDs

Hugo Salgado, .CL
Sebastián Castro, .NZ

DNS-OARC 29, Amsterdam

nic chile
SOMOS EL PUNTO CL

InternetNZ

What is EDNS?

- RFC 6891
  - Defines a backward compatible mechanism to signal support for new DNS options
  - Original specification includes support for DNS responses larger than 512 bytes, extended response codes, etc.

How is it used?

Current extensions:

- NSID -- RFC 5001, nameserver identification string
- DNSSEC -- DO bit, signals supports or interest for DNSSEC-related records
- Client-subnet, RFC 7871, signals the network the query comes from
- Keep-alive, RFC 7828, variable timeouts for DNS over TCP
- Cookies, IETF Draft, lightweight security mechanism
- and more to come

So, what's the problem?

Authoritative DNS servers block responses, or don't answer, or answer with the wrong packet.

In general, bad implementations of DNS not following the standards

Poorly implemented firewalls on the way, poor firewall rules blocking valid traffic or unaware of the standards

Resolvers have to send a query, wait for a timeout and retry using a different method: TCP or discard EDNS

Forces delays and thwarts innovation and deployment of new features

What’s DNS Flag day?

DNS implementations decided to remove workarounds in a coordinated way

BIND, Unbound, PowerDNS and Knot will release new versions with the workarounds removed

Feel the pain

If you run inadequate software, your domains will break

How many domains could be affected?

Coordinated effort to measure impact in .CL, .CZ, .SE, .NU and .NZ

Many thanks to Petr Špaček from CZ.NIC for the Compliance Scanner, the .CZ, .SE and .NU data and the feedback

Comparison against existing measures from ISC around root servers and TLDs nameservers

Measurement methodology

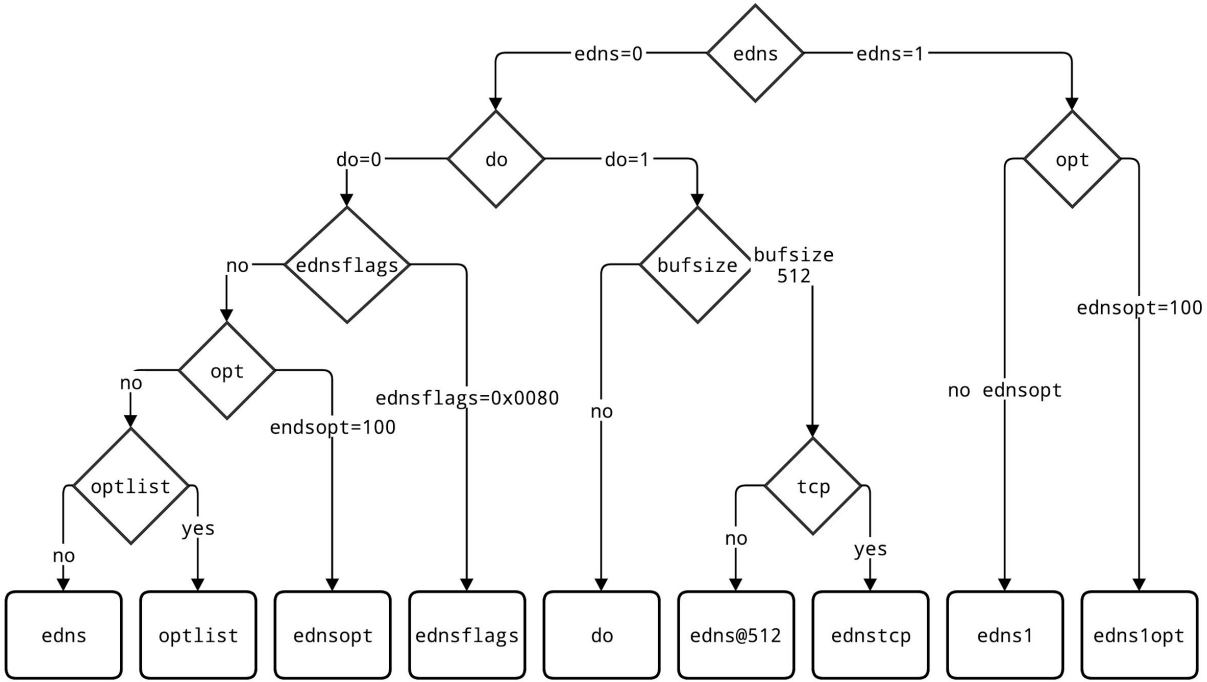
- “DNS Compliance Testing” tool written by ISC
  https://gitlab.isc.org/isc-projects/DNS-Compliance-Testing
  - Only check for EDNS compliance at this stage
- “EDNS Compliance scanner for DNS zones” from CZ.NIC:
  - https://gitlab.labs.nic.cz/knot/edns-zone-scanner/tree/master
  - Uniquely test all addresses of a nameserver
  - Preprocess a TLD zone and generate the minimal set of nameserver tests
  - Test multiple times to discard transient errors

Test hierarchy

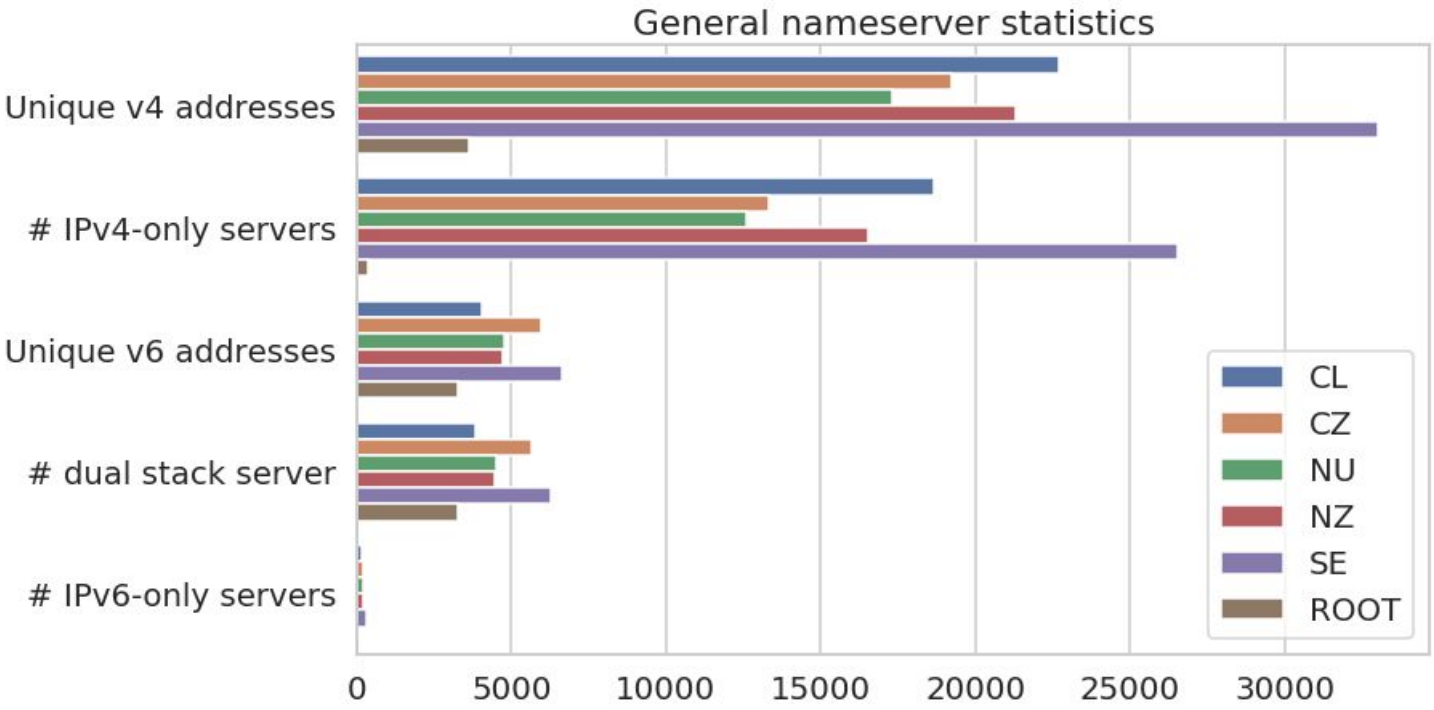
Different values and flags are added to the query

There are dependencies, increasing the complexity of the test

edns1opt requires edns1 and endsopt=100 to pass



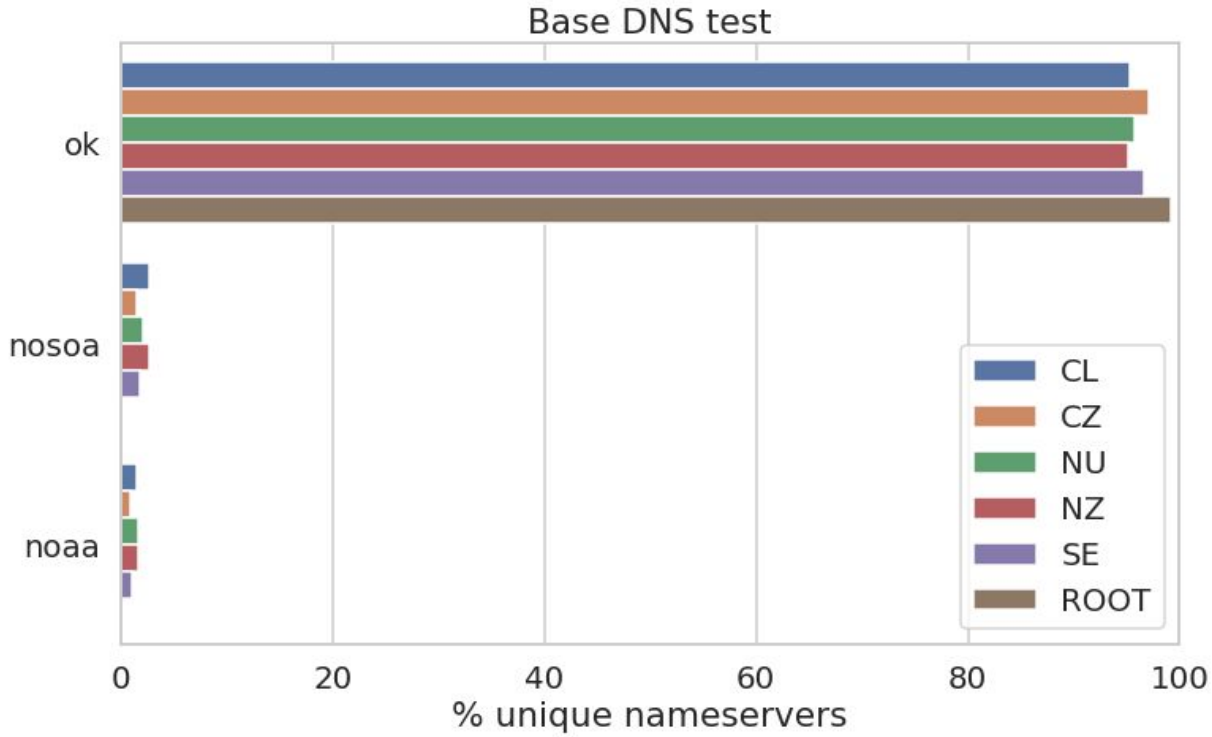
General statistics



DNS test results

dig +noedns +noad +norec SOA <ZONE>

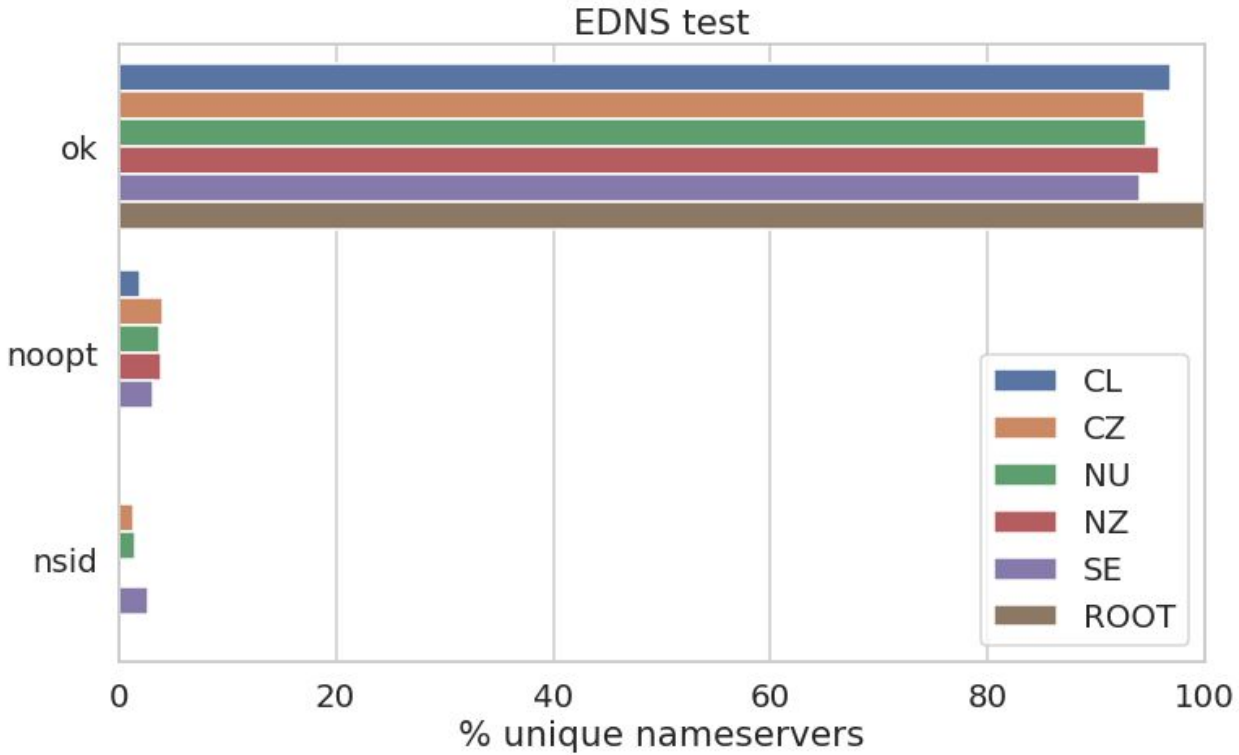
- ok: We got a good answer
- nosoa: Response didn't have SOA record
- noaa: no AA bit in response



DNS vs EDNS

DNS: dig **+noedns** +noad +norec SOA <zone>

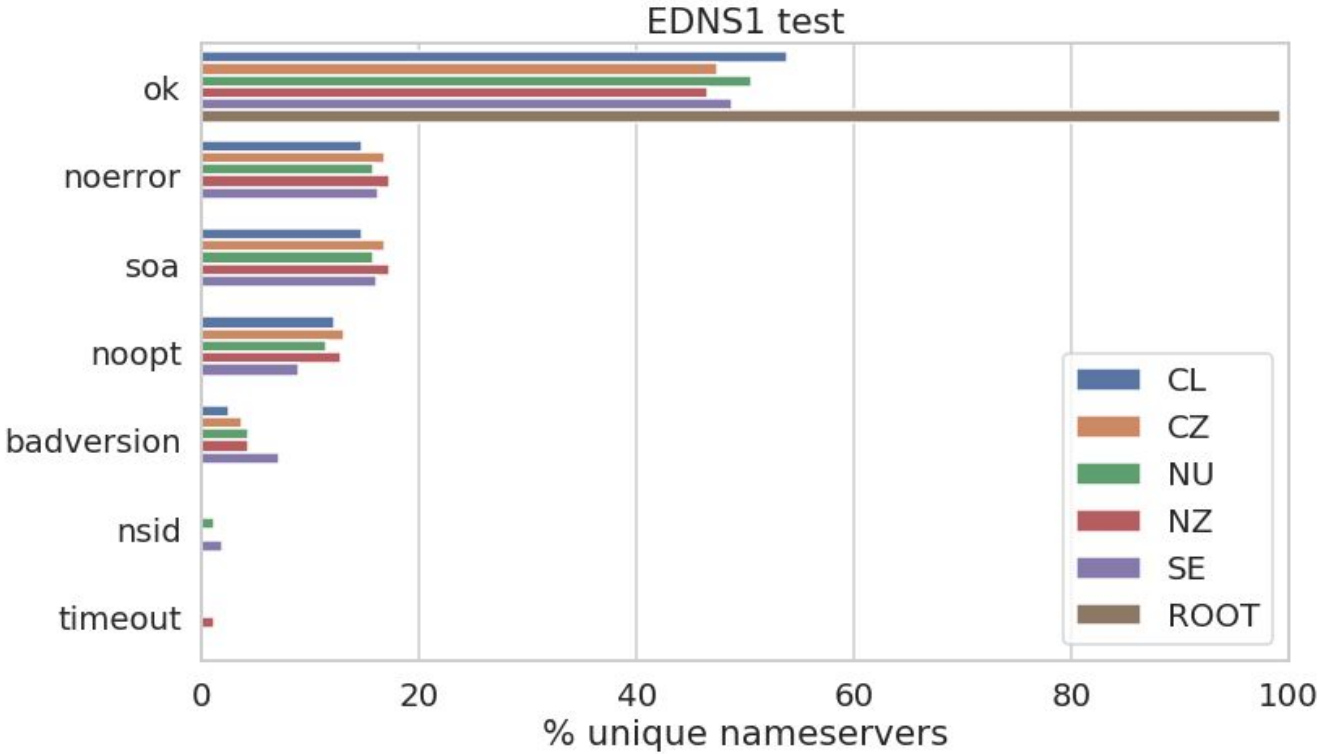
EDNS: dig **+edns=0 +nocookie** +noad +norec SOA <zone>



EDNS0 vs EDNS1

EDNS0: dig
+edns=0 +nocookie
+noad +norec SOA
<zone>

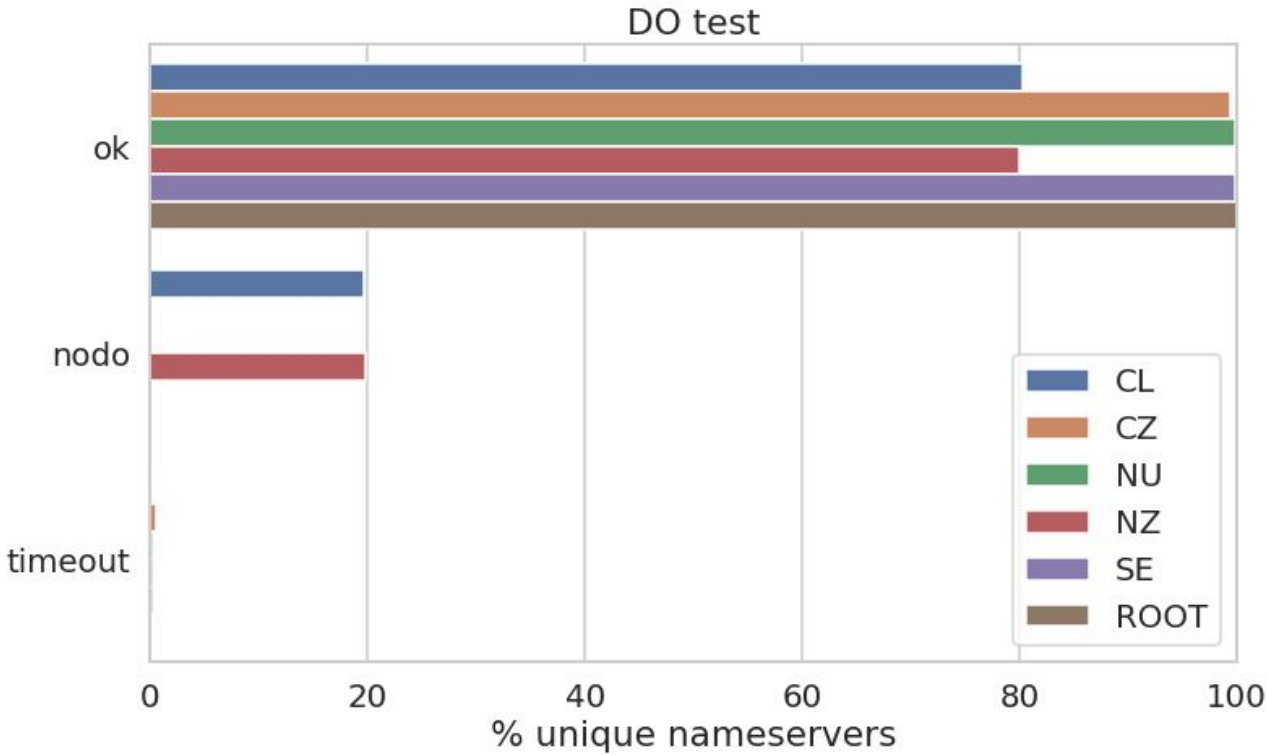
EDNS1: dig
+edns=1
+noednsneg
+nocookie +noad
+norec SOA <zone>



EDNS vs DO

EDNS: dig +edns=0 +nocookie +noad +norec SOA <zone>

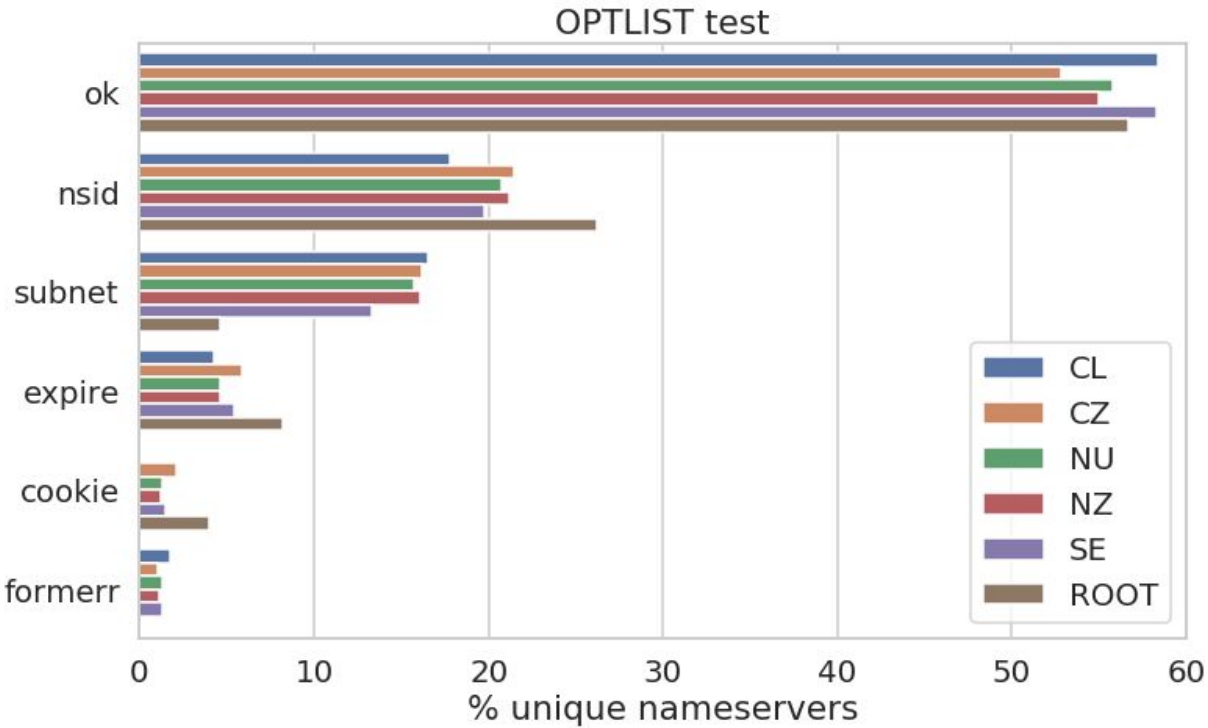
DO: dig +edns=0 +nocookie +noad +norec **+dnssec** SOA <zone>



EDNS vs OPTLIST

EDNS: dig +edns=0 +nocookie +noad +norec SOA <zone>

OPTLIST: dig +edns=0 +noad +norec **+nsid +subnet=0.0.0.0/0 +expire +cookie=0102030405060708** SOA <zone>



IPv4 vs IPv6

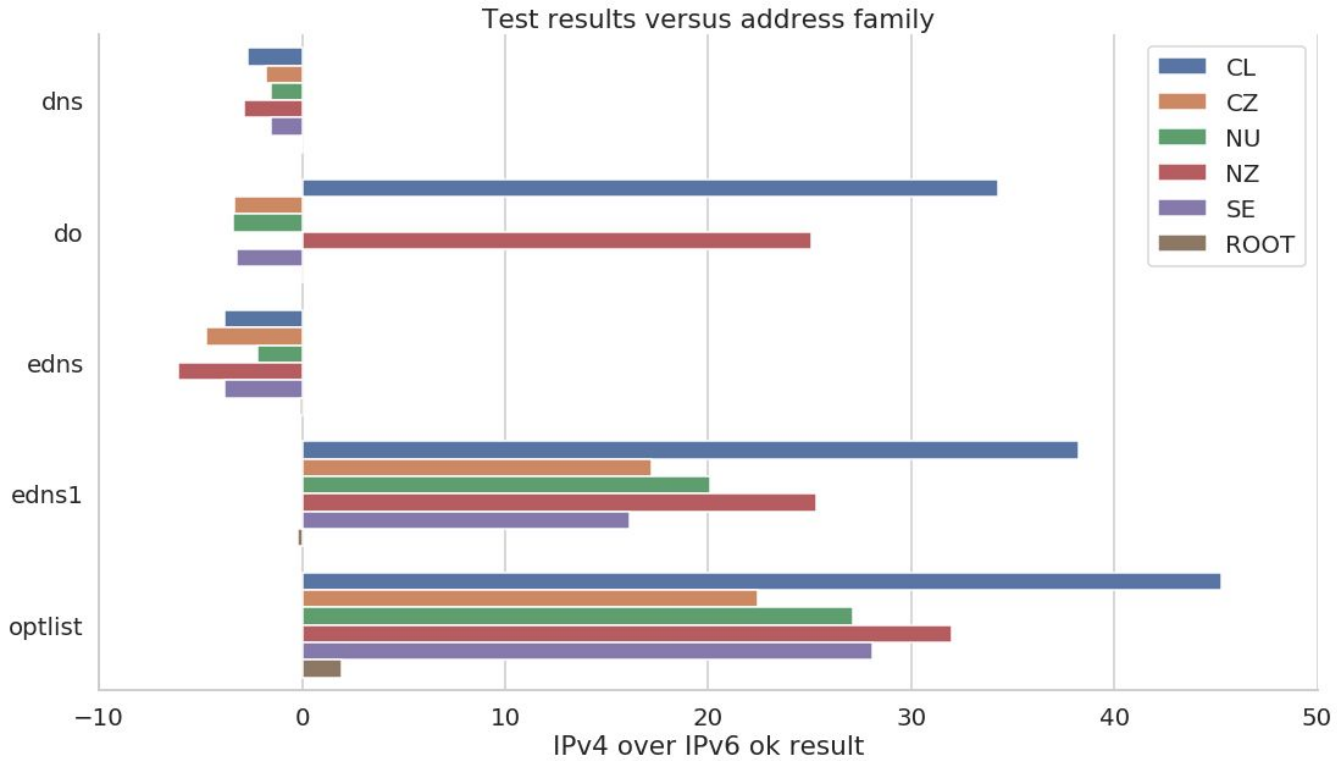
Is the behaviour of a given nameserver different depending on which address family was queried? Are they differences between IPv4 and IPv6

We can explore the tests that passed against the family of the address.

IPv4 vs IPv6

DNS and EDNS tests finish more successfully in IPv6 than IPv4!

EDNS1 and OPTLIST complete a lot more in IPv4 than IPv6!

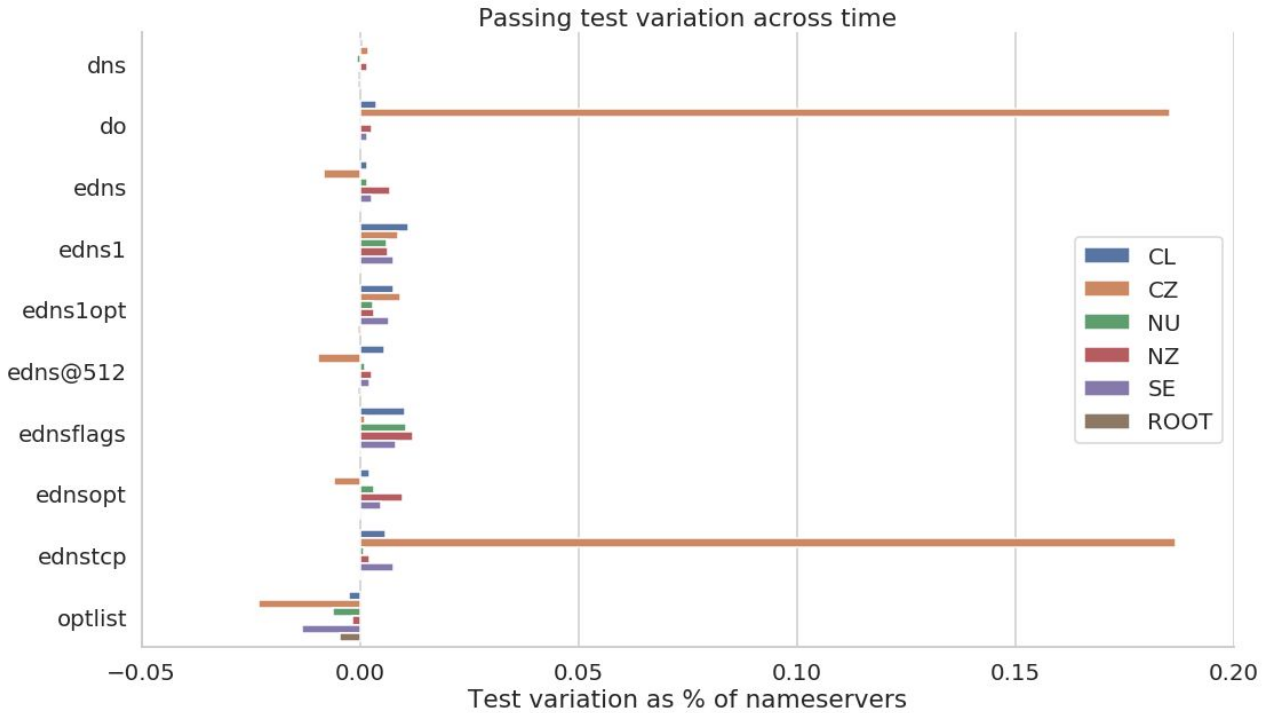


How the results change with time?

First data point is from May to July depending on the ccTLD

Last data point is from October.

CZ is seeing the improvements of their communication campaign.



How can I correct the errors?

- Use a modern implementation of DNS software
- Use software that follows the standards
- Fix your firewall rules, especially around DPI of DNS traffic
- Re-test

Future work

We plan to continue the collection monthly to identify trends

Communication campaign to reduce the number of errors.

We encourage other namespace operators (ccTLDs) to check their domains

Watch the world burn on February 1st 2019

Questions

https://dnsflagday.net

Hugo Salgado, hsalgado@nic.cl
Sebastián Castro, sebastian@internetnz.net.nz

nic chile
SOMOS EL PUNTO CL

InternetNZ