Assessing e-Government DNS Resilience

Raffaele Sommese[1] Mattijs Jonker[1]
Jeroen van der Ham[1,2] **Giovane C. M. Moura**[3,4]

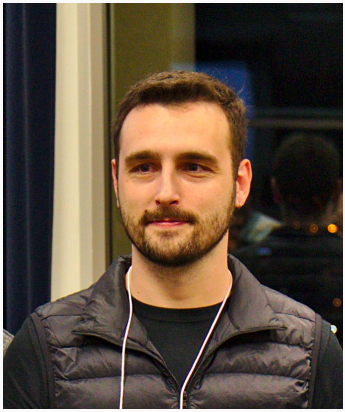
1: University of Twente, **2**: NCSC-NL **3**: SIDN Labs, **4**:TU Delft

RIPE 86
Rotterdam, The Netherlands
2023-05-23

UNIVERSITY OF TWENTE. Nationaal Cyber Security Centrum Ministerie van Justitie en Veiligheid SIDN LABS TU Delft

In memoriam

- Ricardo de Oliveira Schmidt
- † March 2nd, 2023



Context

- The NCSC-NL commissioned SIDN Labs for a study on Dutch e-gov DNS resilience
  - DINO project
- We teamed-up with the University of Twente
- This research is an extension of this project

Introduction

- Governments increasingly use Internet for communication with citizens (e-gov)
- E-gov provide crucial services

E-gov in the Netherlands:

Digid	Taxes
MyOverheid	DUO
Chamber of Commerce	RDW (DMV)
Unemployment Benefits	Welfare

Introduction

- Governments increasingly use Internet for communication with citizens (e-gov)
- E-gov provide crucial services

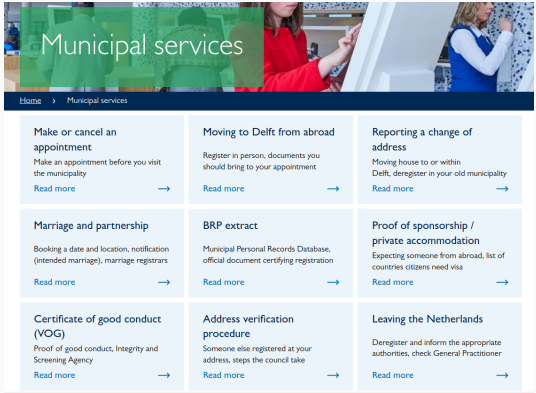
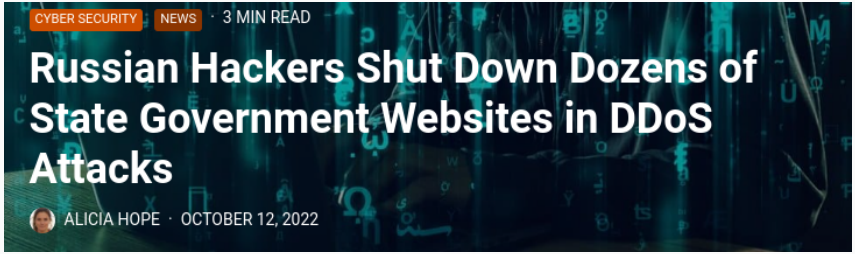


Figure 1: Delft (local government) residents e-gov

When e-gov breaks



source: CPO Magazine

"Russian hackers took responsibility for a wave of cyber attacks that knocked dozens of state government websites offline.
Several states, including Colorado, Connecticut, Kentucky, and Mississippi, were impacted by the politically-motivated cyber attacks ..."

E-gov is fully dependent on DNS

- E-gov provide crucial services
- Internet as core communications fabric of modern societies.
- E-gov is fully dependent on DNS

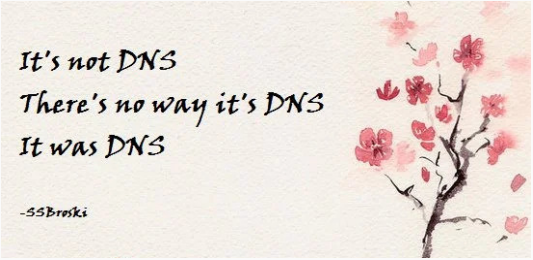


Figure 2: A haiku about DNS.
Source: Cyberciti

DNS Engineering for resilience

- DNS has been designed for resilience
  - multiple layers of redundancy
- Deploying those features is not easy/cheap
- Configuration errors may go unnoticed
  - system will still work
  - until it breaks

Source: Unsplash

Research Question

Are e-gov DNS serves configured following best-practices for robustness?

Approach: Internet measurements

Research Question

Are e-gov DNS serves configured following best-practices for robustness?

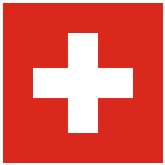
Approach: Internet measurements

Our contribution

1. E-gov DNS infrastructure evaluation for four countries
    - using active measurements
2. A comparative analysis among them
3. Recommendations for improvement

The Netherlands

Switzerland



Sweden

United States

Datasets

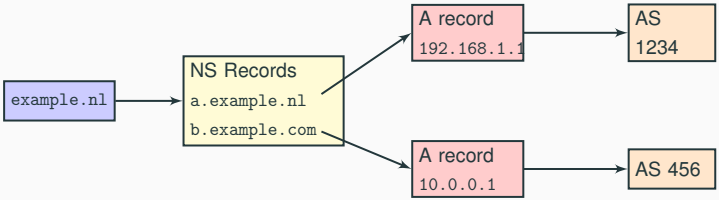
Country	Netherlands .nl 	Sweden .se 	Switzerland .ch 	United States .gov 
e-gov domains (SLD)	602	614	3971	7972
Population	17.4M	10.4M	8.7M	332.9M

Results: single points of failure (SPoF)

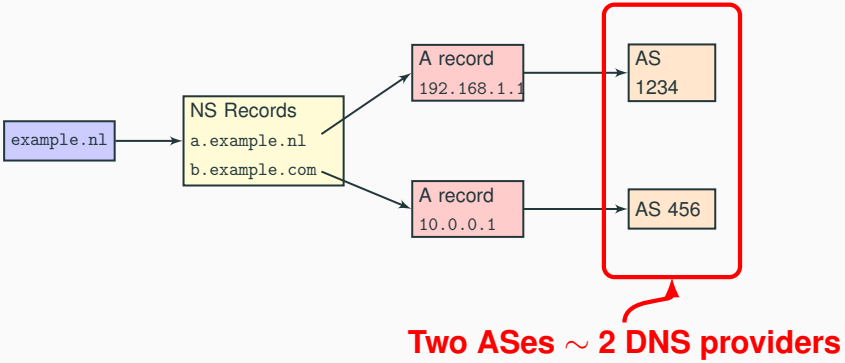
- Don´t put all your eggs in one basket
  - We will look into diff basket types

Source: Unsplash

First SPOF: single DNS providers



First SPOF: single DNS providers



First SPOF: single DNS providers

	Netherlands 	Sweden 	Switzerland 	United States 
second-level domains	602	614	3971	7972
Responsive	601	609	3546	7911
single provider(v4/v6)	43% /55%	41%/41%	43%/54%	82%/ 55%

- **US: $\sim$ 80% single DNS provider**

“But this is a bogus metric!”

- “I’ll put everything in the **cloud**”
- But even clouds occasionally fail:
  - Dyn 2016
  - AWS Route 53 - 2019
- Even Amazon.com does not use AWS for DNS:

```
pdns1.ultradns.net.
ns4.p31.dynect.net.
ns2.p31.dynect.net.
pdns6.ultradns.co.uk.
ns1.p31.dynect.net.
ns3.p31.dynect.net.
```

“But this is a bogus metric!”

- “I’ll put everything in the **cloud**”
- But even clouds occasionally fail:
  - Dyn 2016
  - AWS Route 53 - 2019
- Even Amazon.com does not use AWS for DNS:

```
pdns1.ultradns.net.
ns4.p31.dynect.net.
ns2.p31.dynect.net.
pdns6.ultradns.co.uk.
ns1.p31.dynect.net.
ns3.p31.dynect.net.
```

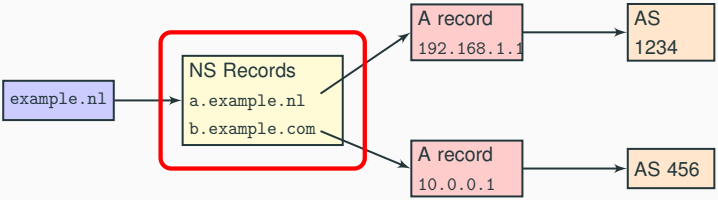
DNS centralization: who are these DNS providers

Netherlands		Sweden		Switzerland		United States	
ASN	e-gov	ASN	e-gov	ASN	e-gov	ASN	e-gov
Transip	112	Loopia	47	Infomaniak	278	GoDaddy	1215
CLDIN	39	Tele2	23	Swisscomm	115	Cloudflare	909
QSP	28	Microsoft	21	Novatrend	100	Amazon	676
Solvinity	8	Telia	21	Abraxas	97	Akamai	334
SSC-ICT	8	Telia	19	Metanet	91	Tiggee	316

Table 1: Top 5 DNS providers for e-gov domains

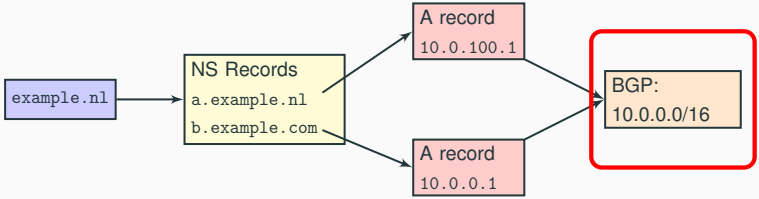
Most DNS providers are **local**

Second SPoF: single DNS server



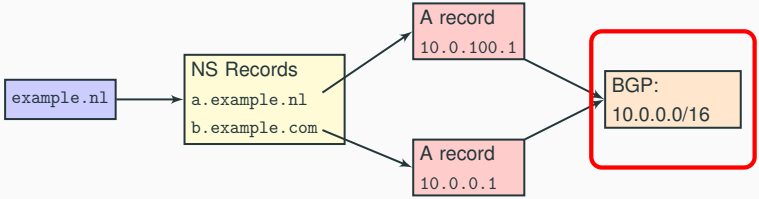
- RFC1034 (35 years old!) mandates at least two NS records
- We found 6 `.gov` domains that did have a single NS record
- We notified the `.gov` registry, 3 fixed it (2023-05-09)

Third SPoF: BGP prefixes



- If two DNS servers share the same prefix, they are not topologically diverse
  - they share the same infrastructure
- We map the IP addresses of each NS to their prefixes

Third SPoF: BGP prefixes

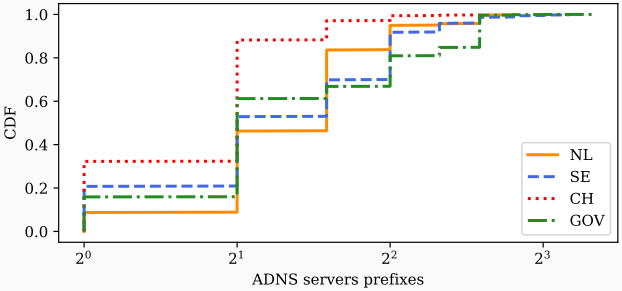


One BGP prefix = same location

- If two DNS servers share the same prefix, they are not topologically diverse
  - they share the same infrastructure
- We map the IP addresses of each NS to their prefixes

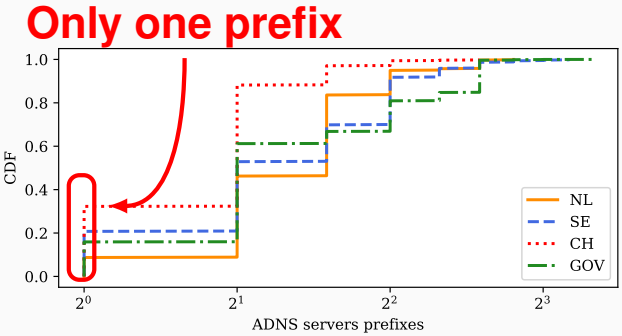
Third SPoF: BGP prefixes

- Switzerland: 1/3 e-gov domains have a single prefix
- NL, SE, US: $<$ 20%

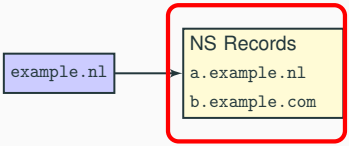


Third SPoF: BGP prefixes

- Switzerland: 1/3 e-gov domains have a single prefix
- NL, SE, US: $<$ 20%

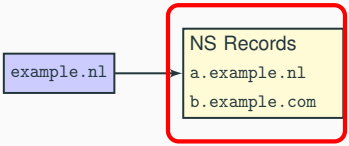


Fourth SPoF: Number of TLDs



- NS records depend on top-level domains (TLDs)
- Having more than one TLD protect you fail TLD failures
  - Warning: it's TLDs for NS records, not the domains themselves

Fourth SPoF: Number of TLDs

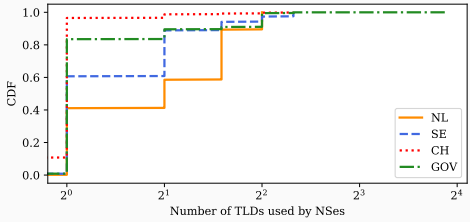


Two TLDs: `.nl` and `.com`

- NS records depend on top-level domains (TLDs)
- Having more than one TLD protect you fail TLD failures
  - Warning: it's TLDs for NS records, not the domains themselves

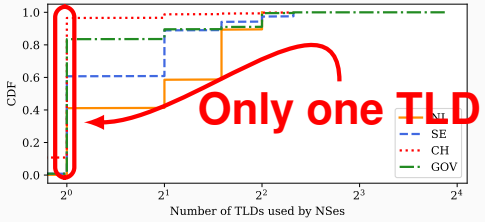
Fourth SPoF: Number of TLDs

- Switzerland e-gov mostly uses only one TLD
- Netherlands is the most diverse
- All four countries can diversity still



Fourth SPoF: Number of TLDs

- Switzerland e-gov mostly uses only one TLD
- Netherlands is the most diverse
- All four countries can diversity still



TLD dependency

	Netherlands	Sweden	Switzerland	United States
1	170 (.nl)	483 (.se)	609 (.ch)	2507 (.com)
2	69 (.net)	100 (.net)	190 (.com)	1541 (.net)
3	26 (.com)	82 (.com)	150 (.net)	894 (.gov)
4	12 (.eu)	14 (.info)	19 (.org)	485 (.org)
5	4 (.be)	8 (.org)	12 (.de)	302 (.us)

Table 2: Most used TLD by e-gov ADNS severs.

- Most use their own TLD, then .com and .net

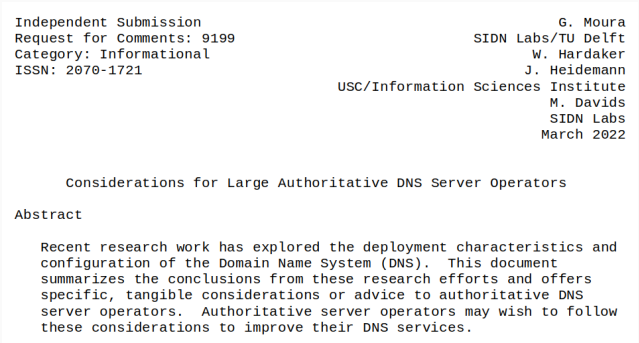
Extra features that improve resilience (RFC9199)

1.IP Anycast

- Covered in Moura16b

2.DNS Time-to-live (TTLs)

- covered in Moura18b, Moura19b



Independent Submission
Request for Comments: 9199
Category: Informational
ISSN: 2070-1721

G. Moura
SIDN Labs/TU Delft
W. Hardaker
J. Heidemann
USC/Information Sciences Institute
M. Davids
SIDN Labs

March 2022

Considerations for Large Authoritative DNS Server Operators

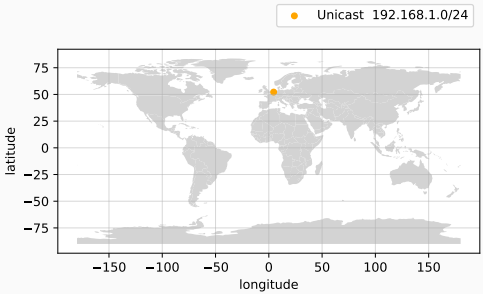
Abstract

Recent research work has explored the deployment characteristics and configuration of the Domain Name System (DNS). This document summarizes the conclusions from these research efforts and offers specific, tangible considerations or advice to authoritative DNS server operators. Authoritative server operators may wish to follow these considerations to improve their DNS services.

Both summarized in RFC9199

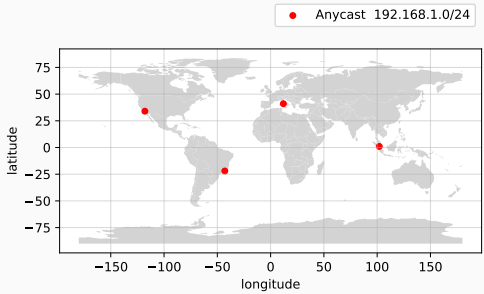
IP anycast

Unicast



- One location
- All traffic to it

Anycast

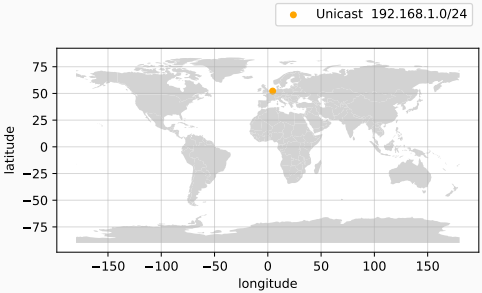


- Multiple locations
- Traffic distributed among them

Anycast is more resilient to DDoS (Moura16b)

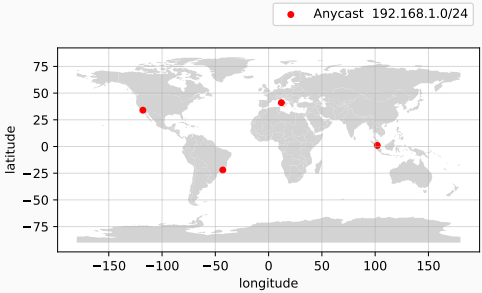
IP anycast

Unicast



- One location
- All traffic to it

Anycast

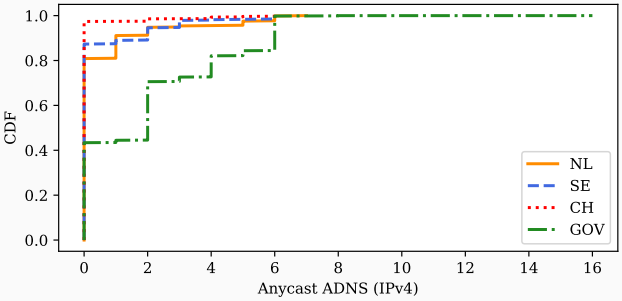


- Multiple locations
- Traffic distributed among them

Anycast is more resilient to DDoS (Moura16b)

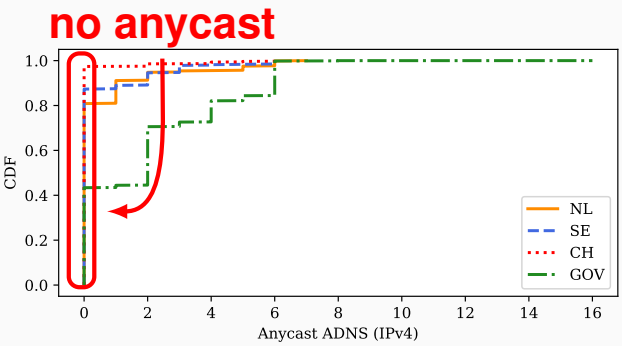
IP anycast adoption on e-gov

- Good: 58% US `.gov` domains have anycast
- Not so good: very few Swiss e-gov domains have anycast
- Sweden and the Netherlands have around 20% of anycast servers



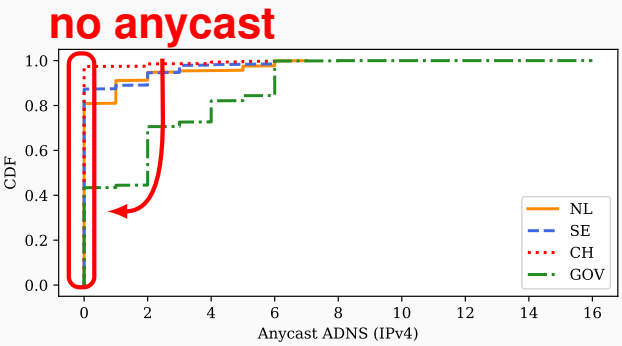
IP anycast adoption on e-gov

- Good: 58% US `.gov` domains have anycast
- Not so good: very few Swiss e-gov domains have anycast
- Sweden and the Netherlands have around 20% of anycast servers



IP anycast adoption on e-gov

- Good: 58% US `.gov` domains have anycast
- Not so good: very few Swiss e-gov domains have anycast
- Sweden and the Netherlands have around 20% of anycast servers



DNS time-to-live (TTL)

- TTLs control how long DNS records should stay in resolver's cache
- Last resort when everything else fails (Moura18b)
- Current recommendations: use at least a couple of hours TTL

Source: Unsplash

DNS time-to-live (TTL)

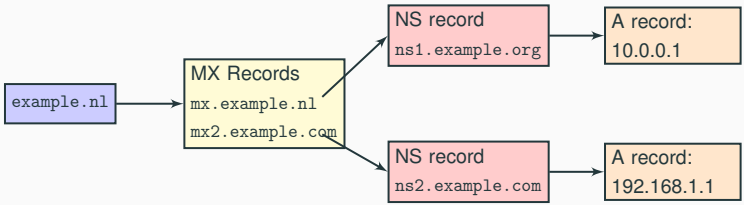
	Netherlands 	Sweden 	Switzerland 	United States 
NS TTL				
Median	10800	3600	3600	10800
A/AAAA TTL				
Median	3047	3600	3600	28800

E-gov e-mail DNS

- So far we've looked into E-gov DNS for **web**
- E-mail is also an important e-gov sevice
- Now we turn to measure the resilience of e-gov DNS for e-mail

Erasmus of Rotterdam writing some mail (1523)
src: Wikipedia

E-gov e-mail DNS



- For e-mail we first retrieve their MX records, and proceed as previous

E-gov e-mail DNS

Country	Netherlands .nl 	Sweden .se 	Switzerland .ch 	United States .gov 
e-gov domains (SLD)	602	614	3971	7972
Outlook	164 (39%)	205 (37%)	425 (22.1%)	2243 (41%)

- E-gov E-mail uses mosly Microsoft regardless of the country
- Why? Maybe they seek for more traditional solutions
  - more in the paper[PDF]

Recommendations for e-gov DNS

- **Diversify:** more DNS providers, more NS records, more prefixes, different TLDs for NS records
- **Deploy** anycast for more robust services
- **Reconsider** low TTL values

Robust (1900 years old) infrastructure in Segovia, Spain. Src: Wikipedia

Conclusions

- Many e-gov domains are not following the recommendation for robust services
- This creates unnecessary risk
- We hope our findings prompt the responsible operators to improve the redundancy and resilience of e-gov DNS

Robust (1900 years old) infrastructure in Rome, Italy. Src: Wikipedia

Full paper: Sommese22a

(Side: Free NTS servers at https://time.nl)