Tussle in Domain Namespace

Willem Toorop

NLNETLABS

donderdag 2 mei 2019

snow

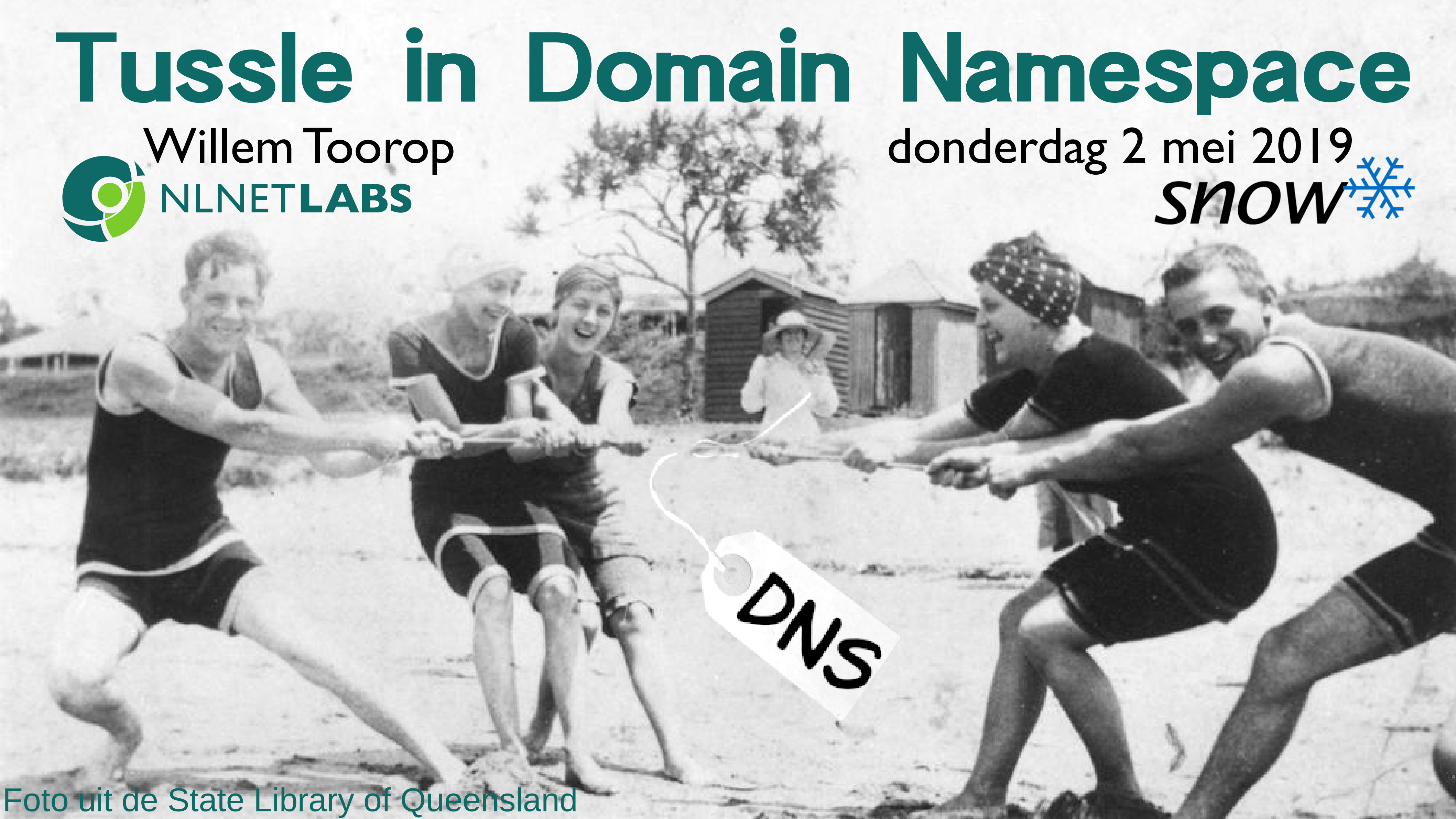
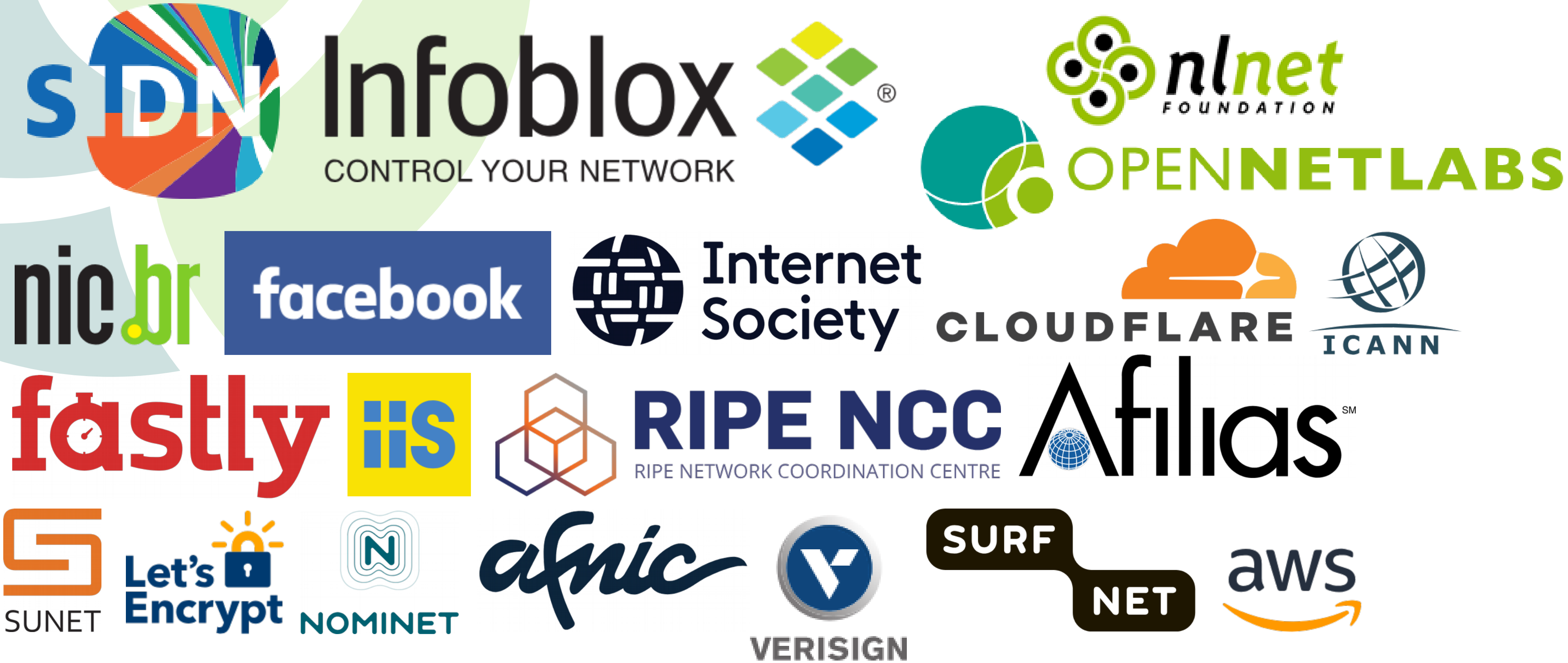


Foto uit de State Library of Queensland

Wat is/Wat doet NLNETLABS

- Non-profit stichting – sinds 1999 – subsidies & donaties



Wat is/Wat doet NLNETLABS

- Missie:

  Leveren van globaal erkende innovaties en expertise in die technologieeën die een netwerk van netwerken maken tot een Open Internet voor allen.

- Doel:
  - *Ontwikkelen van Open Source software en Open Standaarden ten behoeve van het Internet.*

Wat is/Wat doet NLNETLABS

- Doel:
  - *Ontwikkelen van* ***Open Source software*** *en* ***Open Standaarden*** *ten behoeve van het Internet.*

NSD unbound getdns

Open DNSSEC ROUTINATOR Krill

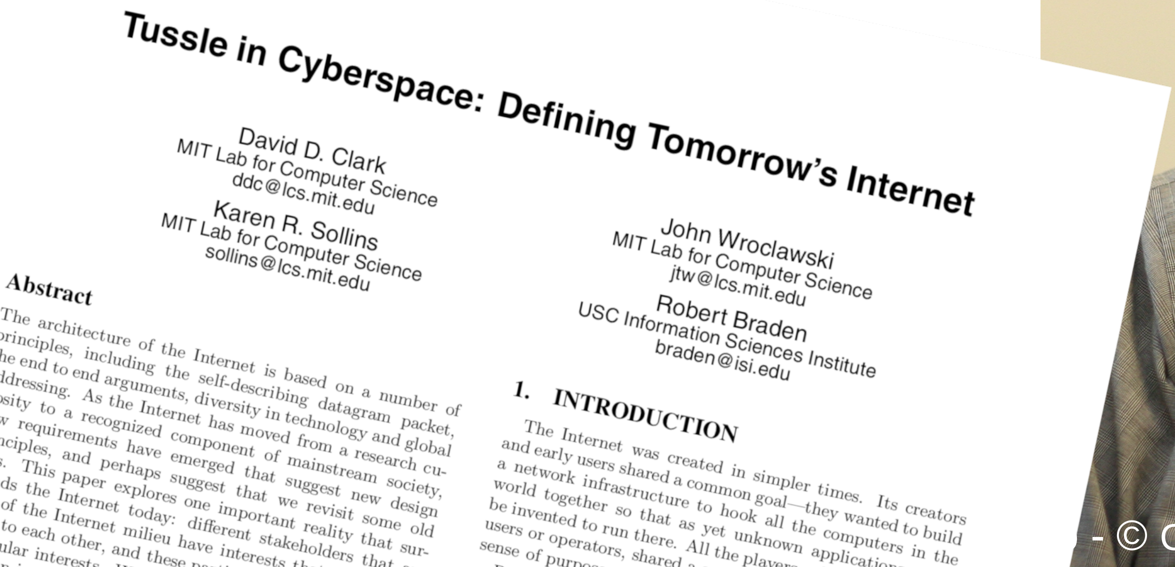
- ldns
- Net::DNS
- Net::DNS::SEC

Research – Internet metingen – Sudenten projecten

Tussle

bakkeleien ; plukharen

https://www.mijnwoordenboek.nl/vertaal/NL/EN/tussle



Tussle in Cyberspace: Defining Tomorrow's Internet

David D. Clark
MIT Lab for Computer Science
ddc@lcs.mit.edu

Karen R. Sollins
MIT Lab for Computer Science
sollins@lcs.mit.edu

John Wroclawski
MIT Lab for Computer Science
jtw@lcs.mit.edu

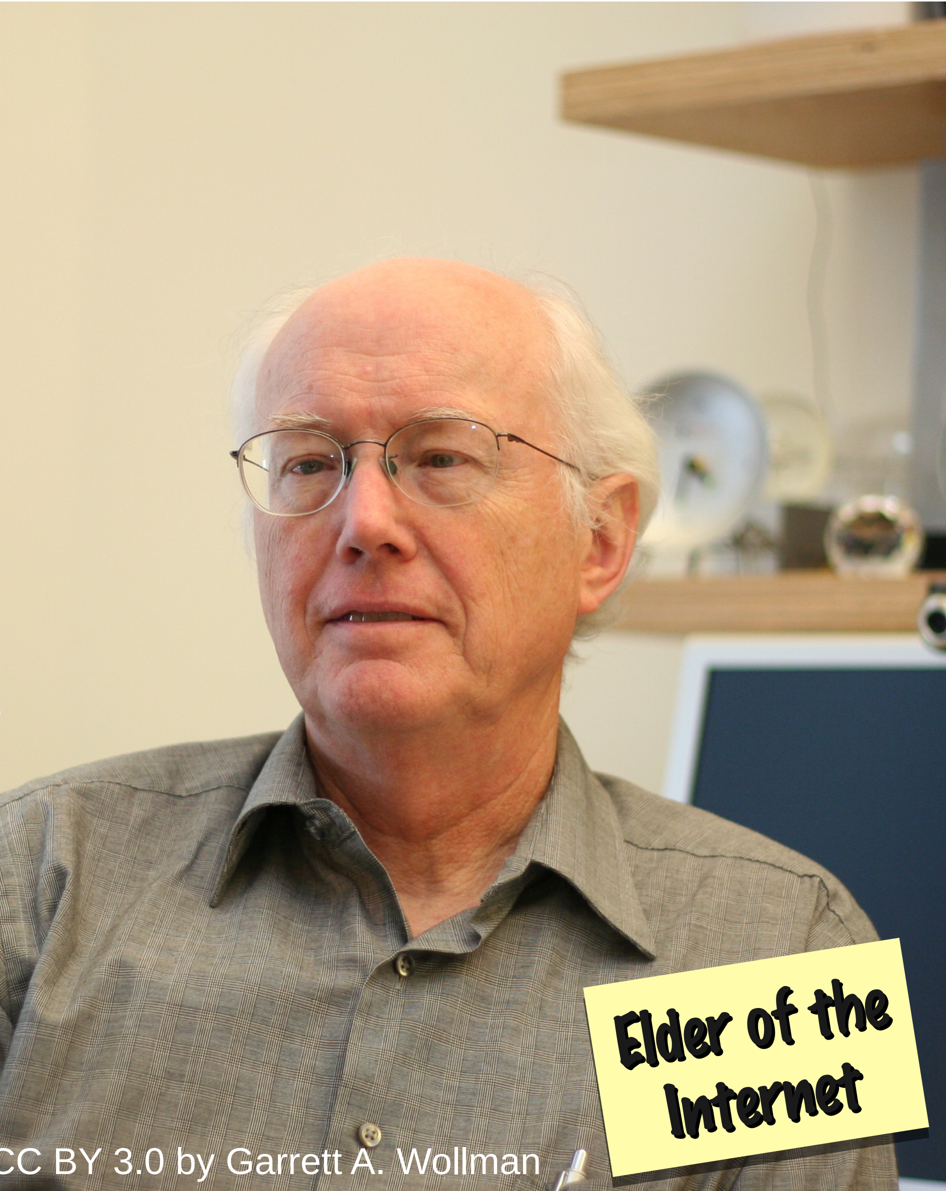
Robert Braden
USC Information Sciences Institute
braden@isi.edu

Abstract

The architecture of the Internet is based on a number of rinciples, including the self-describing datagram packet, he end to end arguments, diversity in technology and global ldressing. As the Internet has moved from a research cuosity to a recognized component of mainstream society, w requirements have emerged that suggest new design nciples, and perhaps suggest that we revisit some old s. This paper explores one important reality that surds the Internet today: different stakeholders that are of the Internet milieu have interests that to each other, and these ular interests

1. INTRODUCTION

The Internet was created in simpler times. Its creators and early users shared a common goal—they wanted to build a network infrastructure to hook all the computers in the world together so that as yet unknown applications be invented to run there. All the players users or operators, shared sense of purpose

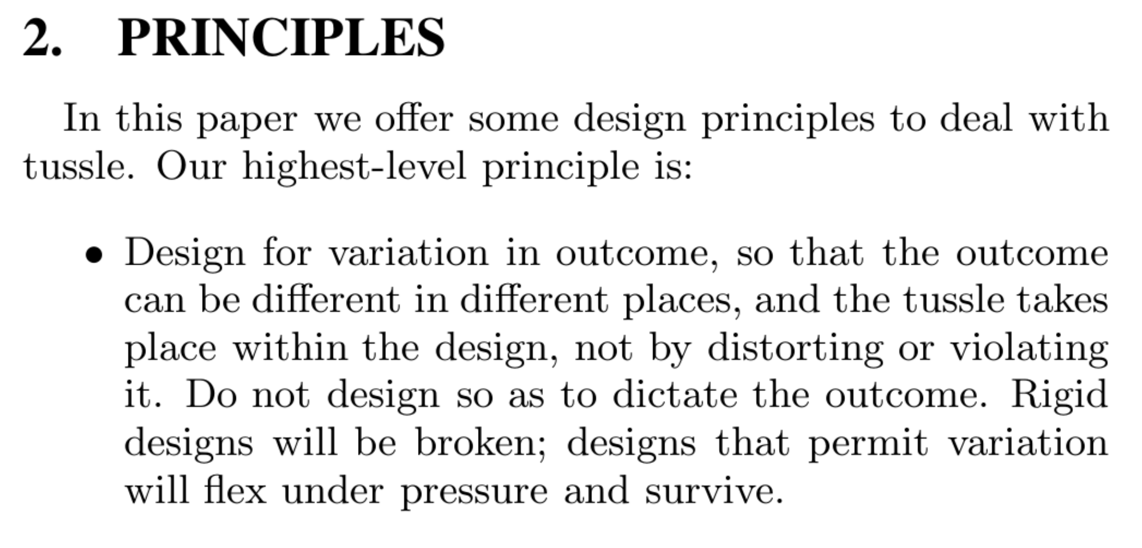


- © CC BY 3.0 by Garrett A. Wollman

Tussle

bakkeleien ; plukharen

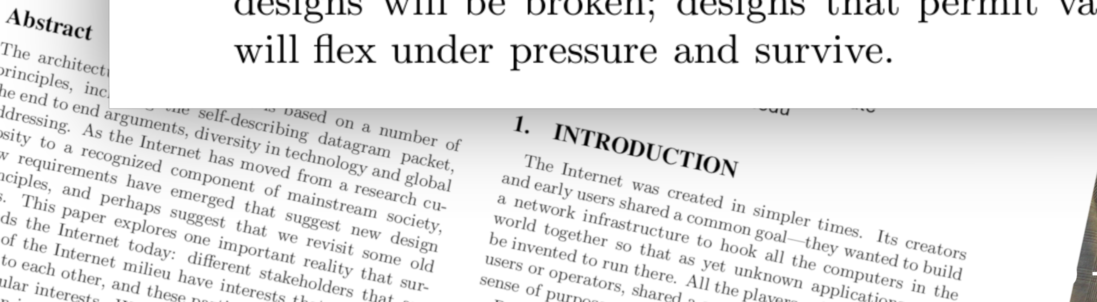
https://www.mijnwoordenboek.nl/vertaal/NL/EN/tussle



2. PRINCIPLES

In this paper we offer some design principles to deal with tussle. Our highest-level principle is:

- Design for variation in outcome, so that the outcome can be different in different places, and the tussle takes place within the design, not by distorting or violating it. Do not design so as to dictate the outcome. Rigid designs will be broken; designs that permit variation will flex under pressure and survive.



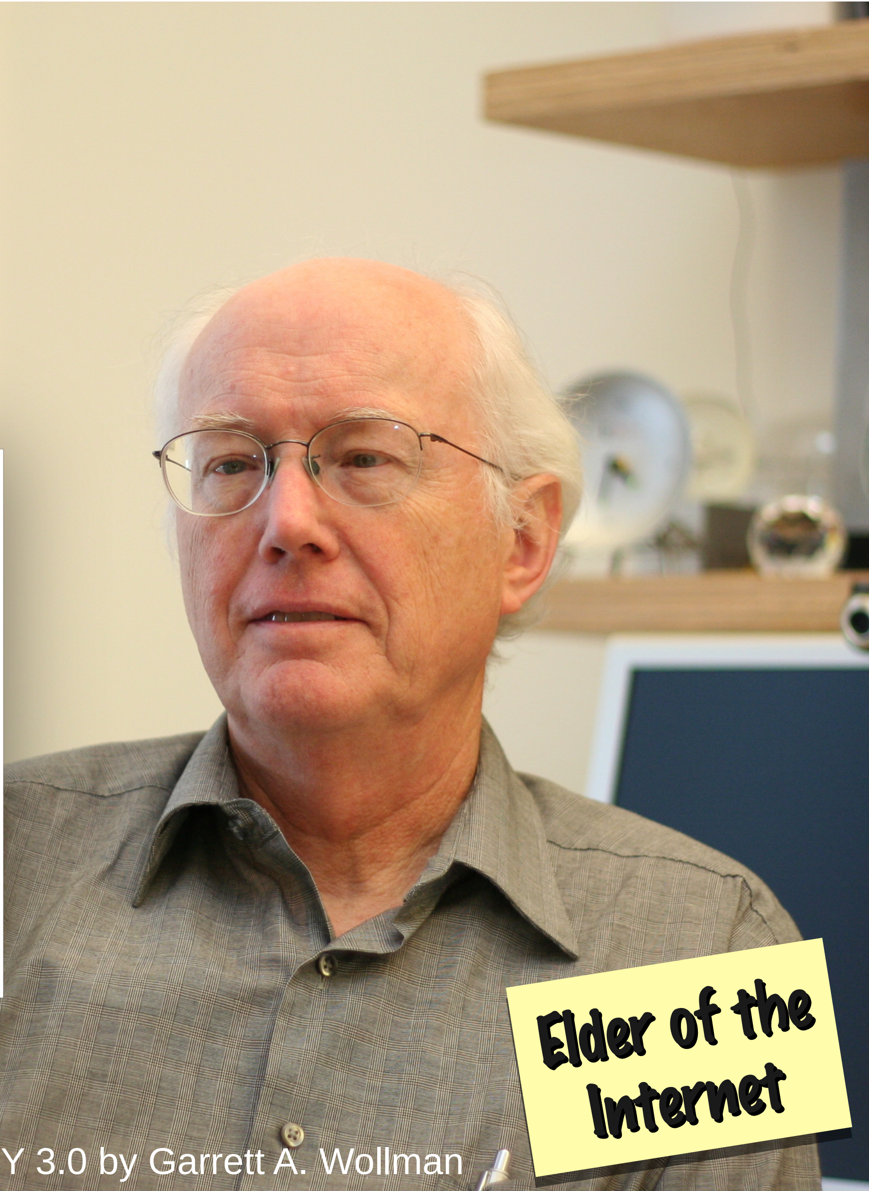
Abstract

The architectu
principles, inc
he end to end arguments, diversity in technology and global
ddressing. As the Internet has moved from a research cu-
osity to a recognized component of mainstream society,
w requirements have emerged that suggest new design
nciples, and perhaps suggest that we revisit some old
. This paper explores one important reality that sur-
ds the Internet today: different stakeholders that
of the Internet milieu have interests that
to each other, and these
ular interests

self-describing datagram packet, based on a number of

1. INTRODUCTION

The Internet was created in simpler times. Its creators and early users shared a common goal—they wanted to build a network infrastructure to hook all the computers in the world together so that as yet unknown applications could be invented to run there. All the players
users or operators, shared
sense of purpos



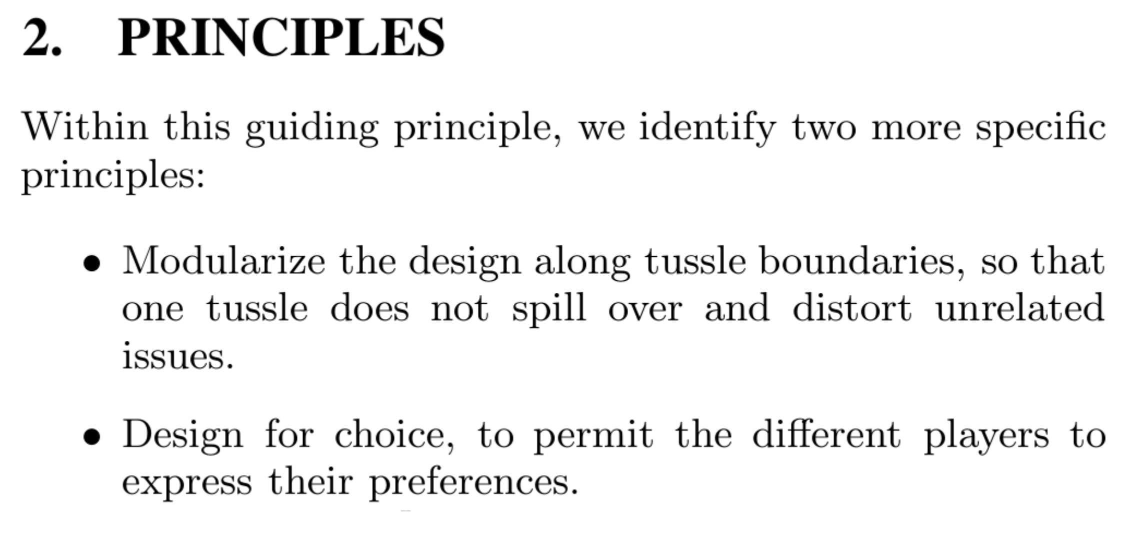
- © CC BY 3.0 by Garrett A. Wollman

Elder of the Internet

Tussle

bakkeleien ; plukharen

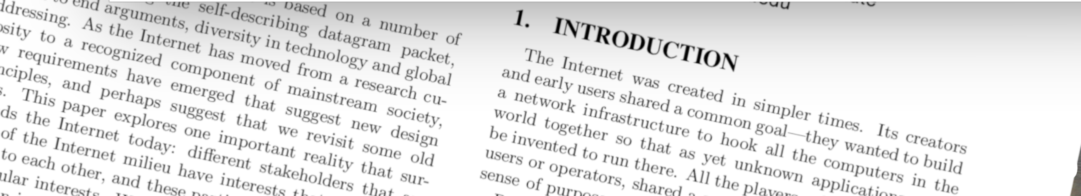
https://www.mijnwoordenboek.nl/vertaal/NL/EN/tussle



2. PRINCIPLES

Within this guiding principle, we identify two more specific principles:

- Modularize the design along tussle boundaries, so that one tussle does not spill over and distort unrelated issues.
- Design for choice, to permit the different players to express their preferences.



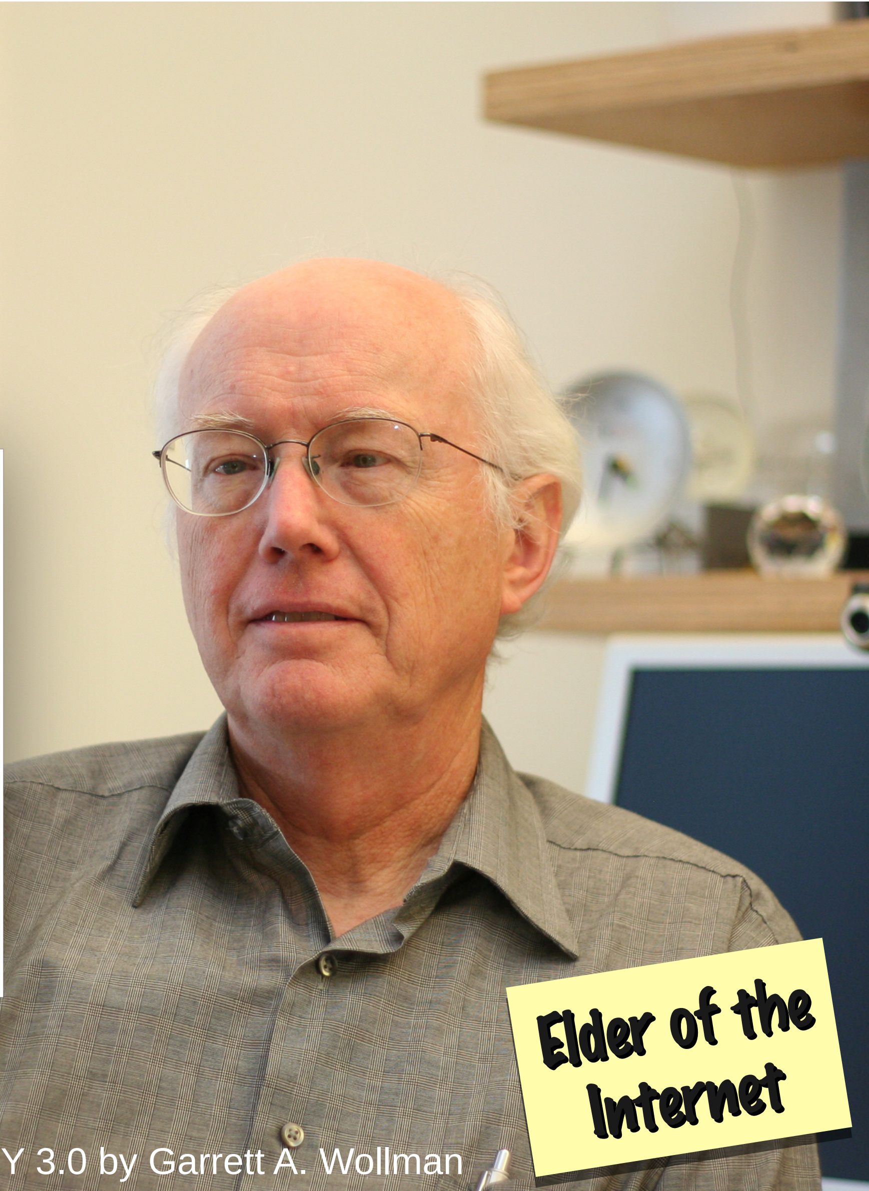
Abstract

The architectu
principles, inc
he end to end arguments, diversity in technology and global
ddressing. As the Internet has moved from a research cu-
osity to a recognized component of mainstream society,
w requirements have emerged that suggest new design
nciples, and perhaps suggest that we revisit some old
s. This paper explores one important reality that sur-
ds the Internet today: different stakeholders that
of the Internet milieu have interests that
to each other, and these partic
ular interests

self-describing datagram packet, is based on a number of

1. INTRODUCTION

The Internet was created in simpler times. Its creators and early users shared a common goal—they wanted to build a network infrastructure to hook all the computers in the world together so that as yet unknown applications could be invented to run there. All the players
users or operators, shared a
sense of purpos



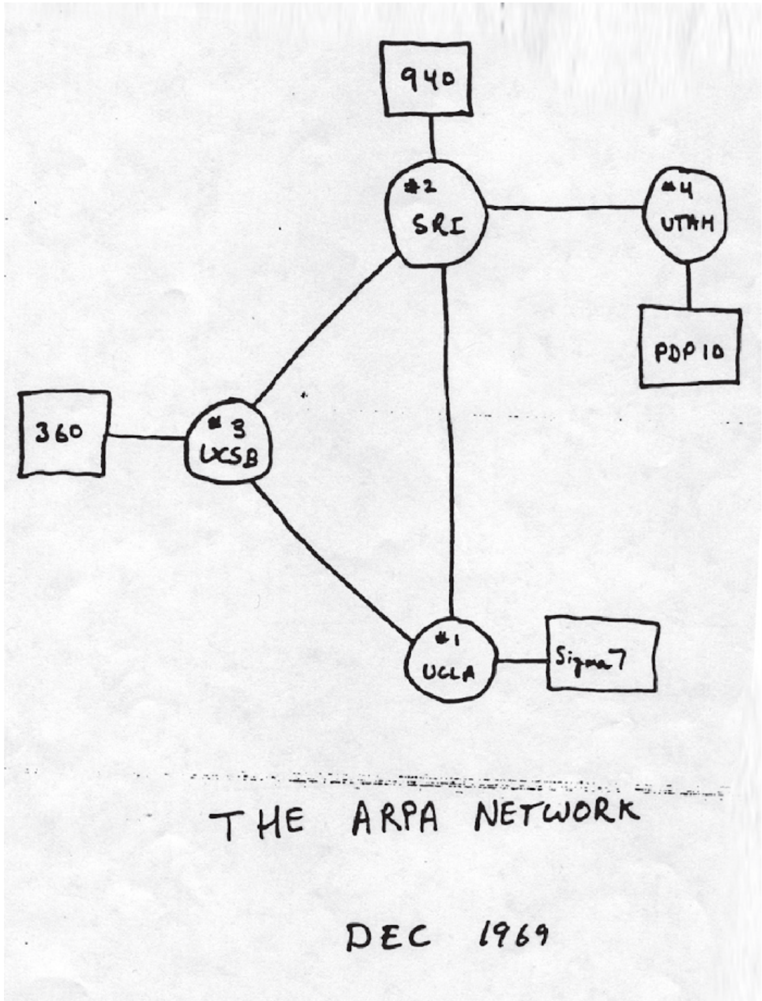
- © CC BY 3.0 by Garrett A. Wollman

Elder of the Internet

Tussle Spaces

50 EURO
T
R
U
S
T
Internet
Information Sciences Institute
braden@isi.edu
Abstract
1. INTRODUCTION
The Internet was created in simpler times. Its creators and early users shared a common goal—they wanted to build a network infrastructure to hook all the computers in the world together so that as yet unknown applications could be invented to run there.

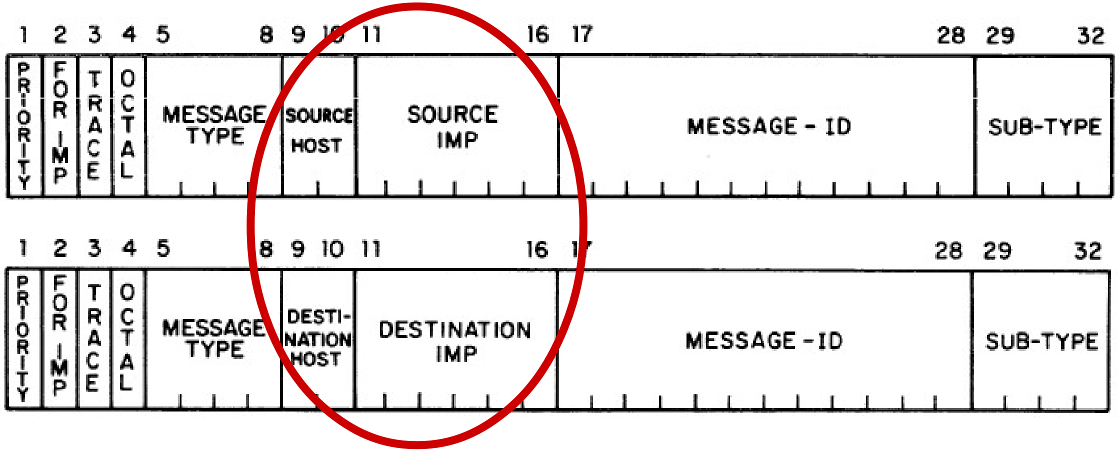
Namespace op het internet



THE ARPA NETWORK

DEC 1969

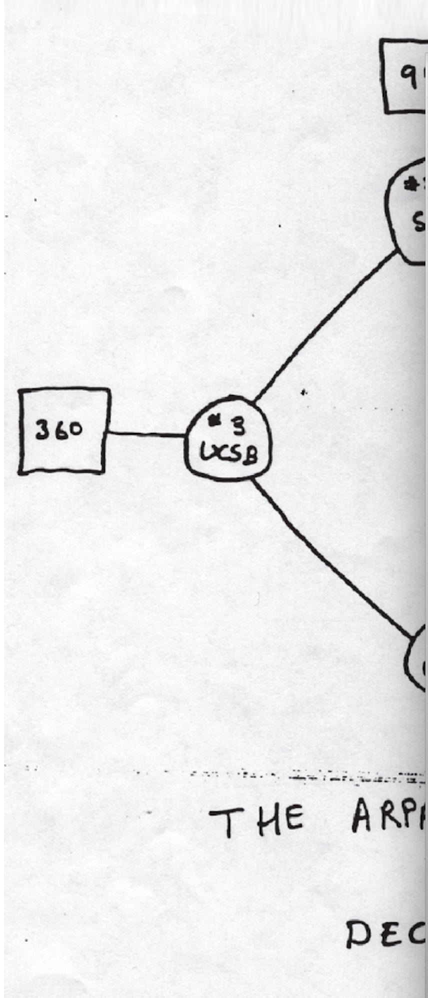
NCP (Network Control Program)

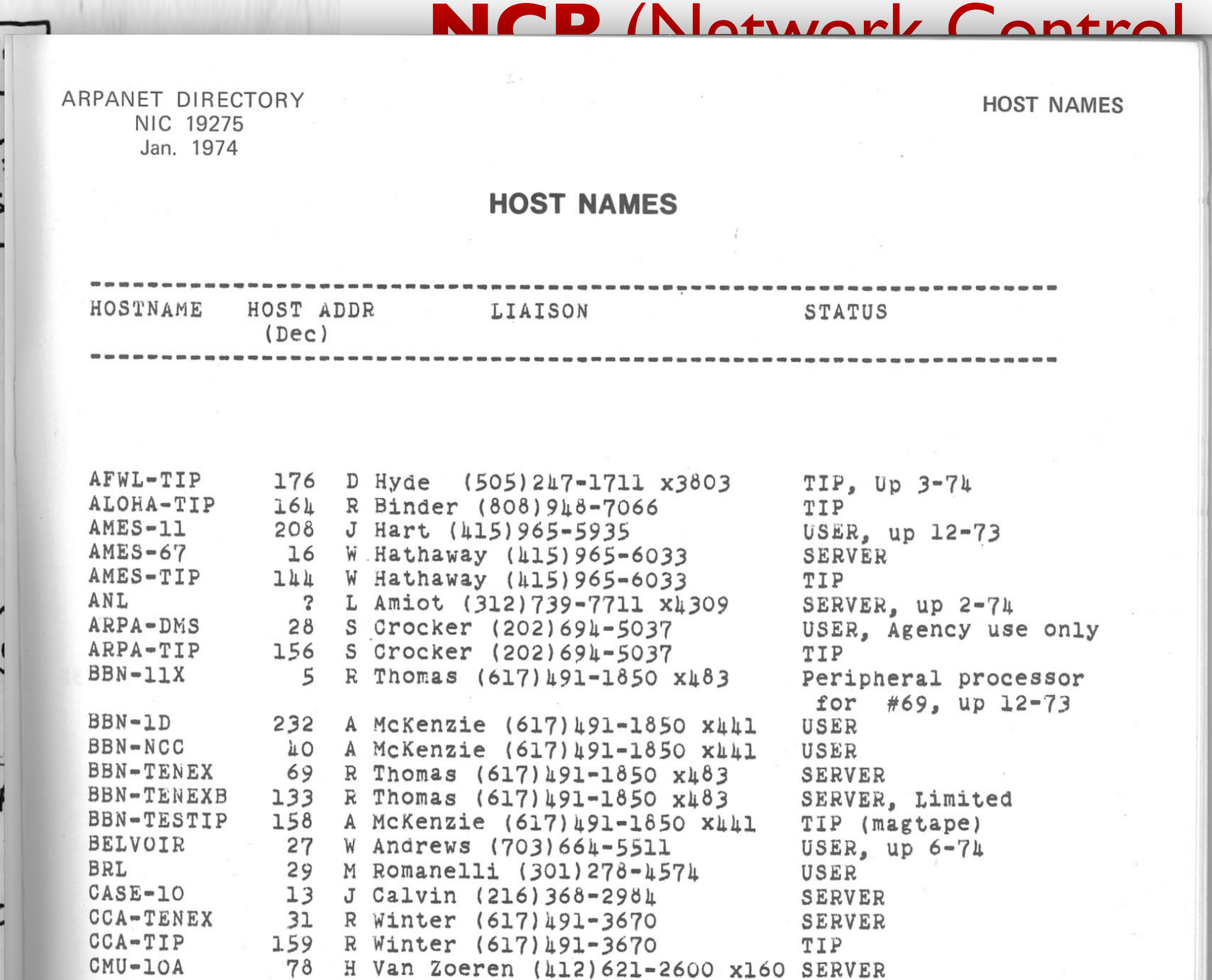


- December 1973
  `HOSTS.TXT` (RFC 606)

Namespace op het internet

NCP (Network Control Program)



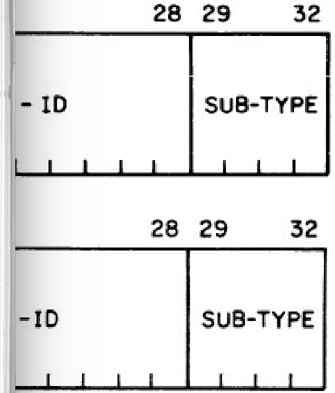


ARPANET DIRECTORY
NIC 19275
Jan. 1974

HOST NAMES

HOST NAMES

HOSTNAME	HOST ADDR (Dec)	LIAISON	STATUS
AFWL-TIP	176	D Hyde (505)247-1711 x3803	TIP, Up 3-74
ALOHA-TIP	164	R Binder (808)948-7066	TIP
AMES-11	208	J Hart (415)965-5935	USER, up 12-73
AMES-67	16	W Hathaway (415)965-6033	SERVER
AMES-TIP	144	W Hathaway (415)965-6033	TIP
ANL	?	L Amiot (312)739-7711 x4309	SERVER, up 2-74
ARPA-DMS	28	S Crocker (202)694-5037	USER, Agency use only
ARPA-TIP	156	S Crocker (202)694-5037	TIP
BBN-11X	5	R Thomas (617)491-1850 x483	Peripheral processor for #69, up 12-73
BBN-1D	232	A McKenzie (617)491-1850 x441	USER
BBN-NCC	40	A McKenzie (617)491-1850 x441	USER
BBN-TENEX	69	R Thomas (617)491-1850 x483	SERVER
BBN-TENEXB	133	R Thomas (617)491-1850 x483	SERVER, Limited
BBN-TESTIP	158	A McKenzie (617)491-1850 x441	TIP (magtape)
BELVOIR	27	W Andrews (703)664-5511	USER, up 6-74
BRL	29	M Romanelli (301)278-4574	USER
CASE-10	13	J Calvin (216)368-2984	SERVER
CCA-TENEX	31	R Winter (617)491-3670	SERVER
CCA-TIP	159	R Winter (617)491-3670	TIP
CMU-10A	78	H Van Zoeren (412)621-2600 x160	SERVER



C 606)

Namespace op het internet

Paul Mockapetris - © CC BY-SA 4.0 by Oscured

- 1 januari 1983 NCP → IP/TCP

  flagday

- max 256 → max 4.294.967.296 hosts

- november 1983 DNS (RFC 882)

  __D__omain __N__ame __S__ystem

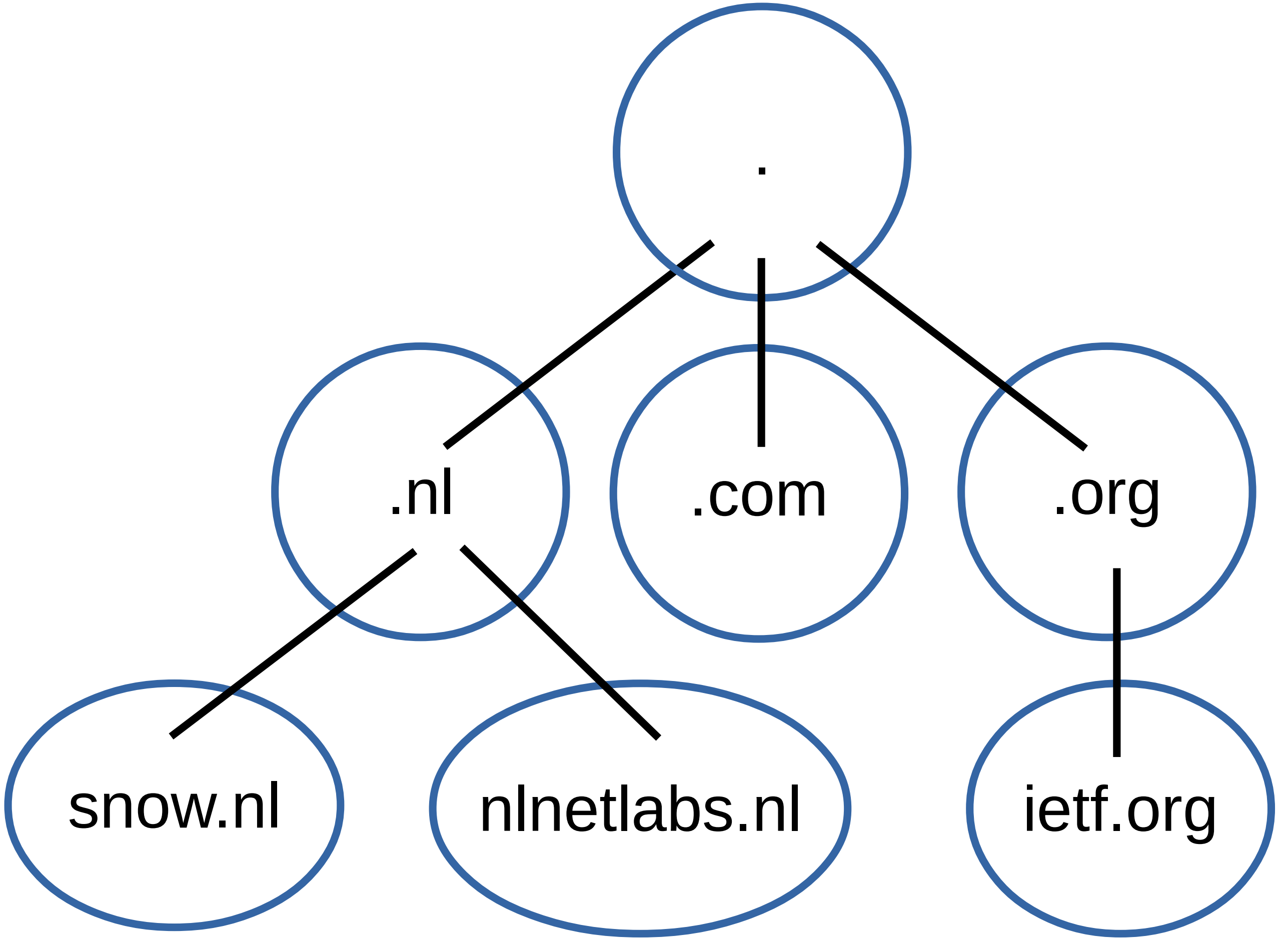
- november 1987 STD13

  (RFC 1034 & RFC 1035)

- Niet alleen IP adressen (ook mail)

Eerste implementatie: https://www.hactrn.net/hacks/jeeves/

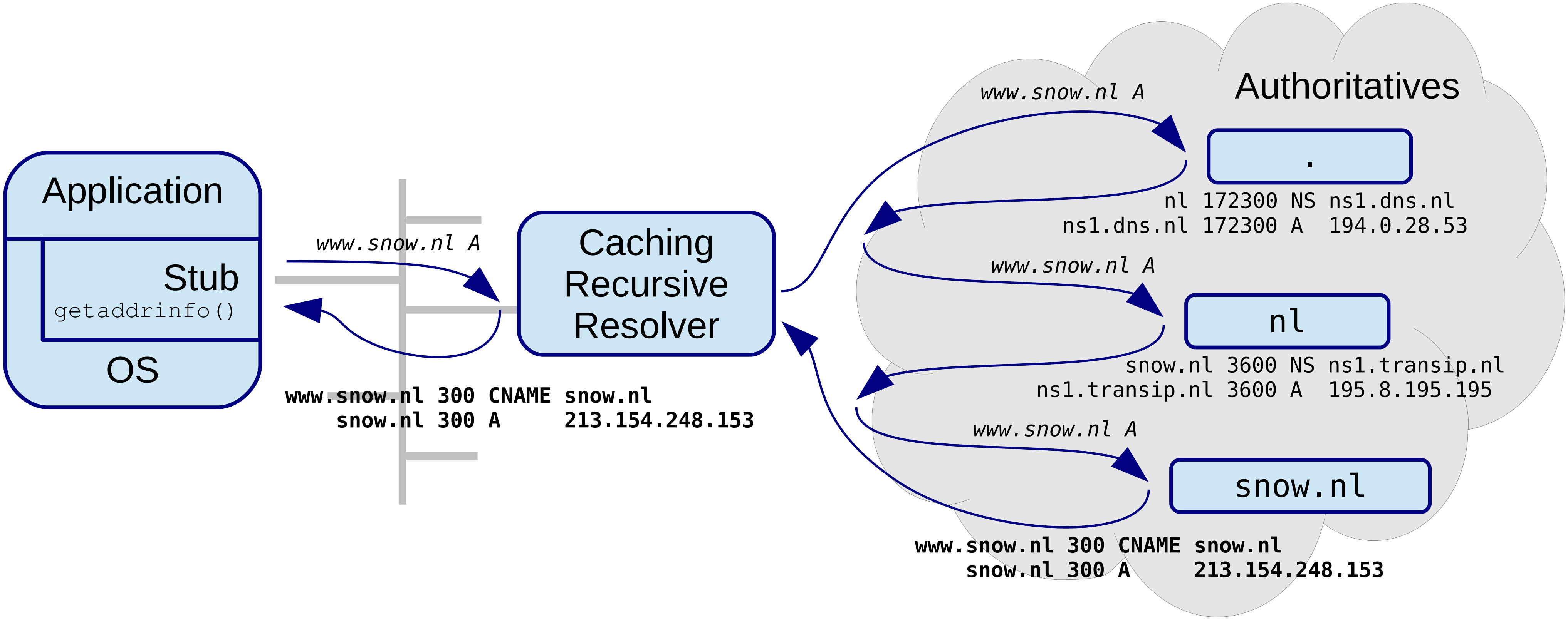
Domain Namespace – schaal



- 13 root servers
  in 12 organisaties

- 1532 tlds
- .com 141.000.000
  .nl 5.000.000

Domain Name System - schaal



```
www.snow.nl 300 CNAME snow.nl
    snow.nl 300 A     213.154.248.153
```

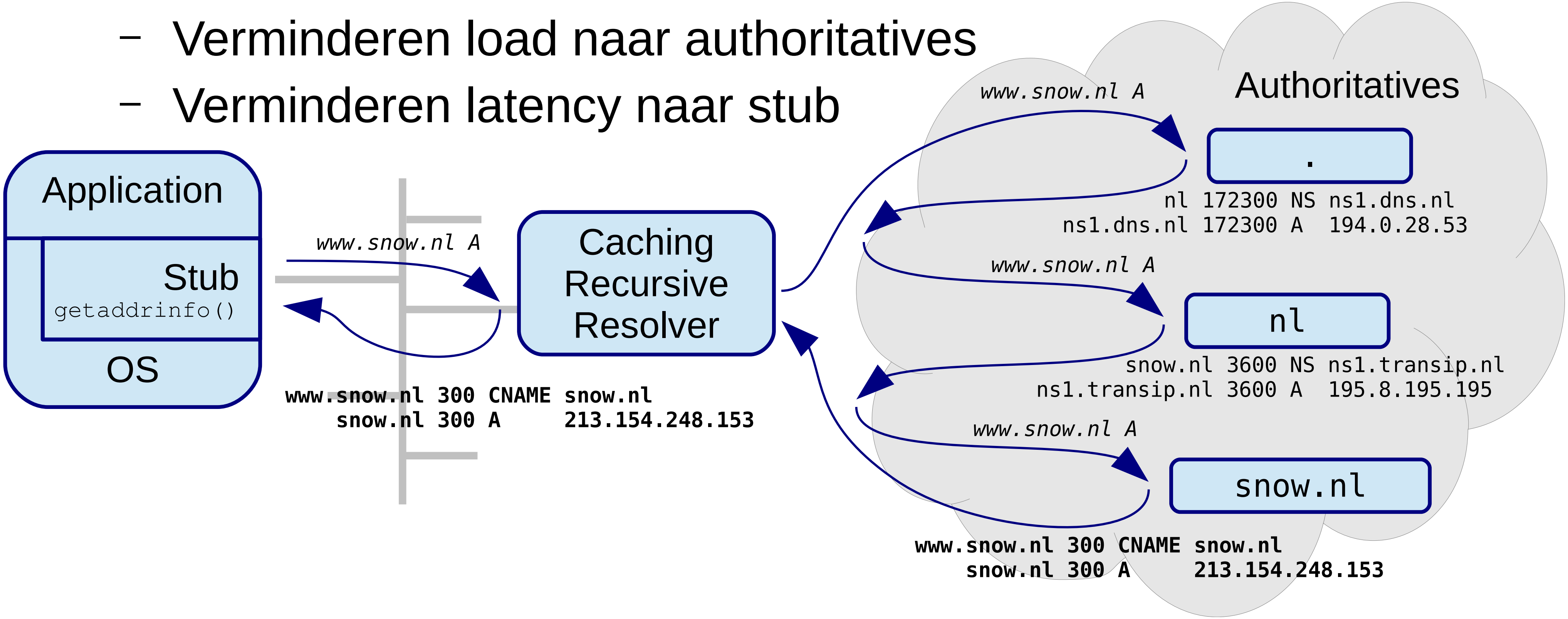
```
         nl 172300 NS ns1.dns.nl
ns1.dns.nl 172300 A  194.0.28.53
```

```
     snow.nl 3600 NS ns1.transip.nl
ns1.transip.nl 3600 A  195.8.195.195
```

```
www.snow.nl 300 CNAME snow.nl
    snow.nl 300 A     213.154.248.153
```

Domain Name System – schaal

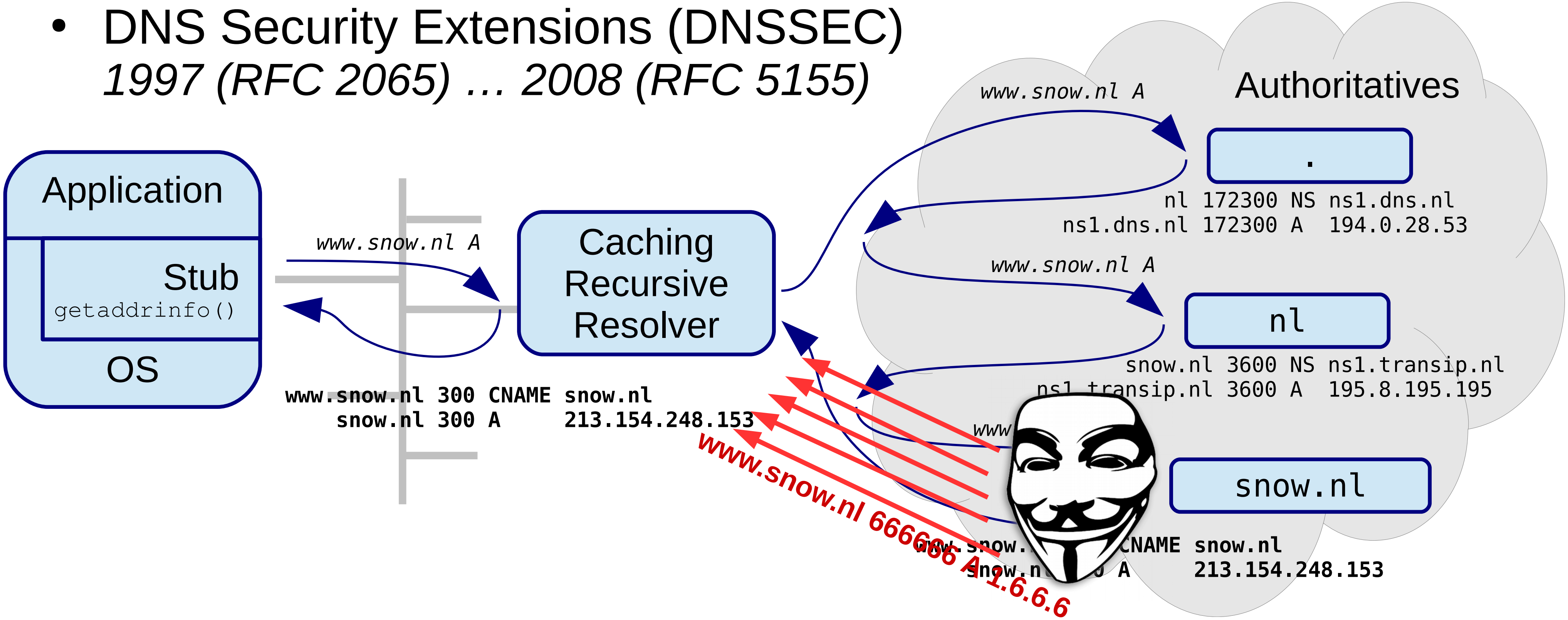
- *UDP* = Geen State op authoritatives
- *Caching* Recursive Resolvers:
  - Verminderen load naar authoritatives
  - Verminderen latency naar stub



Application
Stub
getaddrinfo()
OS
www.snow.nl A
Caching Recursive Resolver
www.snow.nl 300 CNAME snow.nl
snow.nl 300 A 213.154.248.153
Authoritatives
www.snow.nl A
.
nl 172300 NS ns1.dns.nl
ns1.dns.nl 172300 A 194.0.28.53
www.snow.nl A
nl
snow.nl 3600 NS ns1.transip.nl
ns1.transip.nl 3600 A 195.8.195.195
www.snow.nl A
snow.nl
www.snow.nl 300 CNAME snow.nl
snow.nl 300 A 213.154.248.153

Domain Name System – security

- Random bits (65.536 query ID * source ports) & ***Caching*** als security mechanisme
- DNS Security Extensions (DNSSEC)
  1997 (RFC 2065) … 2008 (RFC 5155)



```
www.snow.nl 300 CNAME snow.nl
    snow.nl 300 A     213.154.248.153
```

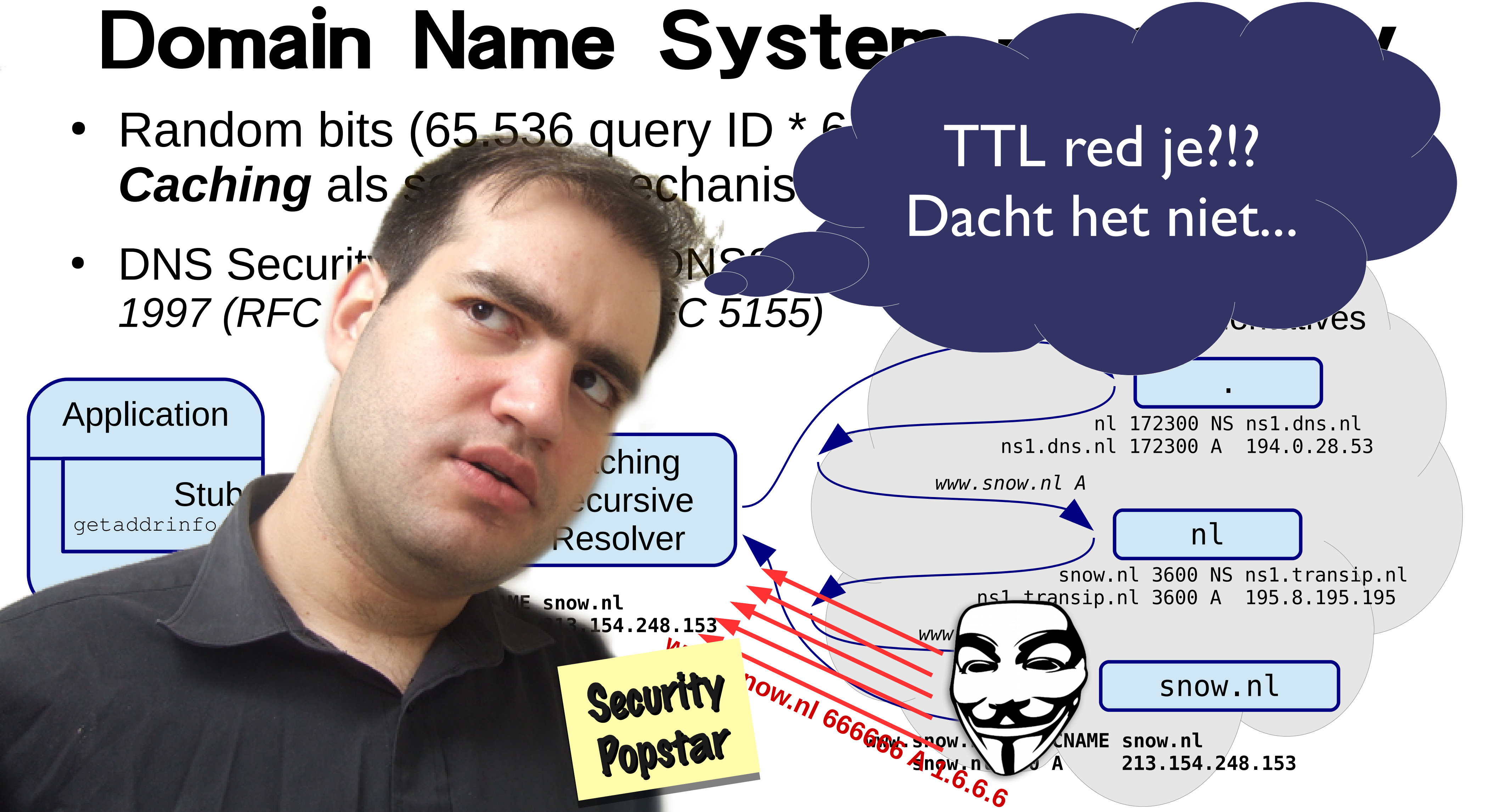
```
nl 172300 NS ns1.dns.nl
ns1.dns.nl 172300 A  194.0.28.53
```

```
snow.nl 3600 NS ns1.transip.nl
ns1.transip.nl 3600 A  195.8.195.195
```

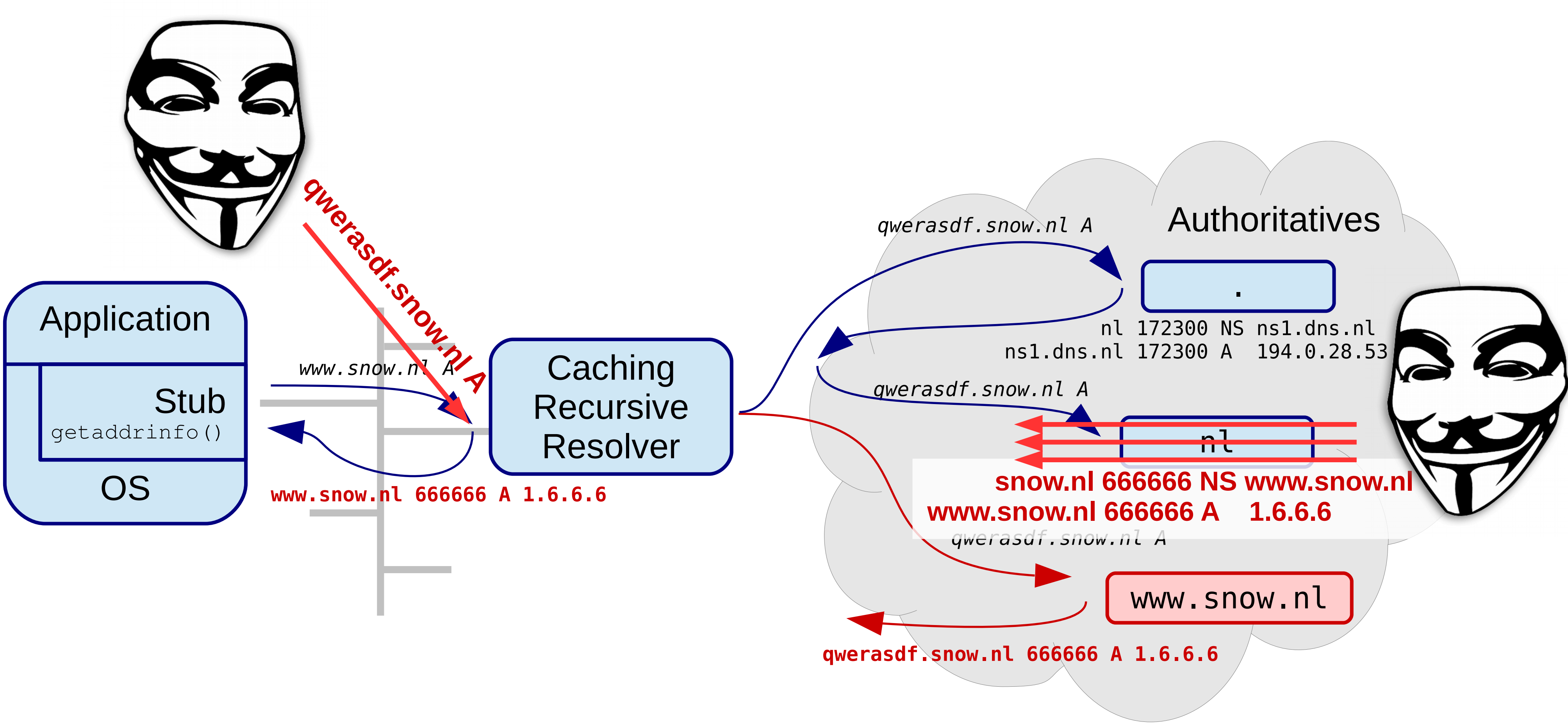
```
www.snow.     CNAME snow.nl
    snow.n    0 A     213.154.248.153
```

Domain Name System

- Random bits (65.536 query ID * 6
  Caching als s echanis
- DNS Securit DNS
  1997 (RFC C 5155)



Domain Name System - security



qwerasdf.snow.nl A

Application

Stub

getaddrinfo()

OS

www.snow.nl A

www.snow.nl 666666 A 1.6.6.6

Caching Recursive Resolver

Authoritatives

qwerasdf.snow.nl A

.

nl 172300 NS ns1.dns.nl
ns1.dns.nl 172300 A 194.0.28.53

qwerasdf.snow.nl A

nl

snow.nl 666666 NS www.snow.nl
www.snow.nl 666666 A 1.6.6.6

qwerasdf.snow.nl A

www.snow.nl

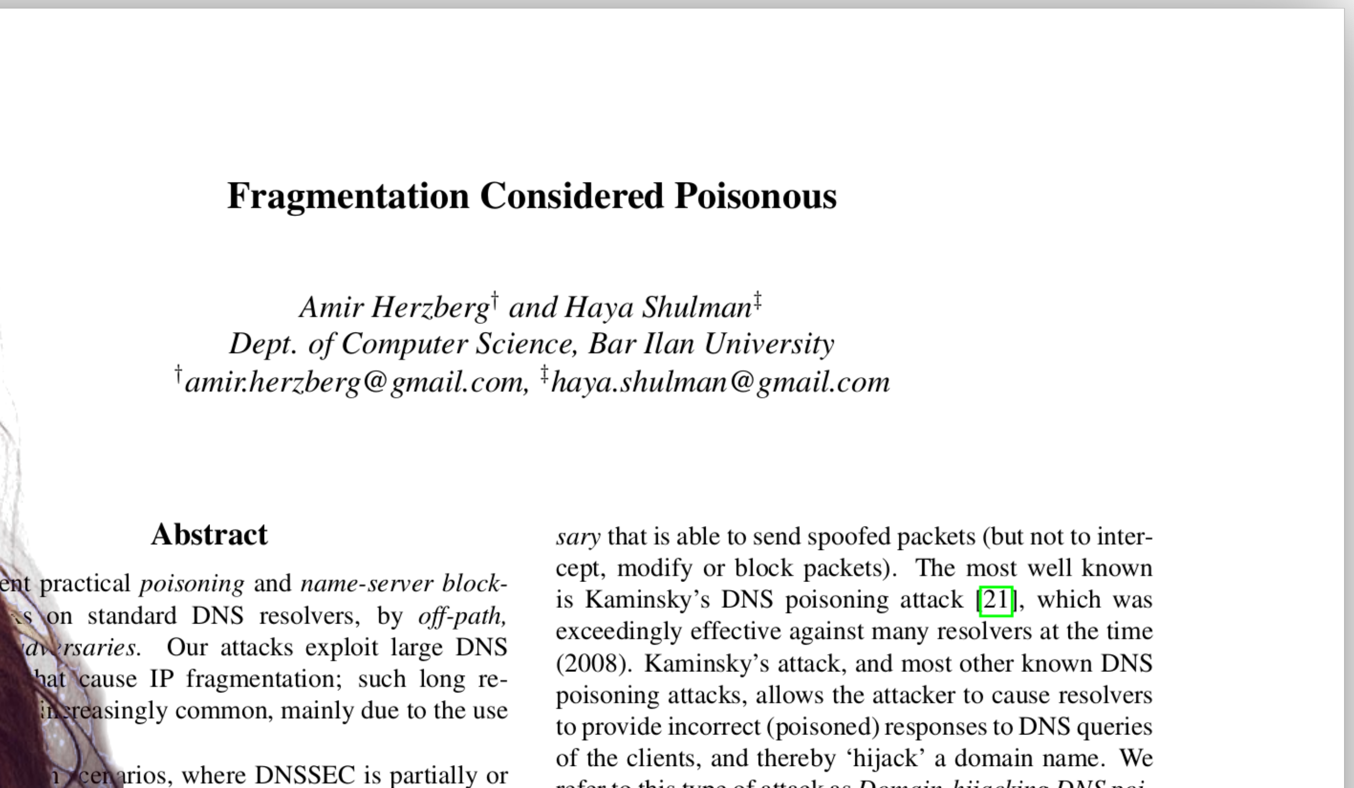
qwerasdf.snow.nl 666666 A 1.6.6.6

Domain Name System - security

# Bits	50% kans	5% kans	Methode
16	10 seconden	1 seconde	Query ID
26	2,8 uur	17 minuten	1024 source poorten
34	28 dagen	2,8 dagen	Alle source poorten + 2 bits server selectie
44	288444 dagen	2844,4 dagen	0x20 hack

Domain Name System - security

- Hulp bij spoofen van DNS antwoorden



Fragmentation Considered Poisonous

Amir Herzberg[†] *and Haya Shulman*[‡]
Dept. of Computer Science, Bar Ilan University
[†]*amir.herzberg@gmail.com,* [‡]*haya.shulman@gmail.com*

Abstract

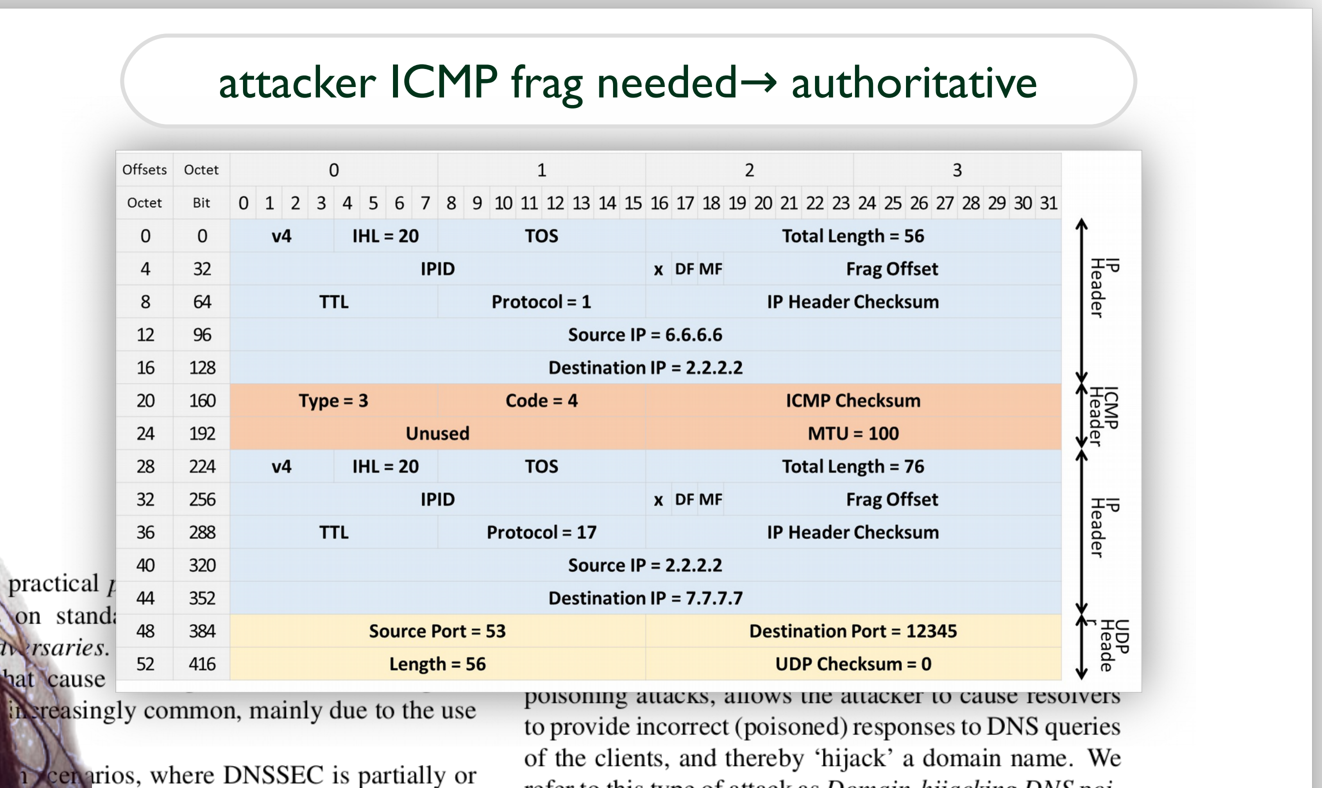
ent practical *poisoning* and *name-server block-*
s on standard DNS resolvers, by *off-path,*
adversaries. Our attacks exploit large DNS
hat cause IP fragmentation; such long re-
increasingly common, mainly due to the use

n scenarios, where DNSSEC is partially or

sary that is able to send spoofed packets (but not to intercept, modify or block packets). The most well known is Kaminsky's DNS poisoning attack [21], which was exceedingly effective against many resolvers at the time (2008). Kaminsky's attack, and most other known DNS poisoning attacks, allows the attacker to cause resolvers to provide incorrect (poisoned) responses to DNS queries of the clients, and thereby 'hijack' a domain name. We refer to this type of attack as *Domain hijacking DNS poi-*

Domain Name System - security

- Hulp bij spoofen van DNS antwoorden



attacker ICMP frag needed→ authoritative

Offsets	Octet	0								1								2								3								
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
0	0	v4				IHL = 20				TOS								Total Length = 56																IP Header
4	32	IPID																x	DF	MF	Frag Offset													
8	64	TTL								Protocol = 1								IP Header Checksum																
12	96	Source IP = 6.6.6.6																																
16	128	Destination IP = 2.2.2.2																																
20	160	Type = 3								Code = 4								ICMP Checksum																ICMP Header
24	192	Unused																MTU = 100																
28	224	v4				IHL = 20				TOS								Total Length = 76																IP Header
32	256	IPID																x	DF	MF	Frag Offset													
36	288	TTL								Protocol = 17								IP Header Checksum																
40	320	Source IP = 2.2.2.2																																
44	352	Destination IP = 7.7.7.7																																
48	384	Source Port = 53																Destination Port = 12345																UDP Header
52	416	Length = 56																UDP Checksum = 0																

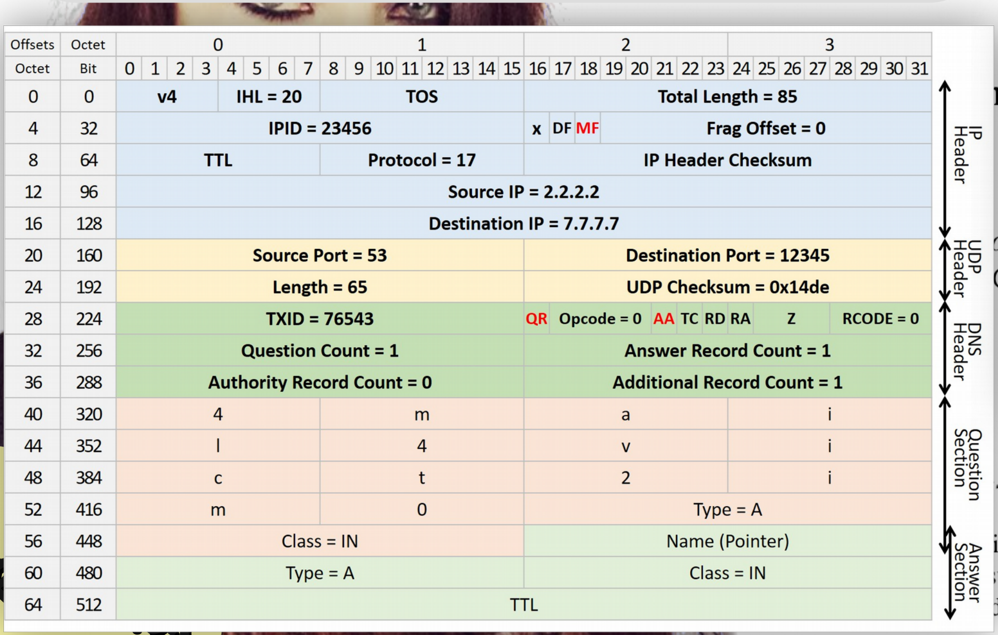
ent practical p
s on standa
adversaries.
hat cause
increasingly common, mainly due to the use
n scenarios, where DNSSEC is partially or

poisoning attacks, allows the attacker to cause resolvers to provide incorrect (poisoned) responses to DNS queries of the clients, and thereby 'hijack' a domain name. We refer to this type of attack as *Domain-hijacking DNS poi*

Domain Name System - security

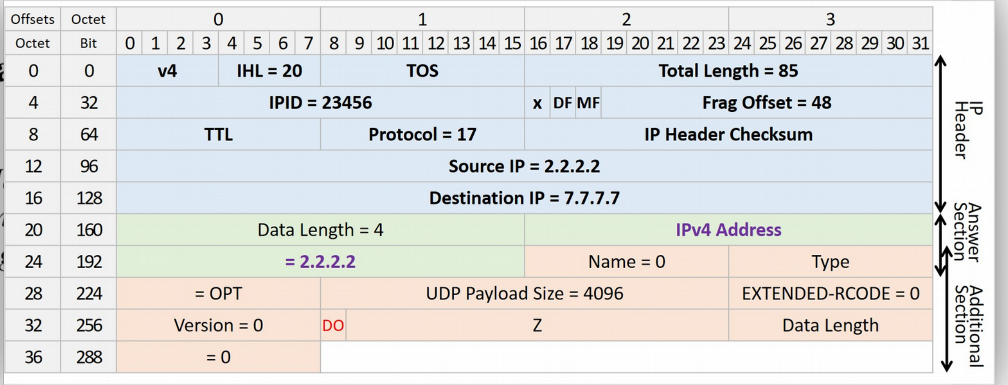
- Hulp bij spoofen van DNS antwoorden

1e fragment
authoritative → resolver



Offsets	Octet	0	1	2	3	
Octet	Bit	0 1 2 3 4 5 6 7	8 9 10 11 12 13 14 15	16 17 18 19 20 21 22 23	24 25 26 27 28 29 30 31	
0	0	v4 / IHL = 20	TOS	Total Length = 85		IP Header
4	32	IPID = 23456		x DF MF / Frag Offset = 0		
8	64	TTL	Protocol = 17	IP Header Checksum		
12	96	Source IP = 2.2.2.2				
16	128	Destination IP = 7.7.7.7				
20	160	Source Port = 53		Destination Port = 12345		UDP Header
24	192	Length = 65		UDP Checksum = 0x14de		
28	224	TXID = 76543		QR Opcode = 0 AA TC RD RA	Z RCODE = 0	DNS Header
32	256	Question Count = 1		Answer Record Count = 1		
36	288	Authority Record Count = 0		Additional Record Count = 1		
40	320	4	m	a	i	Question Section
44	352	l	4	v	i	
48	384	c	t	2	i	
52	416	m	0	Type = A		
56	448	Class = IN		Name (Pointer)		Answer Section
60	480	Type = A		Class = IN		
64	512	TTL				

2e fragment
attacker → resolver



Offsets	Octet	0	1	2	3	
Octet	Bit	0 1 2 3 4 5 6 7	8 9 10 11 12 13 14 15	16 17 18 19 20 21 22 23	24 25 26 27 28 29 30 31	
0	0	v4 / IHL = 20	TOS	Total Length = 85		IP Header
4	32	IPID = 23456		x DF MF / Frag Offset = 48		
8	64	TTL	Protocol = 17	IP Header Checksum		
12	96	Source IP = 2.2.2.2				
16	128	Destination IP = 7.7.7.7				
20	160	Data Length = 4		IPv4 Address		Answer Section
24	192	= 2.2.2.2		Name = 0	Type	Additional Section
28	224	= OPT	UDP Payload Size = 4096		EXTENDED-RCODE = 0	
32	256	Version = 0	DO Z		Data Length	
36	288	= 0				

server block-
by *off-path*,
it large DNS
uch long re-
due to the use
cenarios, where DNSSEC is partially or

sary that is able to send spoofed packets (but not to intercept, modify or block packets). The most well known is Kaminsky's DNS poisoning attack [21], which was exceedingly effective against many resolvers at the time (2008). Kaminsky's attack, and most other known DNS poisoning attacks, allows the attacker to cause resolvers to provide incorrect (poisoned) responses to DNS queries of the clients, and thereby 'hijack' a domain name. We

Domain Name System - security

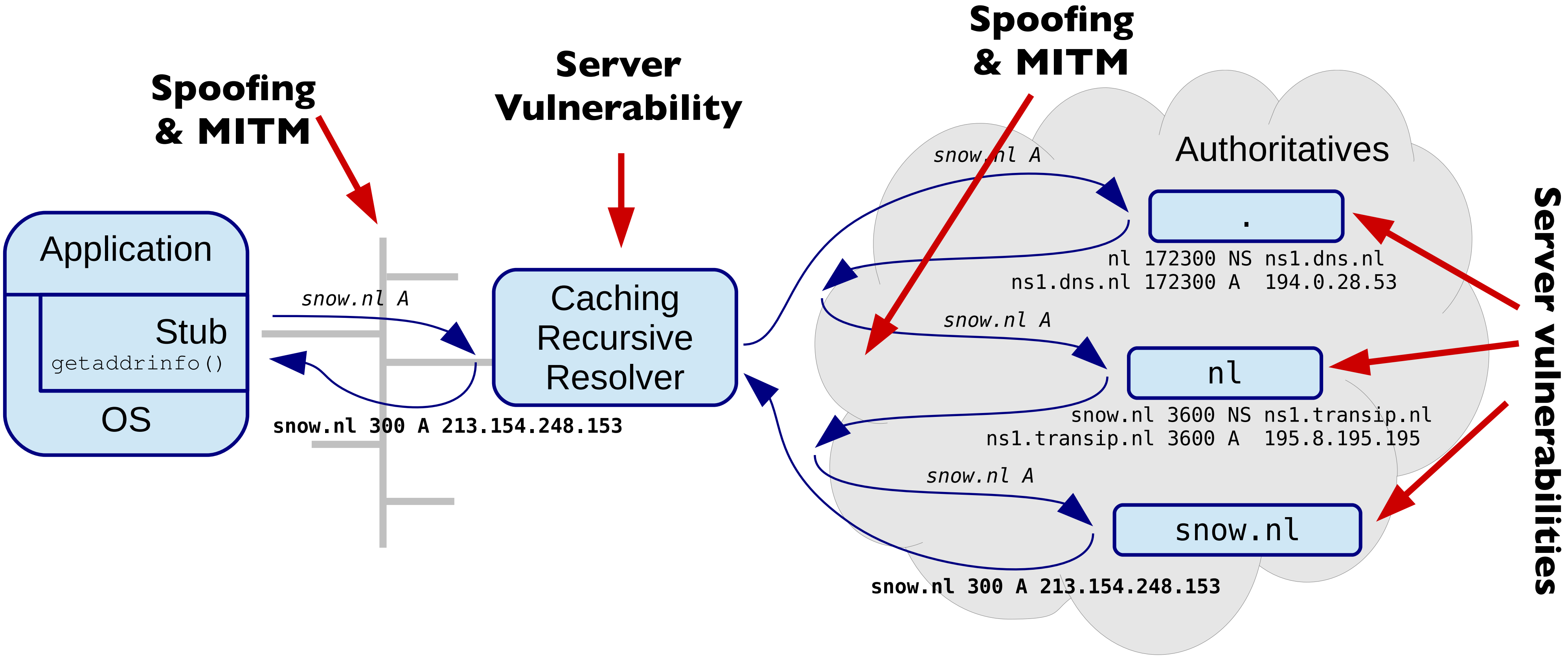
bits	50% kans	5% kans	Methode
~~16~~	~~10 seconden~~	~~1 seconde~~	~~Query ID~~
~~26~~	~~2,8 uur~~	~~17 minuten~~	~~1024 source poorten~~
2	0 seconden	0 seconden	~~Alle source poorten~~ 2 bits server selectie
~~44~~	~~288444 dagen~~	~~2844,4 dagen~~	~~0x20 hack~~
5	0 seconden	0 seconden	IP ID

Domain Name System - security

bits	50% kans	5% kans	Methode
~~16~~	~~10 seconden~~	~~1 seconde~~	~~Query ID~~
~~26~~	~~2,8 uur~~	~~17 minuten~~	~~1024 source poorten~~
2	0 seconden	0 seconden	~~Alle source poorten~~ 2 bits server selectie
~~44~~	~~288444 dagen~~	~~2844,4 dagen~~	~~0x20 hack~~
5	0 seconden	0 seconden	IP ID
69	2.928.370.544 jaar	2.928.370.544 jaar	IPv6 /64 source adres

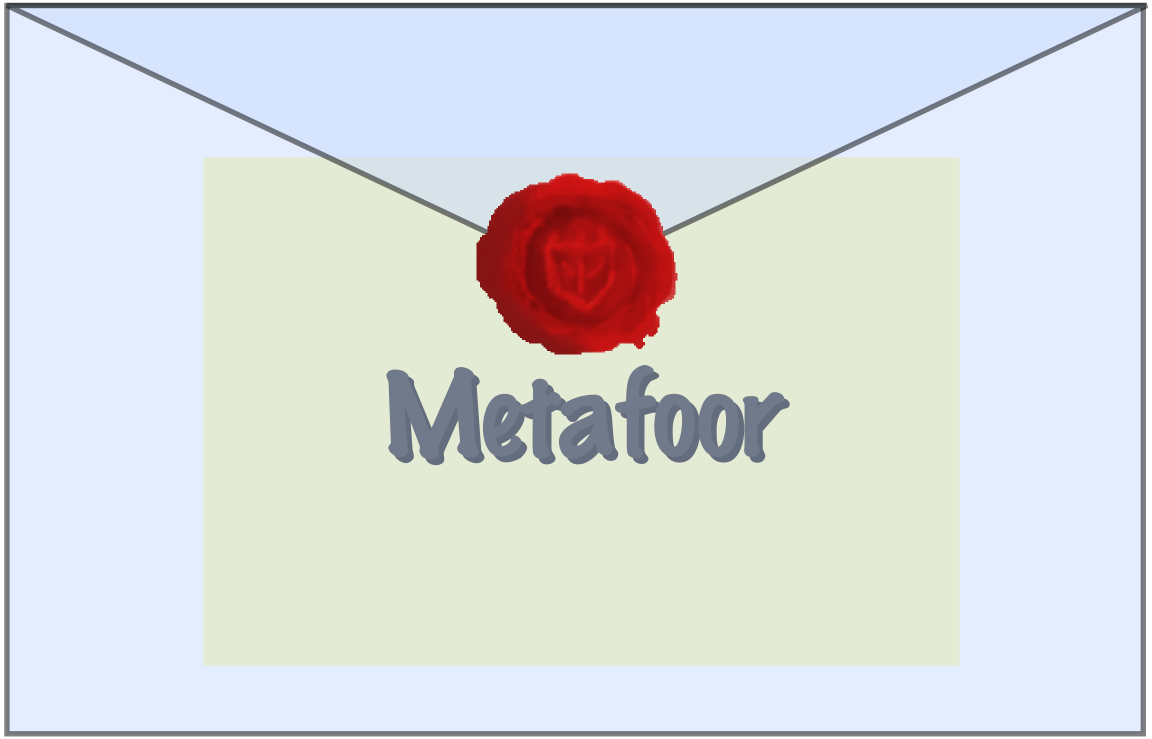
Domain Name System – security

- ‘t is niet alleen spoofing



DNS Security Extensions (DNSSEC)

- end-to-end security bovenop DNS

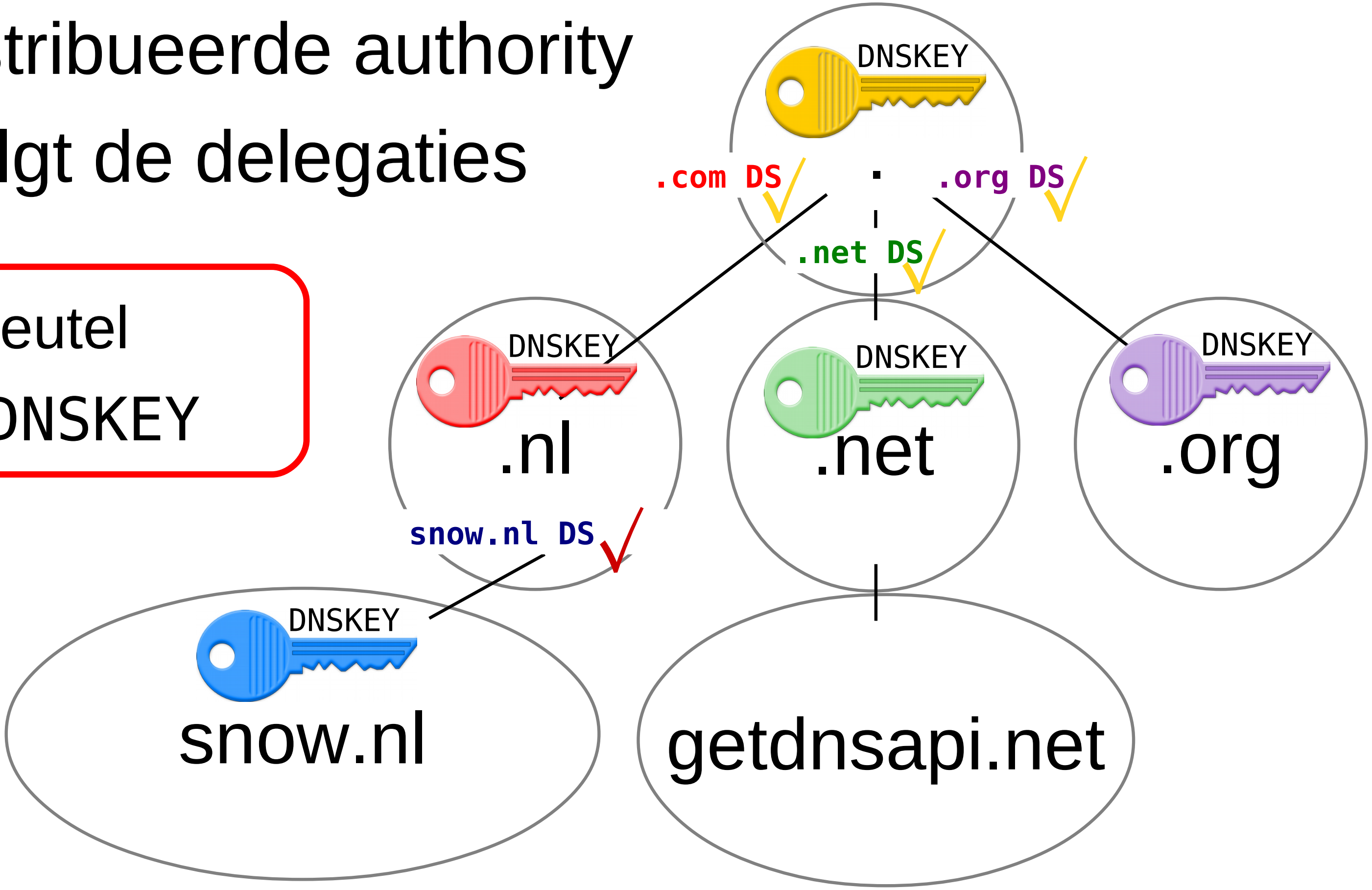


DNS Security Extensions (DNSSEC)

Chain of trust

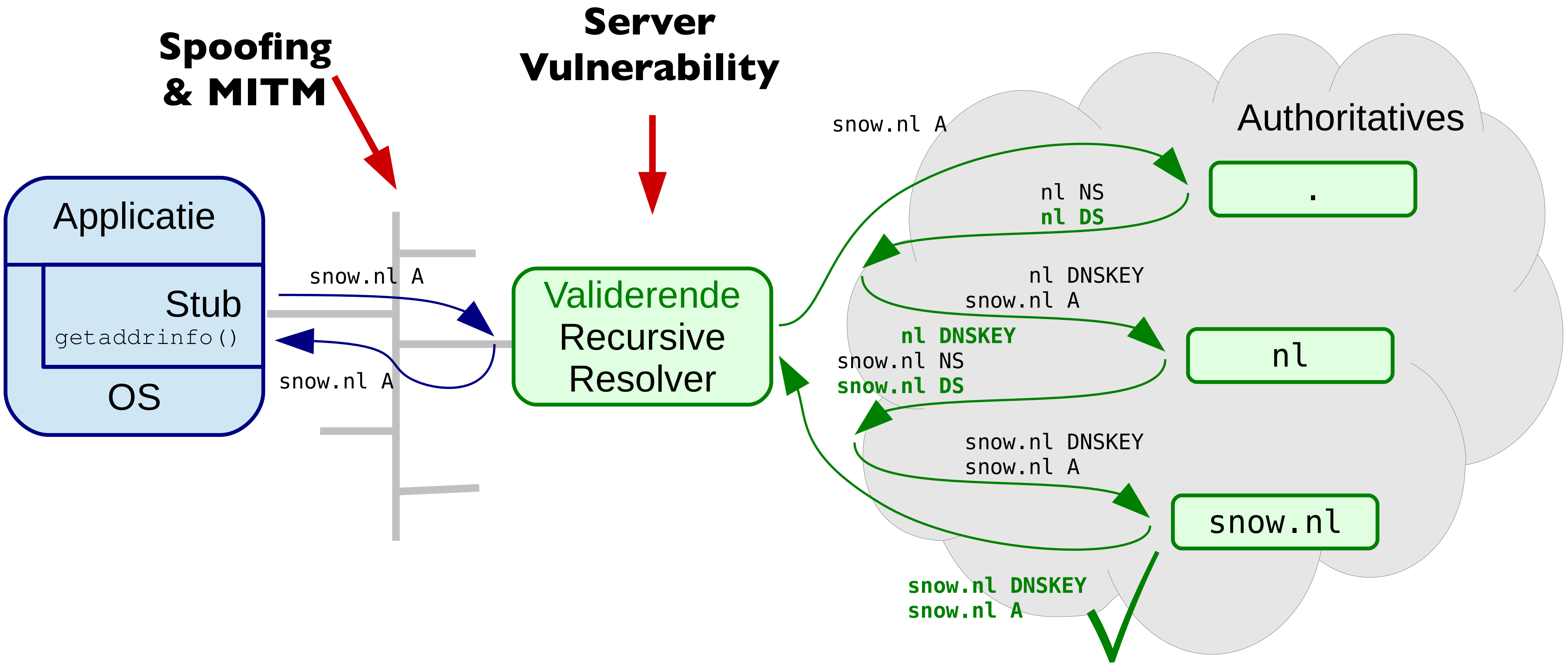
- Zones met gedistribueerde authority
- Chain of trust volgt de delegaties

- DNSKEY Publieke sleutel
- DS Hash van DNSKEY



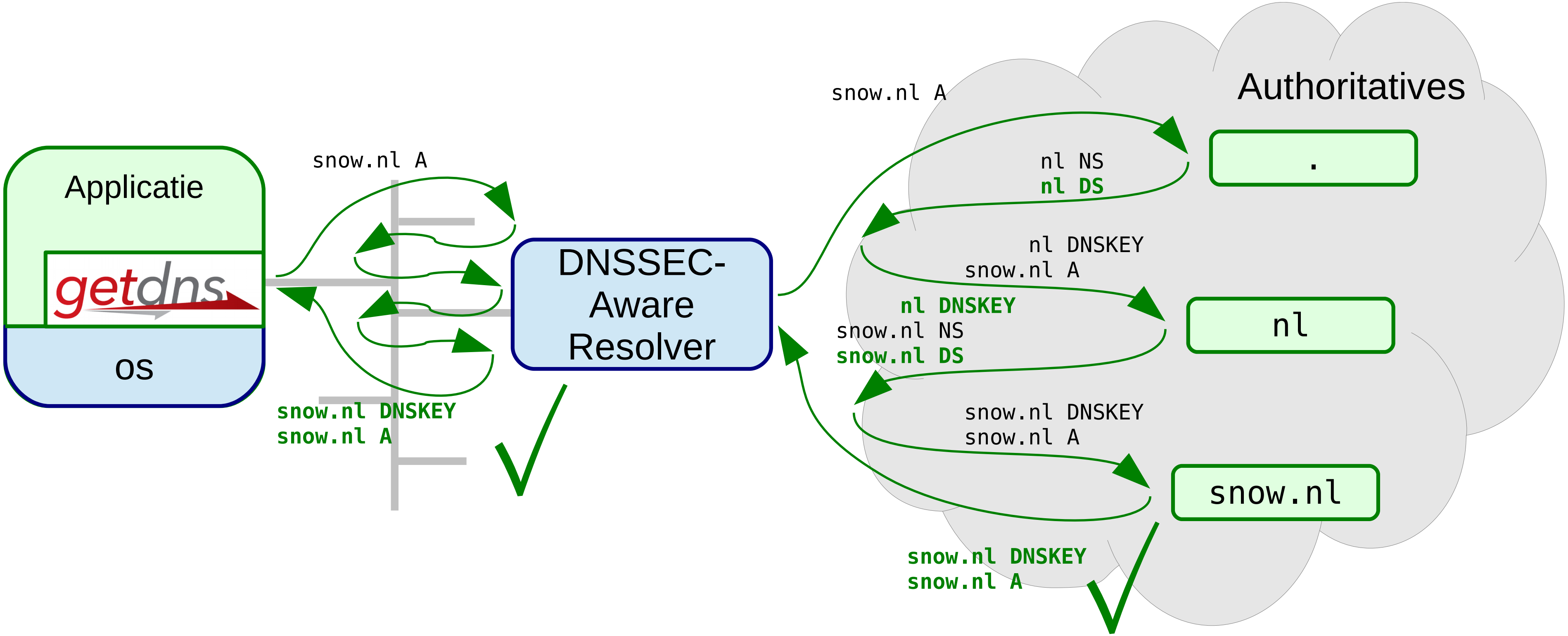
DNS Security Extensions (DNSSEC)

Validatie



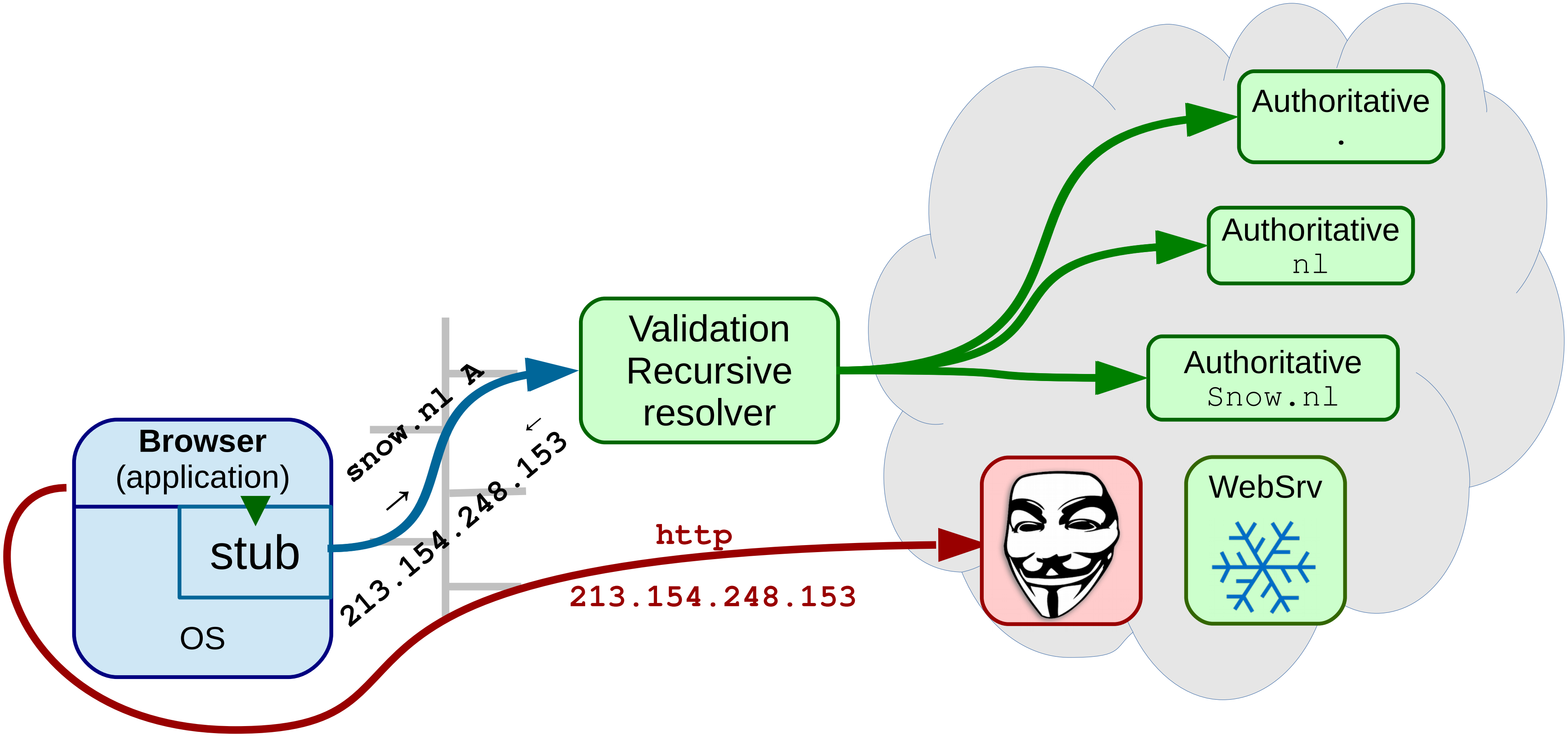
DNS Security Extensions (DNSSEC)

end-to-end validatie



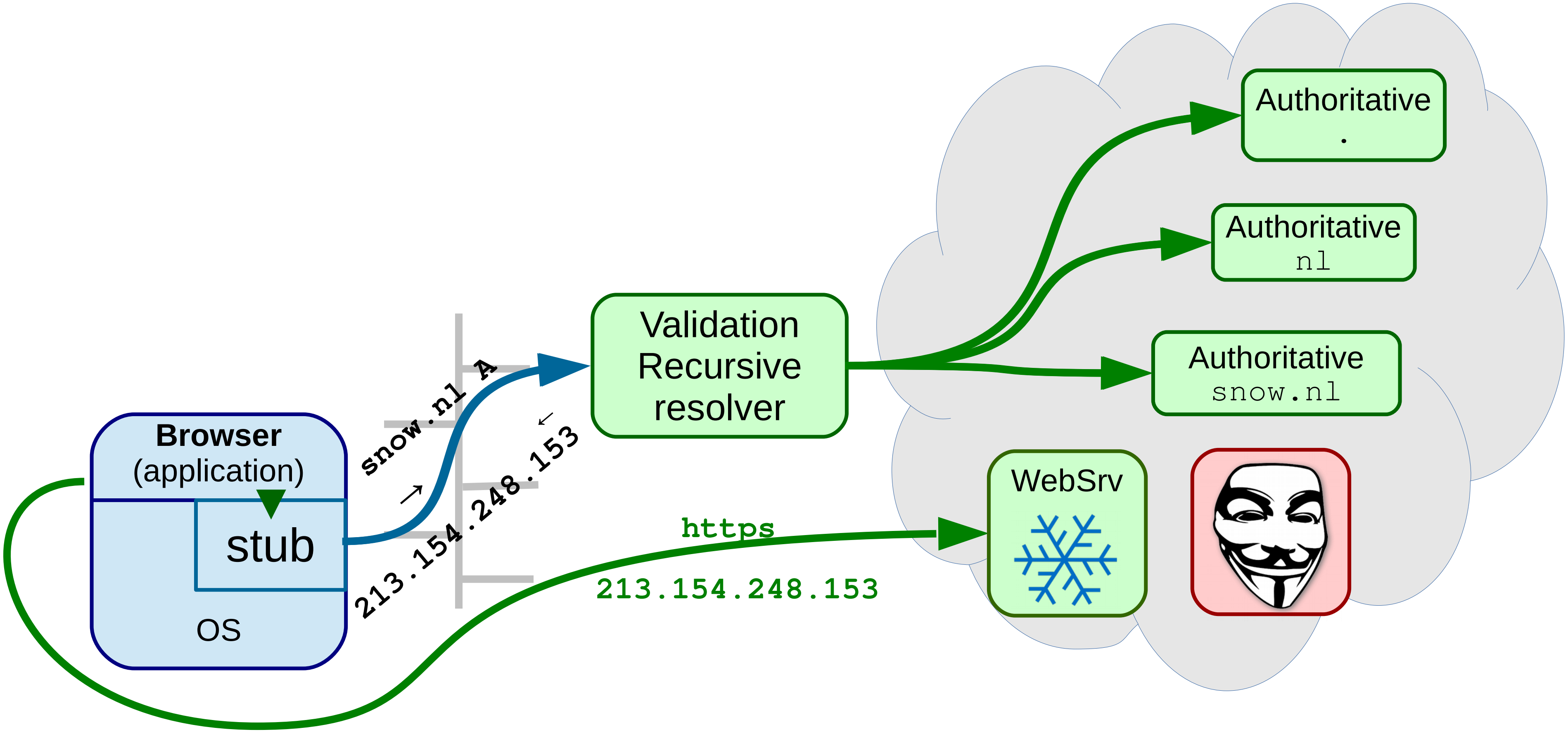
DNS Security Extensions (DNSSEC)

beschermt niet tegen MITM



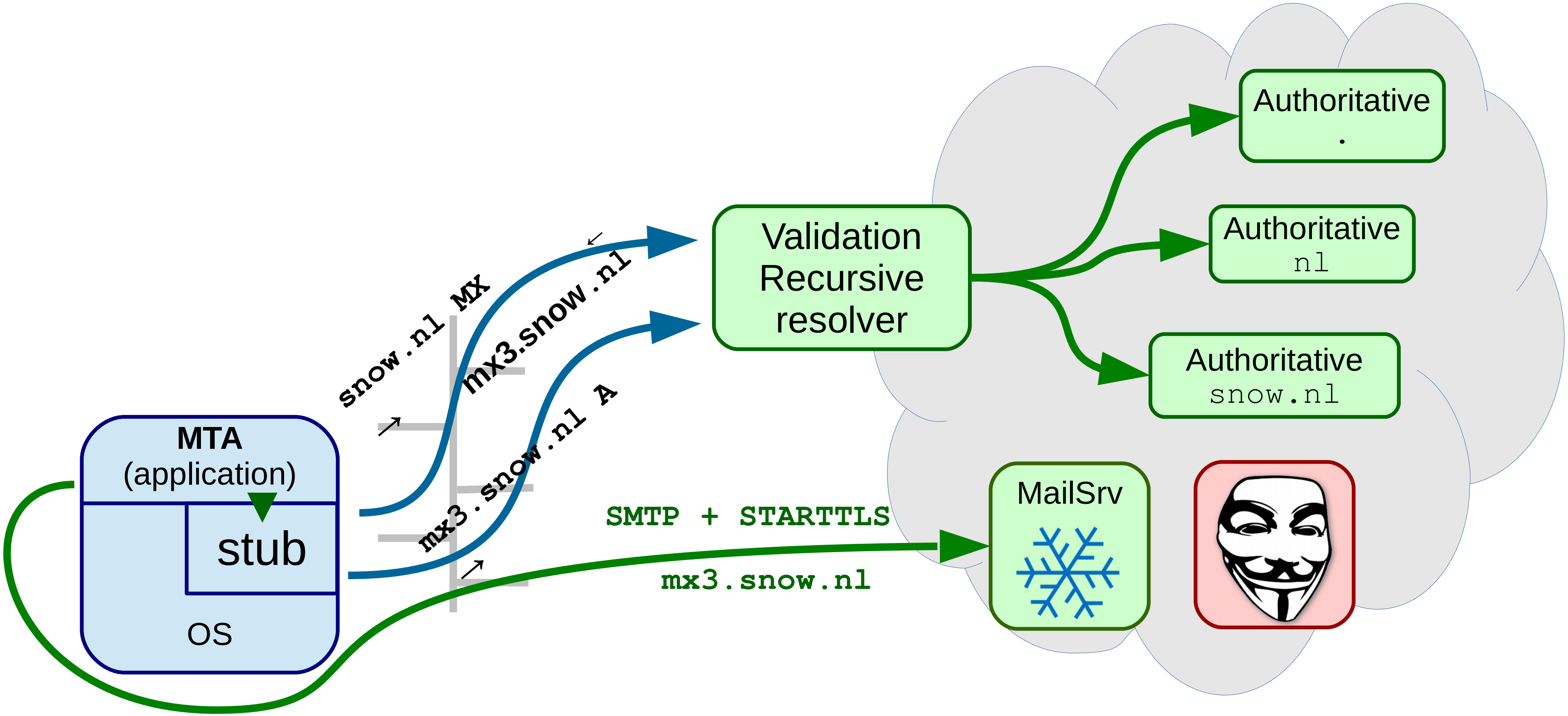
DNS Security Extensions (DNSSEC)

beschermt niet tegen MITM – TLS wel!



DNS Security Extensions (DNSSEC)

toch nodig voor DNS referrals

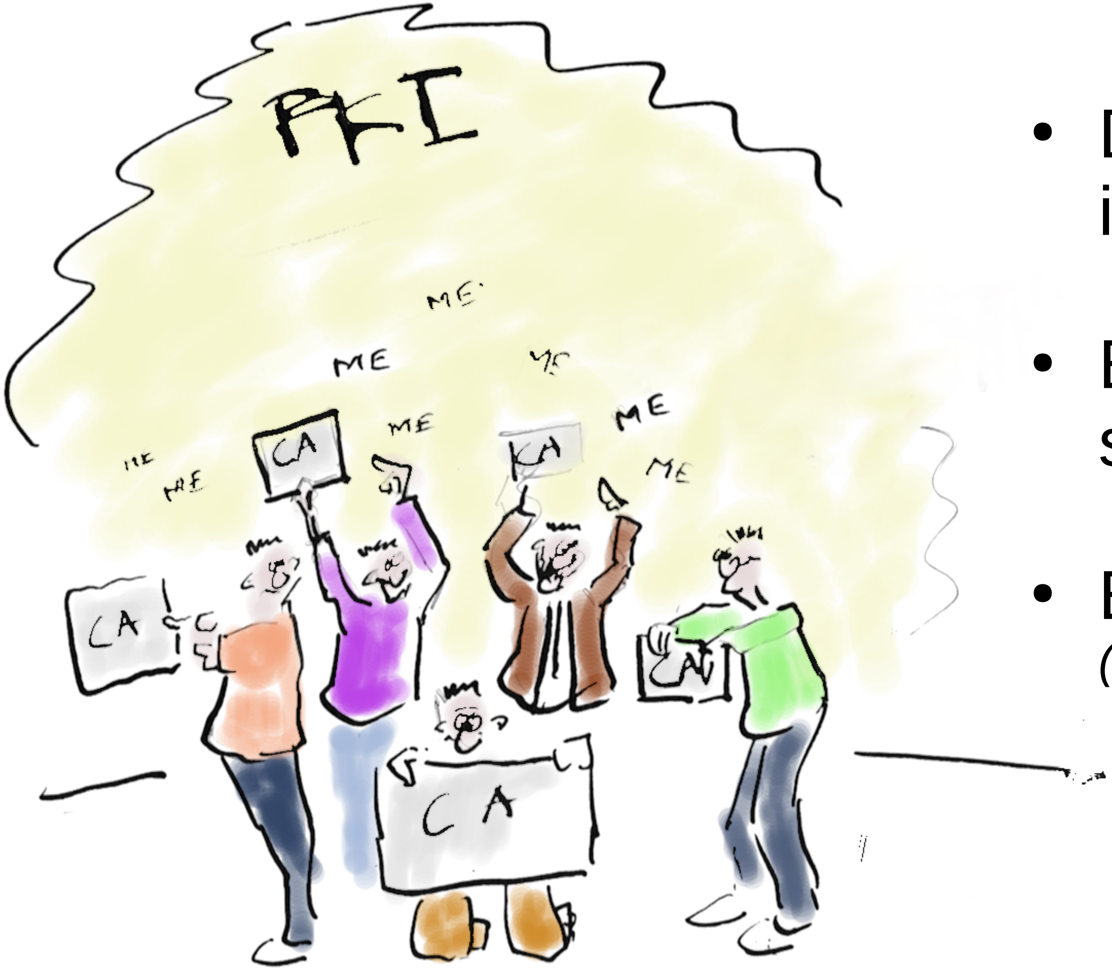


DNSSEC voor Applicaties

voor TLS

- Transport Layer Security (TLS) gebruikt zowel asymmetrische als symmetrische cryptografie
- Een symmetrische sleutel wordt versleuteld verstuurd samen met de publieke sleutel van de andere kant
- Hoe wordt die publieke sleutel geverifieerd?

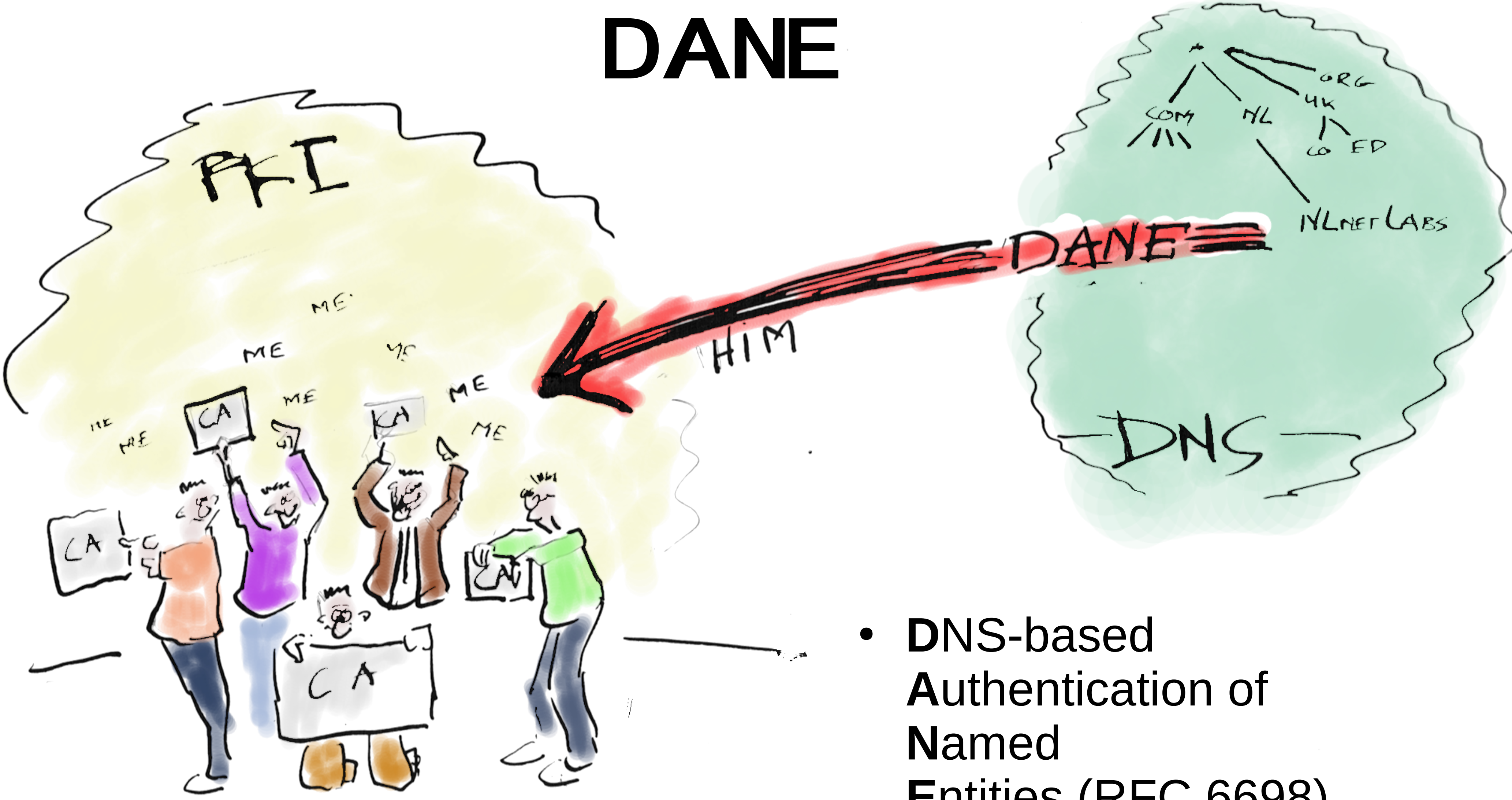
TLS zonder DNSSEC



spotprent van Kloot

- Door de Certificate Authorities in OS en/of browser
- Elke CA is gemachtigd in te staan voor **elke** domein naam
- Er zijn meer dan 1500 CAs
  (in 2010, zie https://www.eff.org/observatory)

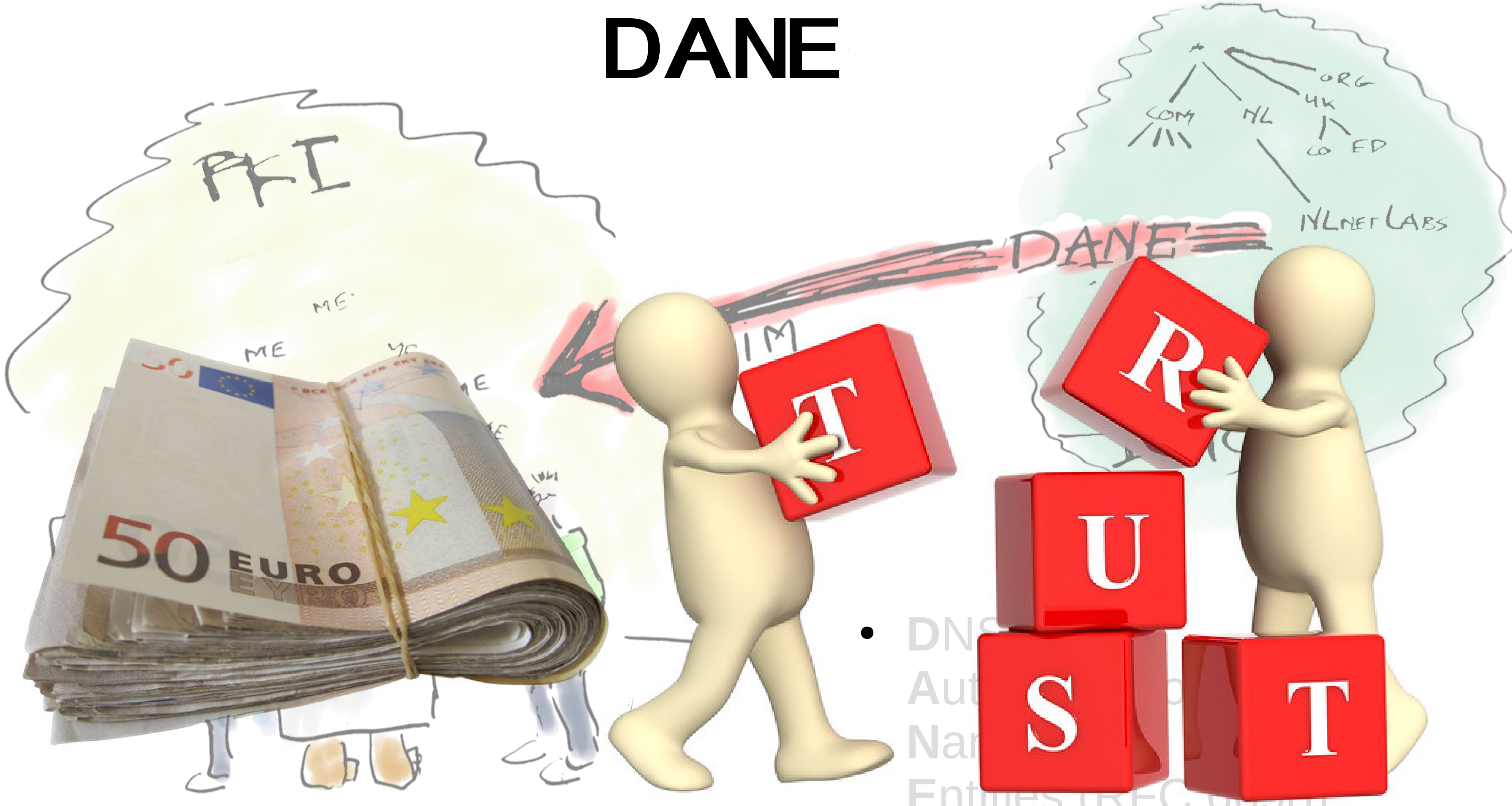
DANE



- **D**NS-based **A**uthentication of **N**amed **E**ntities (RFC 6698)

spotprent van Kloot

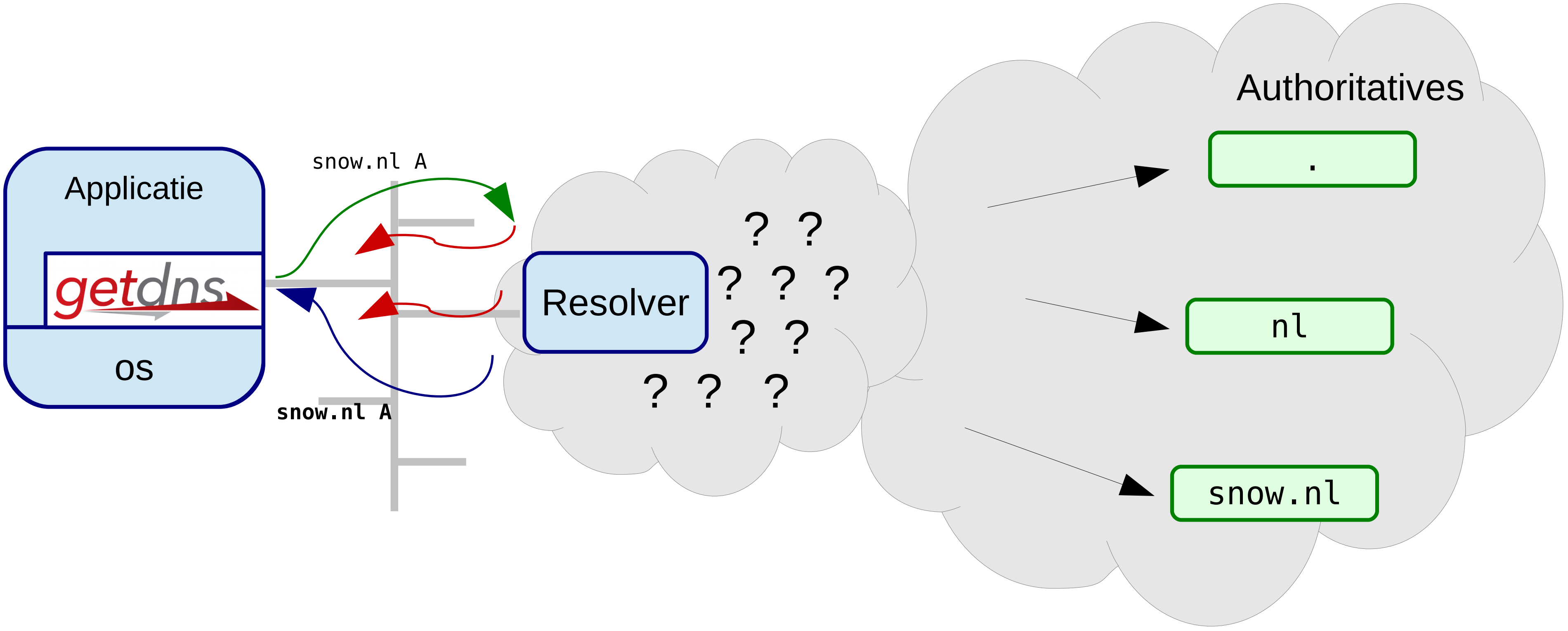
DANE



- DNS
  Aut
  Na
  Entities (RFC 6698)

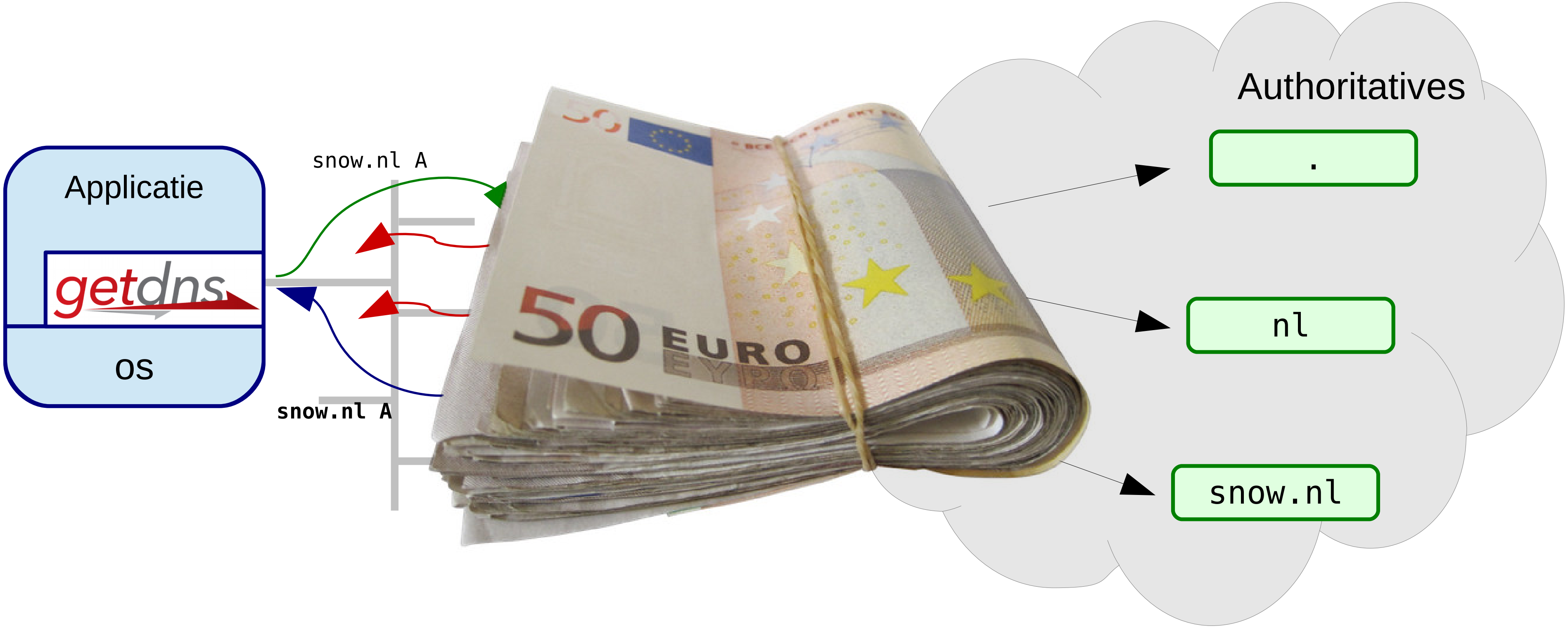
DNS Security Extensions (DNSSEC)

end-to-end validatie in de praktijk



DNS Security Extensions (DNSSEC)

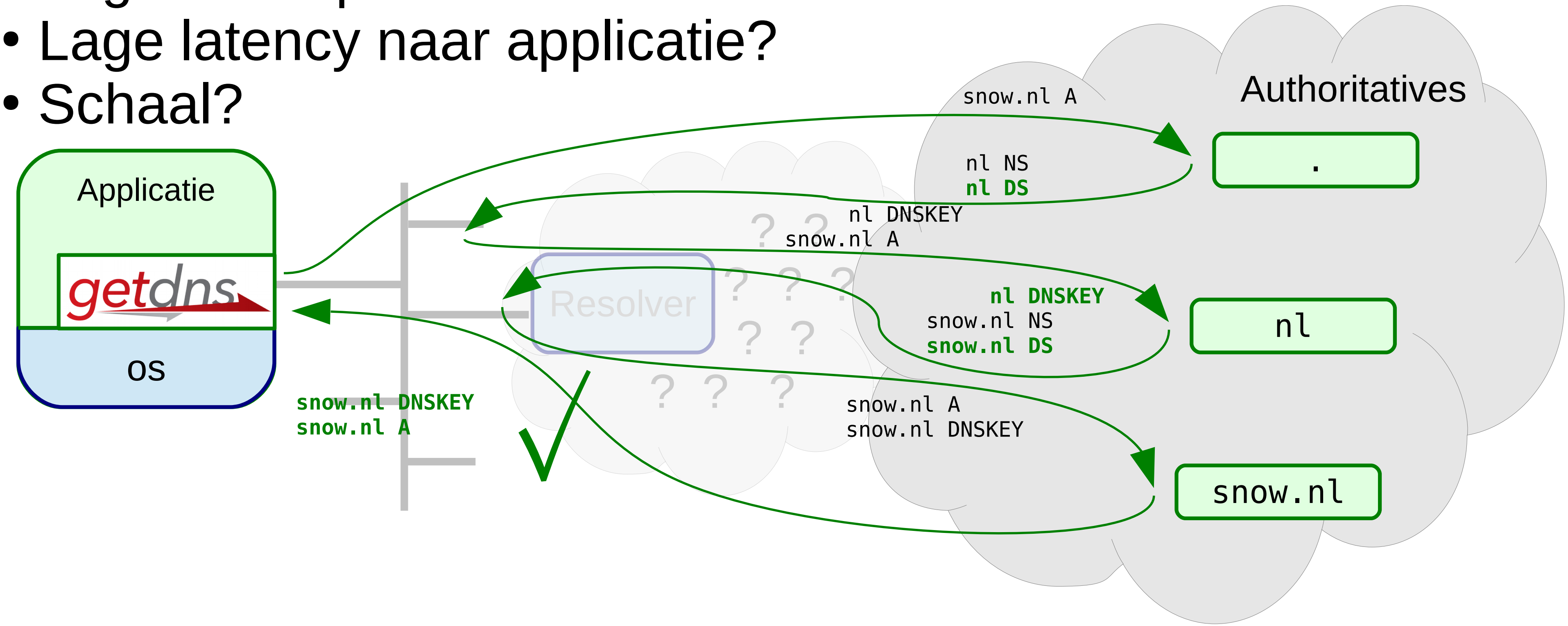
end-to-end validatie in de praktijk



DNS Security Extensions (DNSSEC)

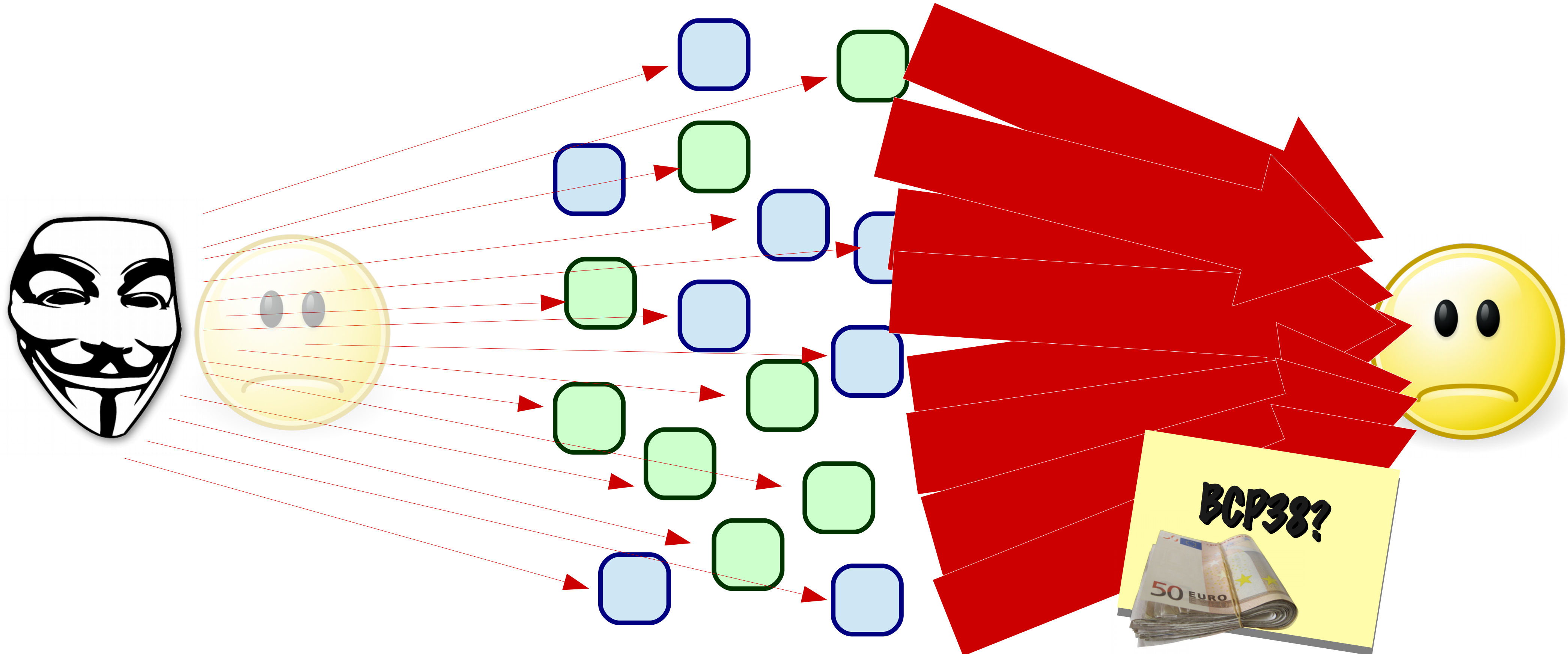
end-to-end validatie in de praktijk

- Lage load op de authoritatives?
- Lage latency naar applicatie?
- Schaal?



DNS Security Extensions (DNSSEC)

consequentie van UDP erger met DNSSEC



Privacy

maart 2011 :	I-D Privacy Considerations for Internet Protocols
juni 2013 :	[redacted] Revelations Morecowbell
juli 2013 :	RFC6973 Privacy Considerations for Internet Protocols
mei 2014 :	RFC7258 Pervasive Monitoring is an Attack

Privacy Folk Singer

Picture © (CC BY 3.0) Laura Poitras

Overal
Encryptie

tions
tocols

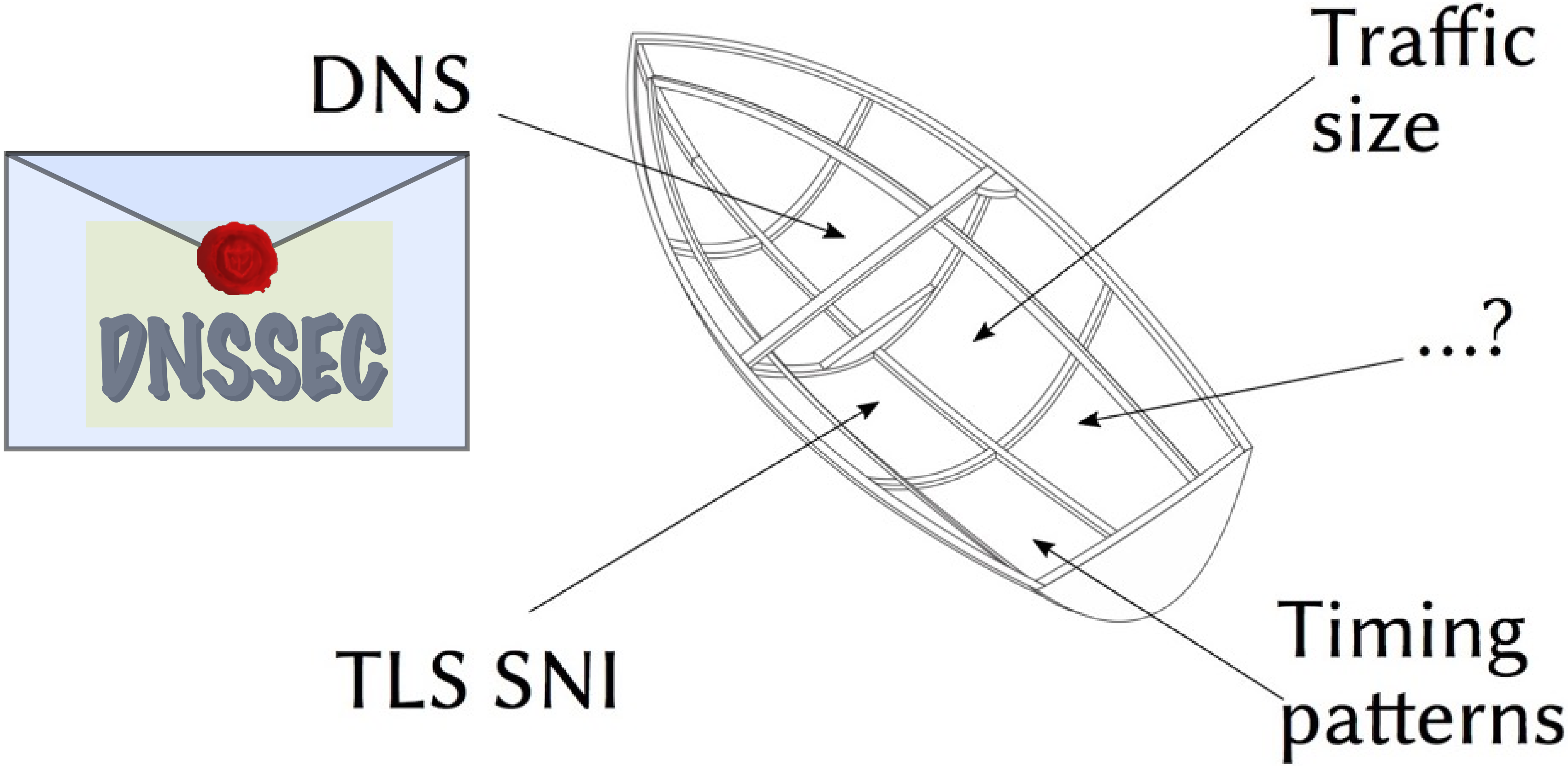
juni 2013 : [redacted] Revelations
Morecowbell

juli 2013 : RFC6973
Privacy Considerations
for Internet Protocols

mei 2014: RFC7258
Pervasive Monitoring
is an Attack

Picture © (CC BY 3.0) Laura Poitras

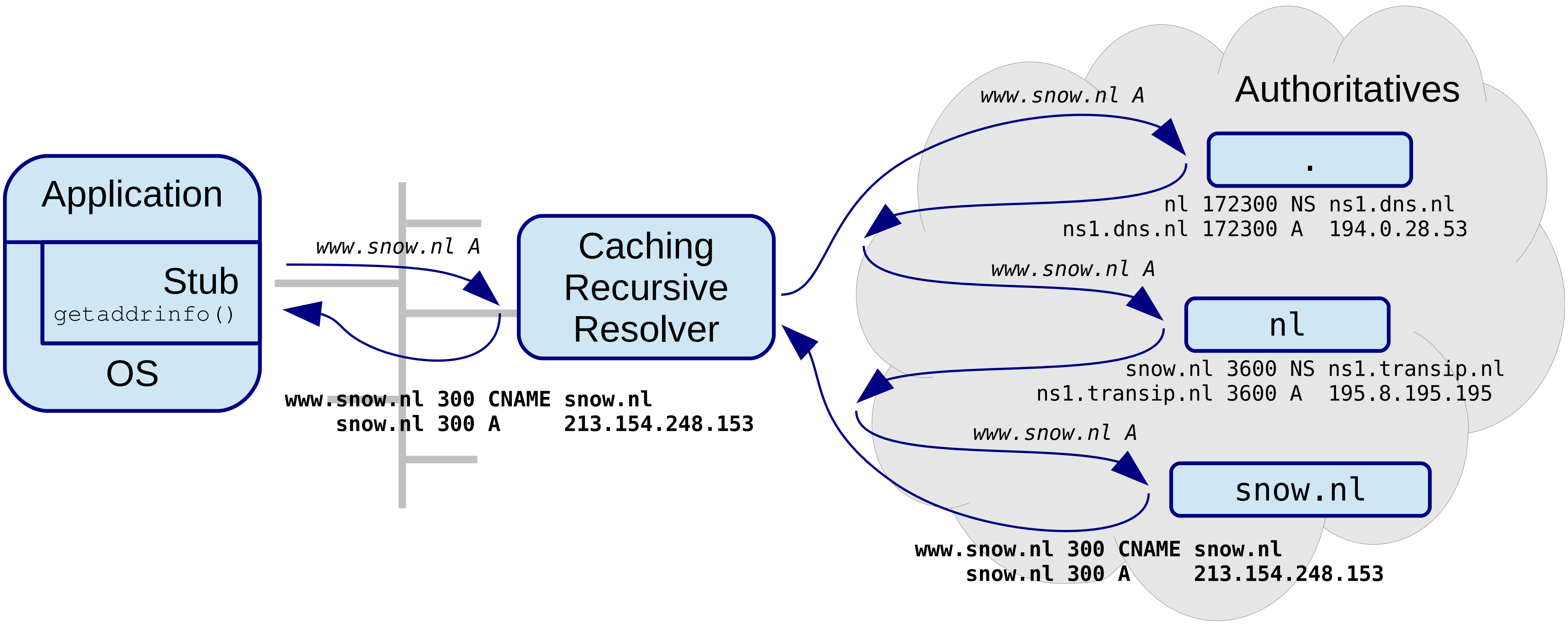
Privacy



- NSA's Morecowbell op DNS gebaseerde monitoring systeem

Leaky Boat van DKG

Privacy issues met DNS



```
www.snow.nl 300 CNAME snow.nl
    snow.nl 300 A     213.154.248.153
```

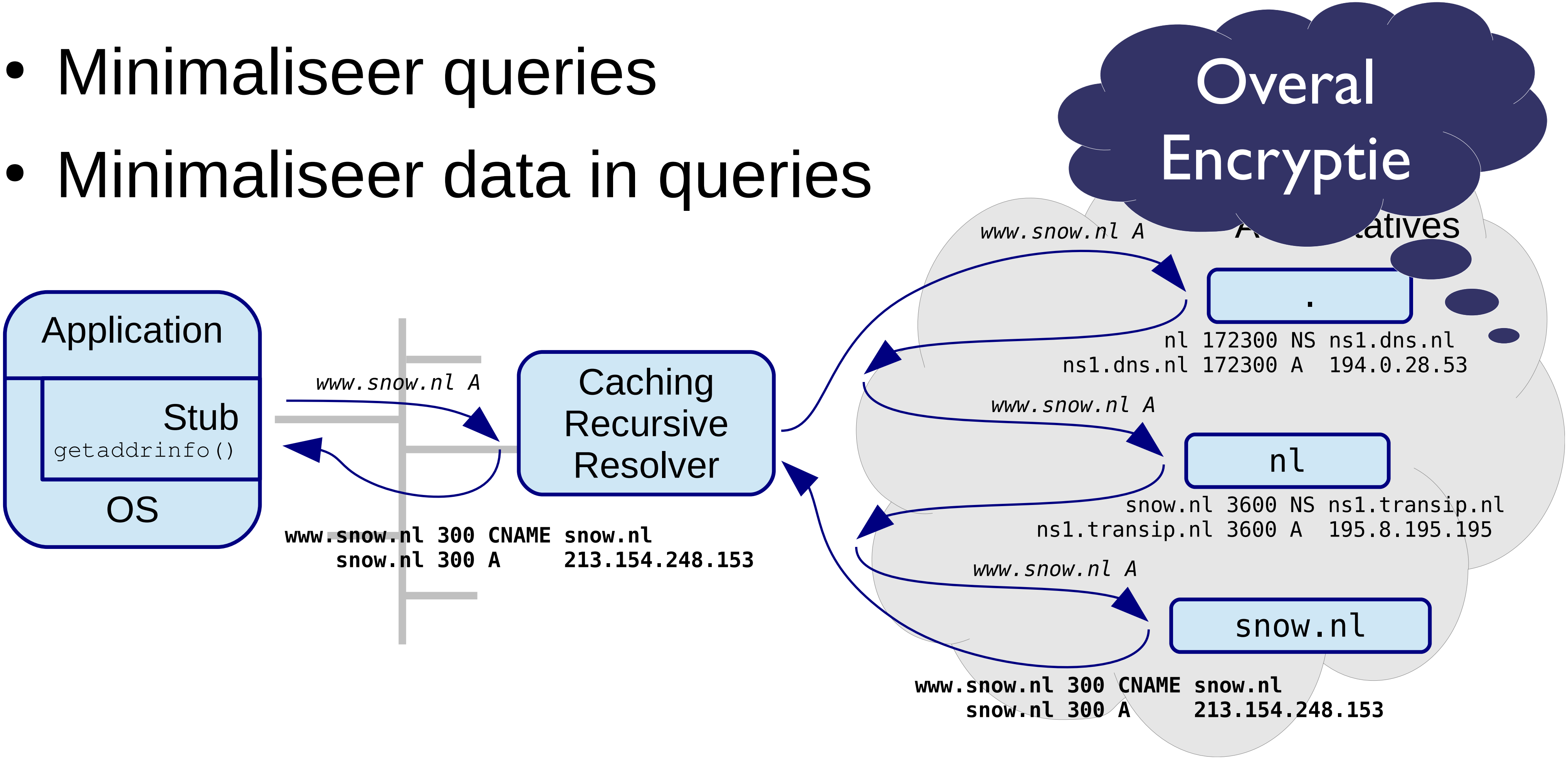
```
     nl 172300 NS ns1.dns.nl
ns1.dns.nl 172300 A  194.0.28.53
```

```
    snow.nl 3600 NS ns1.transip.nl
ns1.transip.nl 3600 A  195.8.195.195
```

```
www.snow.nl 300 CNAME snow.nl
    snow.nl 300 A     213.154.248.153
```

Privacy issues met DNS

- Minimaliseer queries
- Minimaliseer data in queries



```
www.snow.nl 300 CNAME snow.nl
    snow.nl 300 A     213.154.248.153
```

```
         nl 172300 NS ns1.dns.nl
ns1.dns.nl 172300 A  194.0.28.53
```

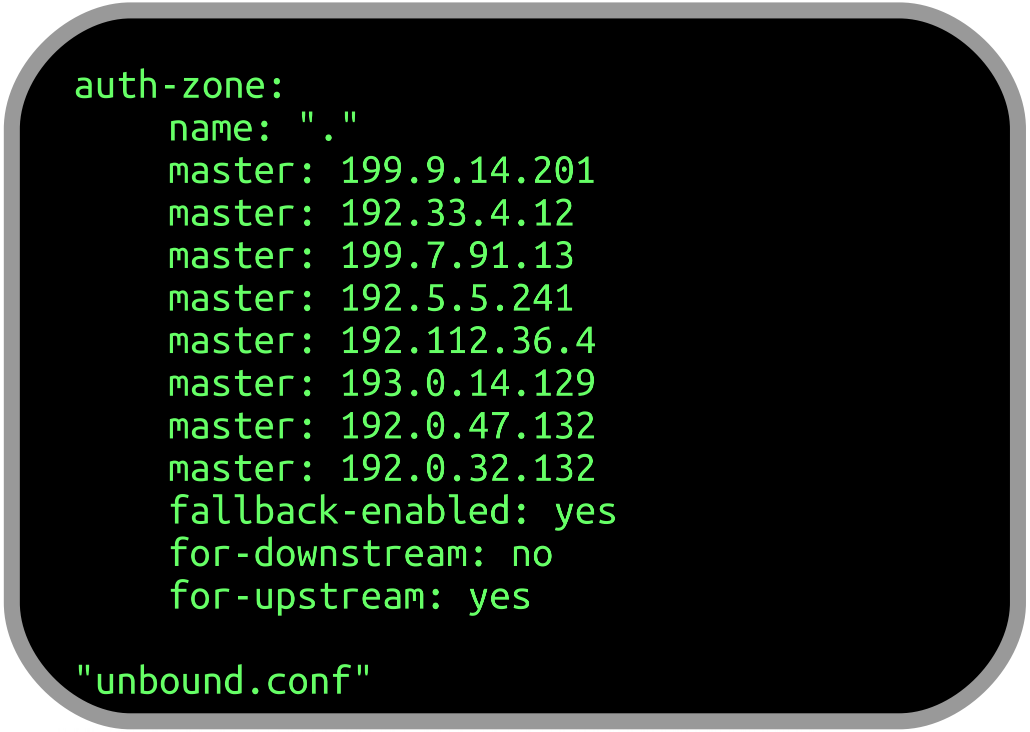
```
      snow.nl 3600 NS ns1.transip.nl
ns1.transip.nl 3600 A  195.8.195.195
```

```
www.snow.nl 300 CNAME snow.nl
    snow.nl 300 A     213.154.248.153
```

Privacy issues met DNS

minimaliseer queries – local root

- RFC 7706 -
  Running a Root Server Local to a Resolver



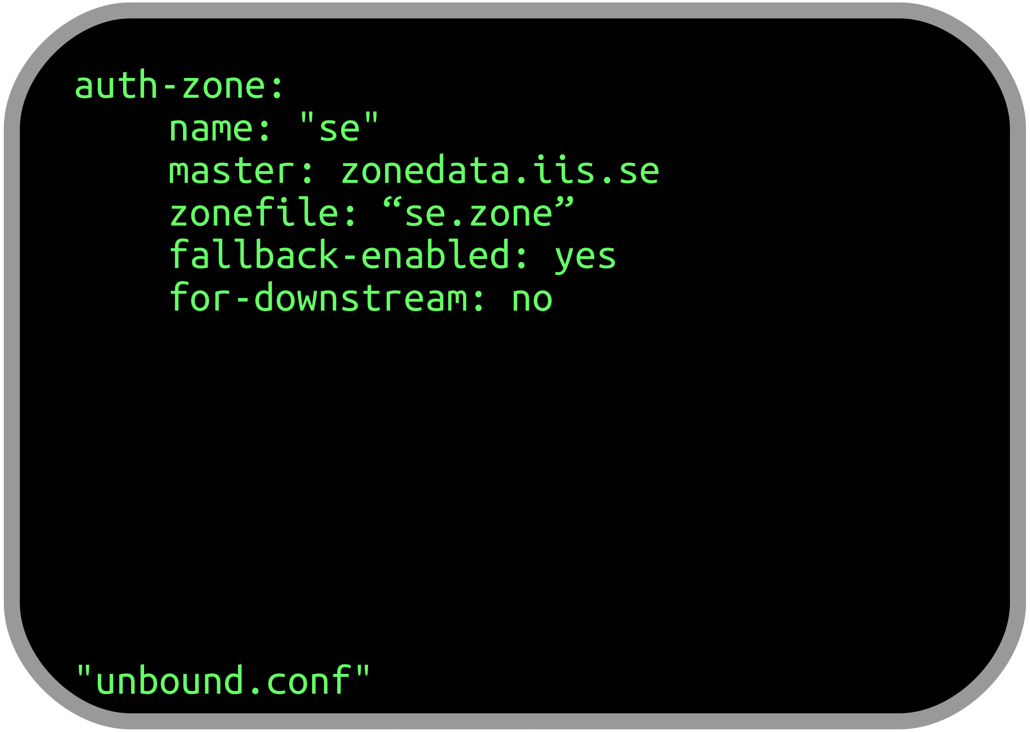
```
auth-zone:
    name: "."
    master: 199.9.14.201
    master: 192.33.4.12
    master: 199.7.91.13
    master: 192.5.5.241
    master: 192.112.36.4
    master: 193.0.14.129
    master: 192.0.47.132
    master: 192.0.32.132
    fallback-enabled: yes
    for-downstream: no
    for-upstream: yes

"unbound.conf"
```

unbound

Privacy issues met DNS

minimaliseer queries – local auth zone

- RFC 7706 -
  Running a Root Server Local to a Resolver
- Kan ook voor andere authoritative servers



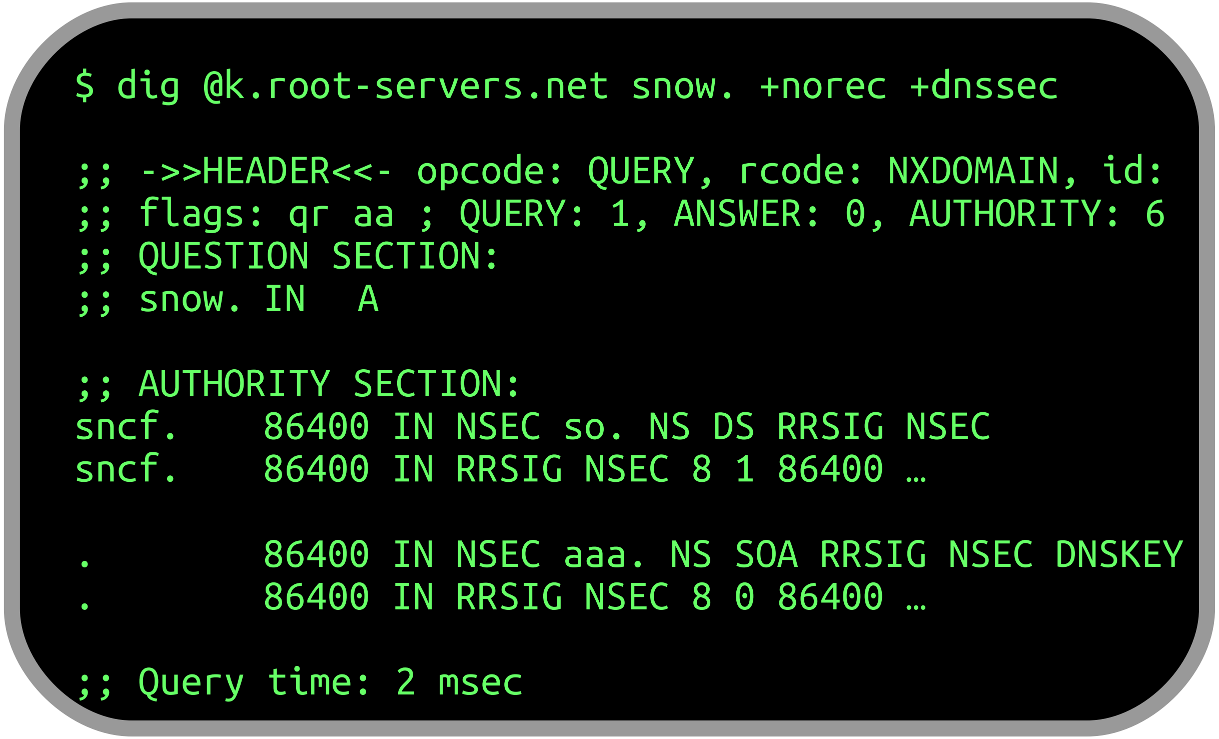
```
auth-zone:
    name: "se"
    master: zonedata.iis.se
    zonefile: “se.zone”
    fallback-enabled: yes
    for-downstream: no




"unbound.conf"
```

unbound

Privacy issues met DNS

minimaliseer queries – aggressive NSEC

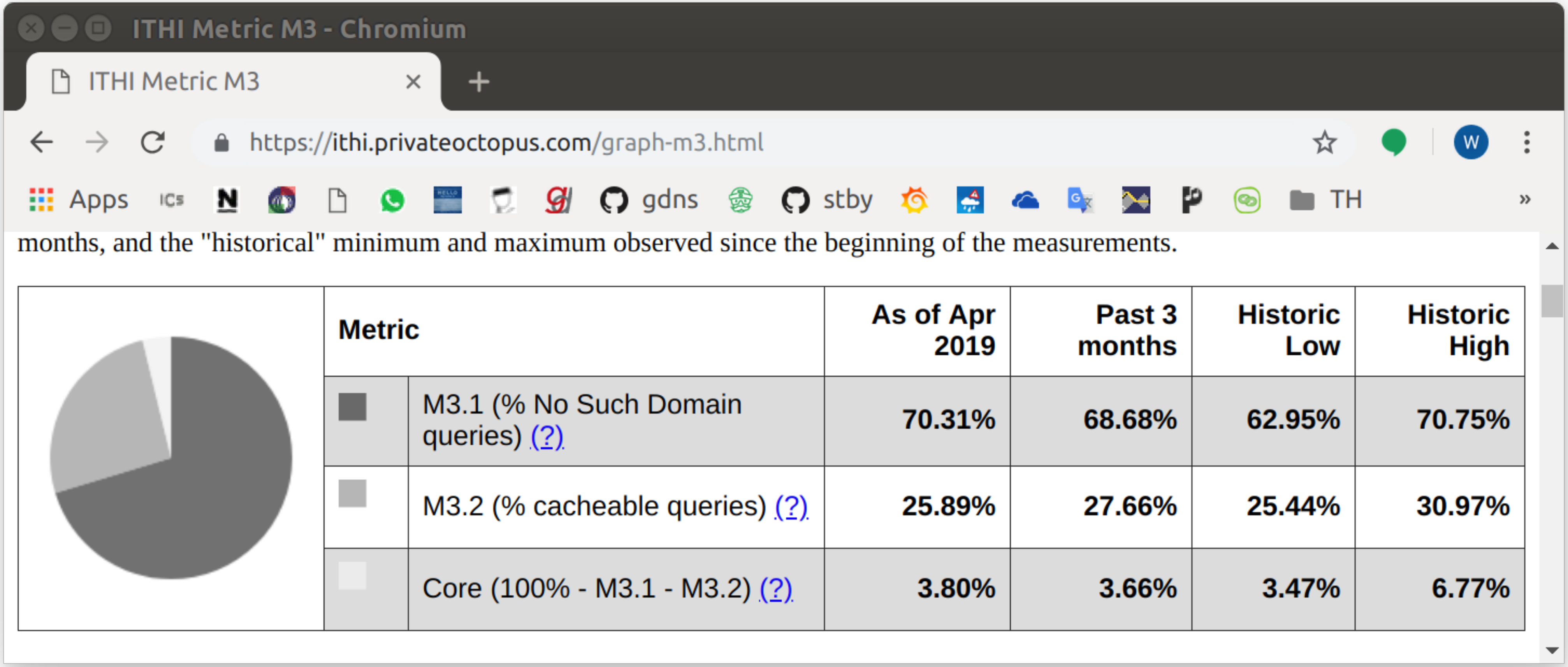
- RFC8198 - Aggressive NSEC



```
$ dig @k.root-servers.net snow. +norec +dnssec

;; ->>HEADER<<- opcode: QUERY, rcode: NXDOMAIN, id:
;; flags: qr aa ; QUERY: 1, ANSWER: 0, AUTHORITY: 6
;; QUESTION SECTION:
;; snow. IN   A

;; AUTHORITY SECTION:
sncf.    86400 IN NSEC so. NS DS RRSIG NSEC
sncf.    86400 IN RRSIG NSEC 8 1 86400 …

.        86400 IN NSEC aaa. NS SOA RRSIG NSEC DNSKEY
.        86400 IN RRSIG NSEC 8 0 86400 …

;; Query time: 2 msec
```

Privacy issues met DNS

minimaliseer queries – aggressive NSEC


ITHI Metric M3 - Chromium
ITHI Metric M3
https://ithi.privateoctopus.com/graph-m3.html
W
Apps
ICs
gdns
stby
TH
»

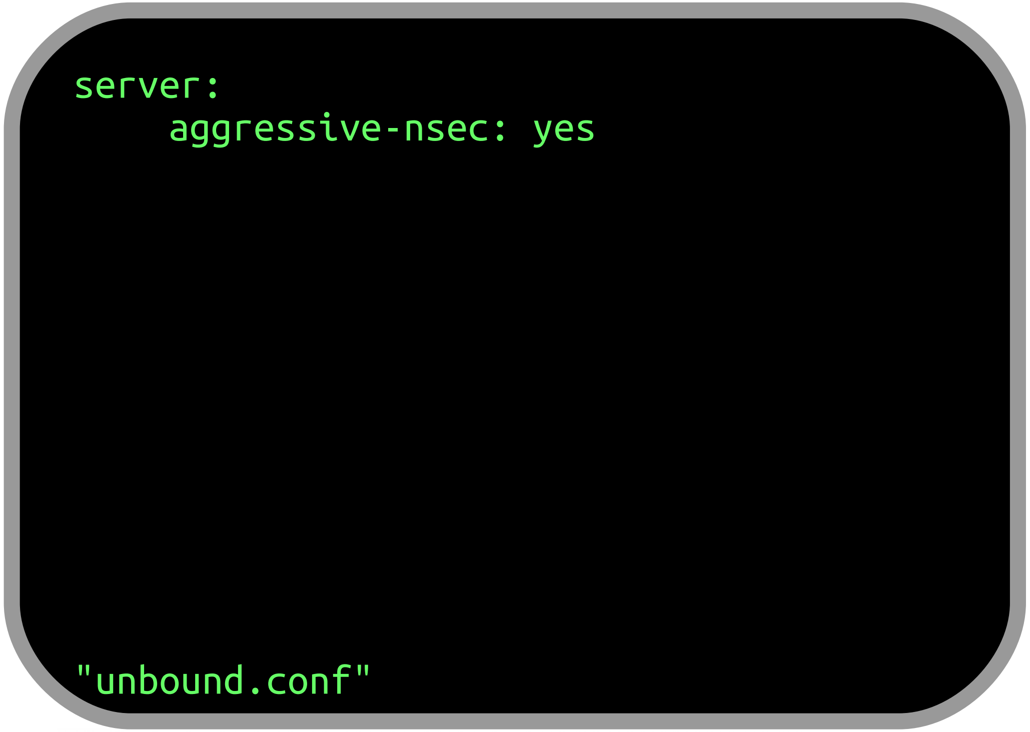
months, and the "historical" minimum and maximum observed since the beginning of the measurements.

		Metric	As of Apr 2019	Past 3 months	Historic Low	Historic High
	■	M3.1 (% No Such Domain queries) (?)	70.31%	68.68%	62.95%	70.75%
	▨	M3.2 (% cacheable queries) (?)	25.89%	27.66%	25.44%	30.97%
	□	Core (100% - M3.1 - M3.2) (?)	3.80%	3.66%	3.47%	6.77%

Privacy issues met DNS

minimaliseer queries – aggressive NSEC

- RFC8198 - Aggressive NSEC



```
server:
    aggressive-nsec: yes
```

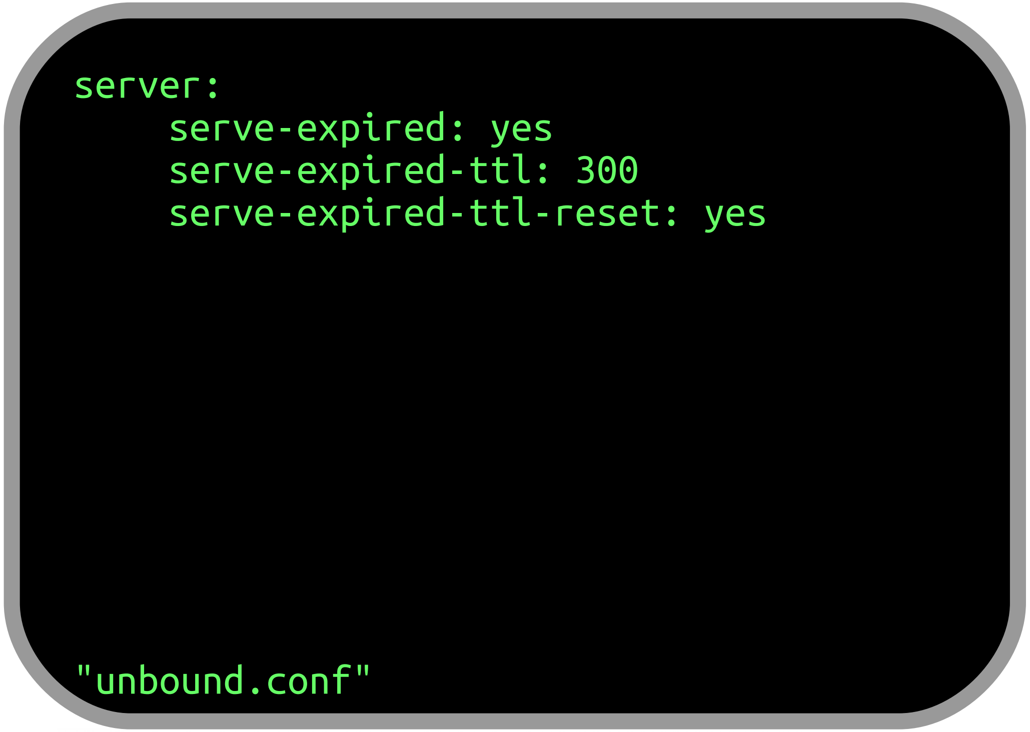
```
"unbound.conf"
```

unbound

Privacy issues met DNS

minimaliseer queries – serve stale

- draft-ietf-dnsop-serve-stale
- Privacy aspect en/of Performance aspect



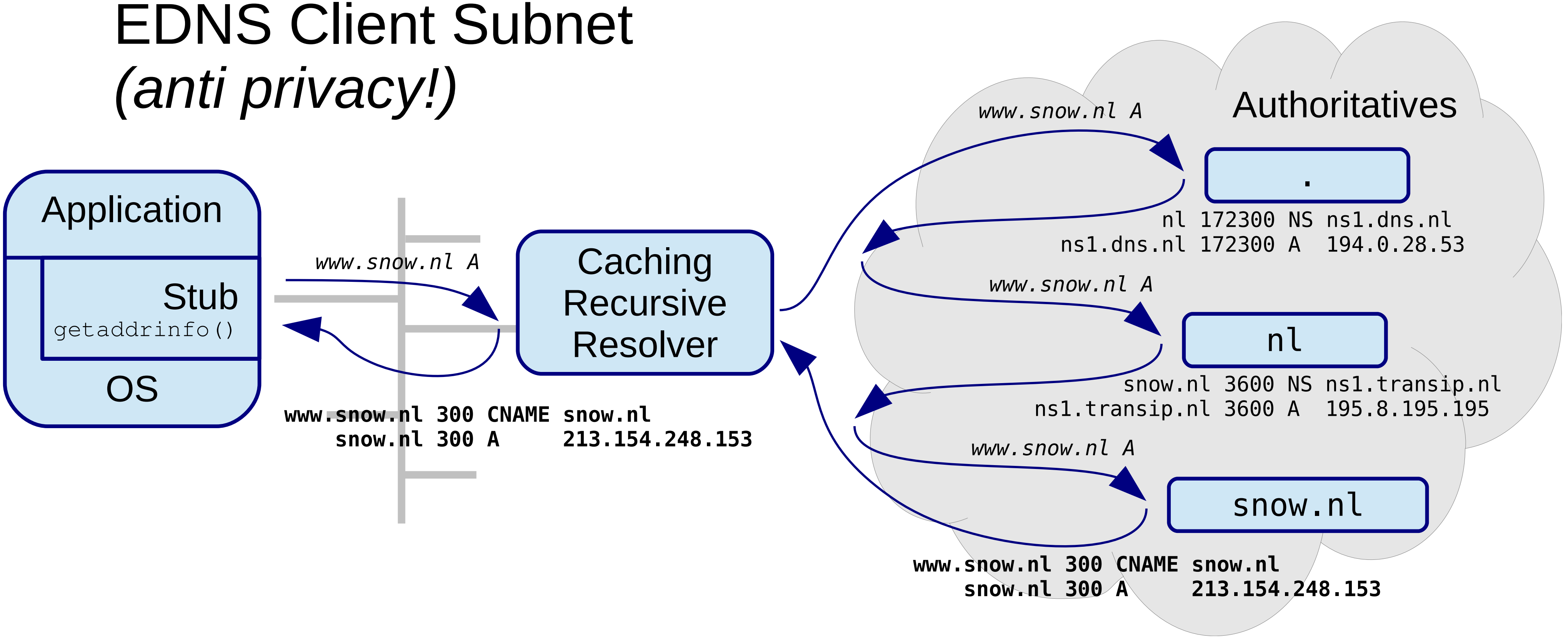
```
server:
    serve-expired: yes
    serve-expired-ttl: 300
    serve-expired-ttl-reset: yes




"unbound.conf"
```

unbound

Privacy issues met DNS

minimaliseer data in queries – ECS

- RFC7871 -
  EDNS Client Subnet
  (anti privacy!)



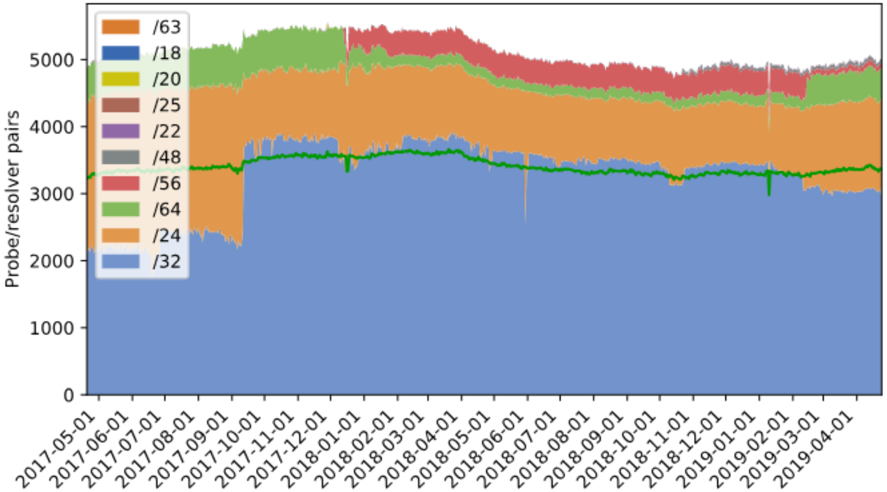
```
www.snow.nl 300 CNAME snow.nl
    snow.nl 300 A     213.154.248.153
```

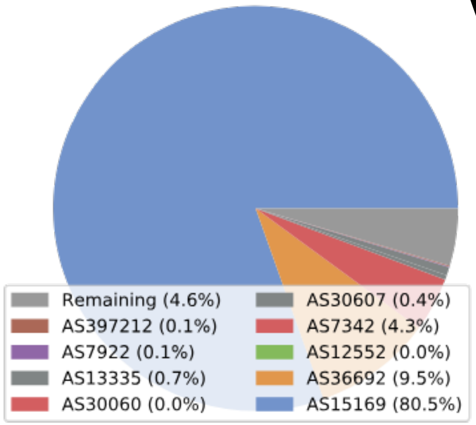
```
www.snow.nl 300 CNAME snow.nl
    snow.nl 300 A     213.154.248.153
```

Privacy issues met DNS

minimaliseer data in queries – ECS

- RFC7871 -
  EDNS Client Subnet
  (anti privacy!)





DNSThought

Privacy issues met DNS

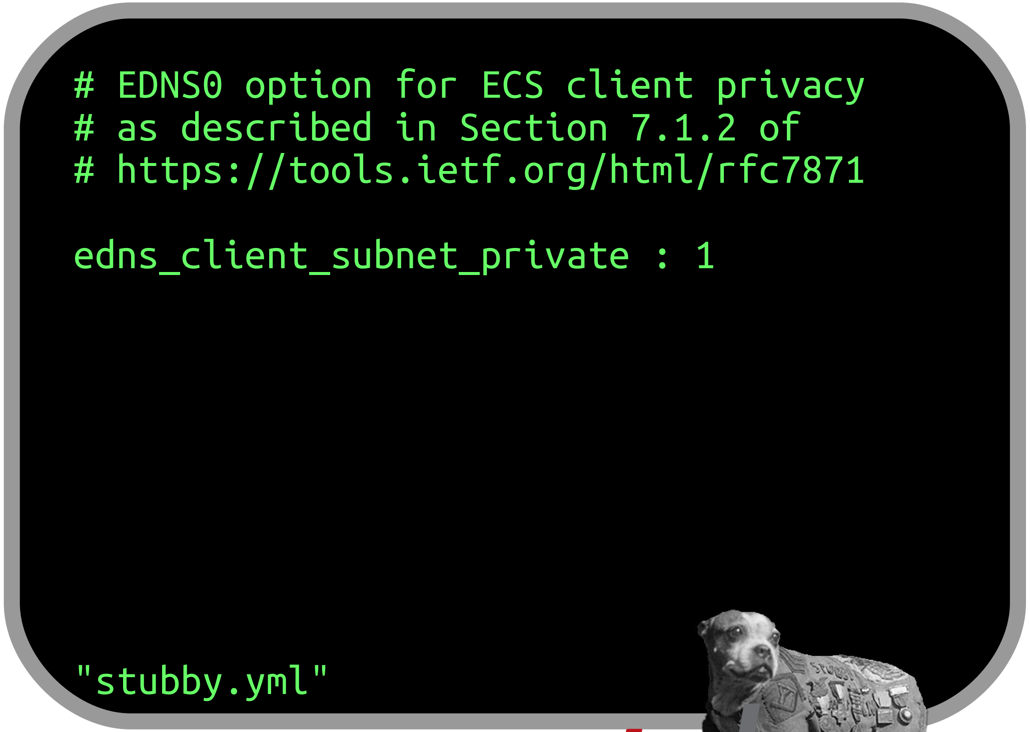
minimaliseer data in queries – ECS priv.

- RFC7871 -
  EDNS Client Subnet
  sectie 7.1.2:
  “ A SOURCE PREFIX-LENGTH value of 0 means that the Recursive Resolver MUST NOT add the client's address information to its queries. ”

unbound respecteert dit

- Google respecteert dit

OpenDNS respecteert dit niet



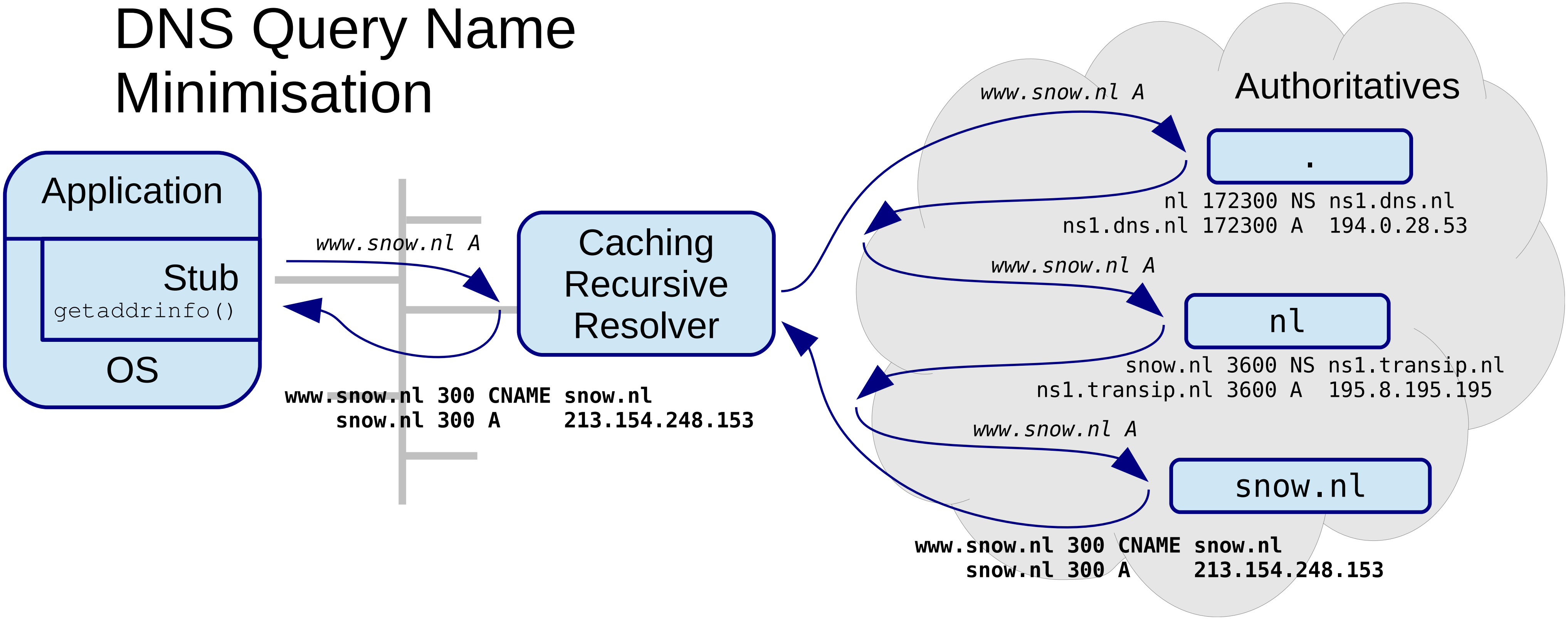
```
# EDNS0 option for ECS client privacy
# as described in Section 7.1.2 of
# https://tools.ietf.org/html/rfc7871

edns_client_subnet_private : 1
```

"stubby.yml"

Privacy issues met DNS

minimaliseer data in queries – qname min

- Zonder RFC7816 - DNS Query Name Minimisation



```
nl 172300 NS ns1.dns.nl
ns1.dns.nl 172300 A  194.0.28.53
```

```
snow.nl 3600 NS ns1.transip.nl
ns1.transip.nl 3600 A  195.8.195.195
```

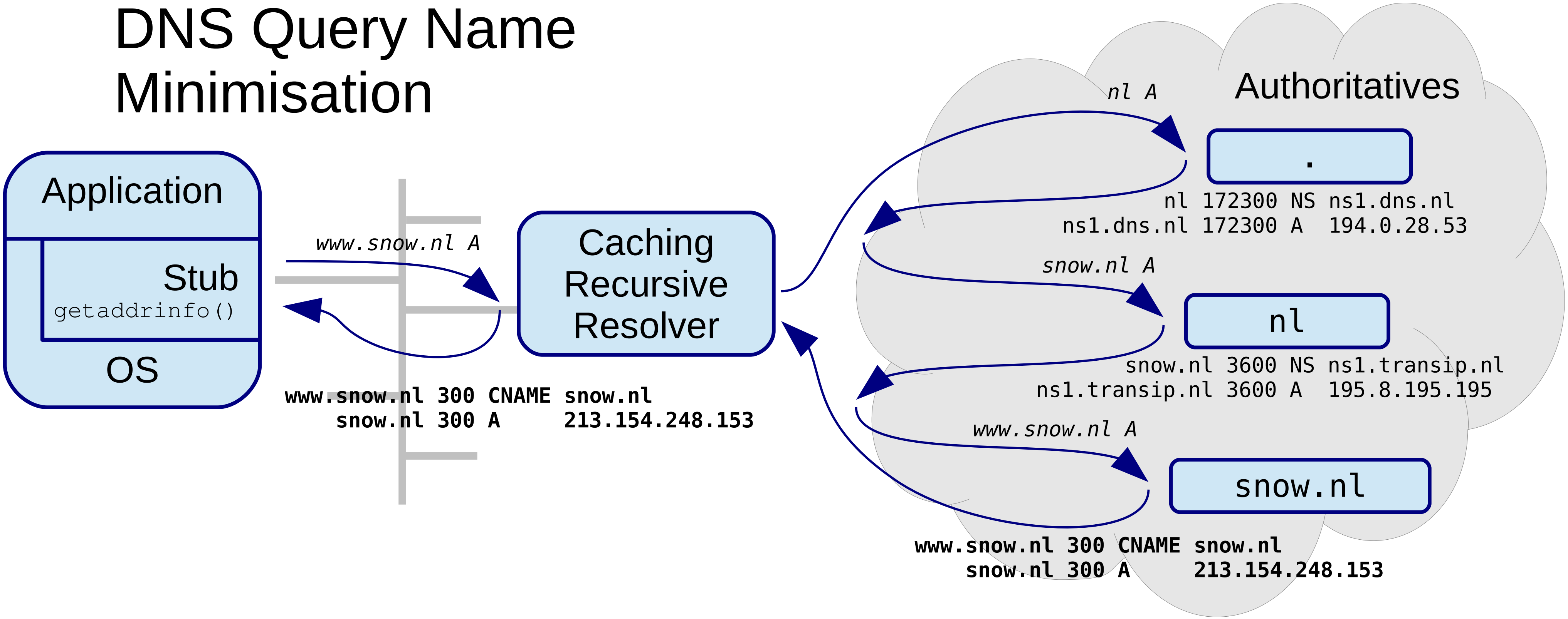
```
www.snow.nl 300 CNAME snow.nl
    snow.nl 300 A     213.154.248.153
```

```
www.snow.nl 300 CNAME snow.nl
    snow.nl 300 A     213.154.248.153
```

Privacy issues met DNS

minimaliseer data in queries – qname min

- Met RFC7816 - DNS Query Name Minimisation



```
nl 172300 NS ns1.dns.nl
ns1.dns.nl 172300 A  194.0.28.53
```

```
 snow.nl 3600 NS ns1.transip.nl
ns1.transip.nl 3600 A  195.8.195.195
```

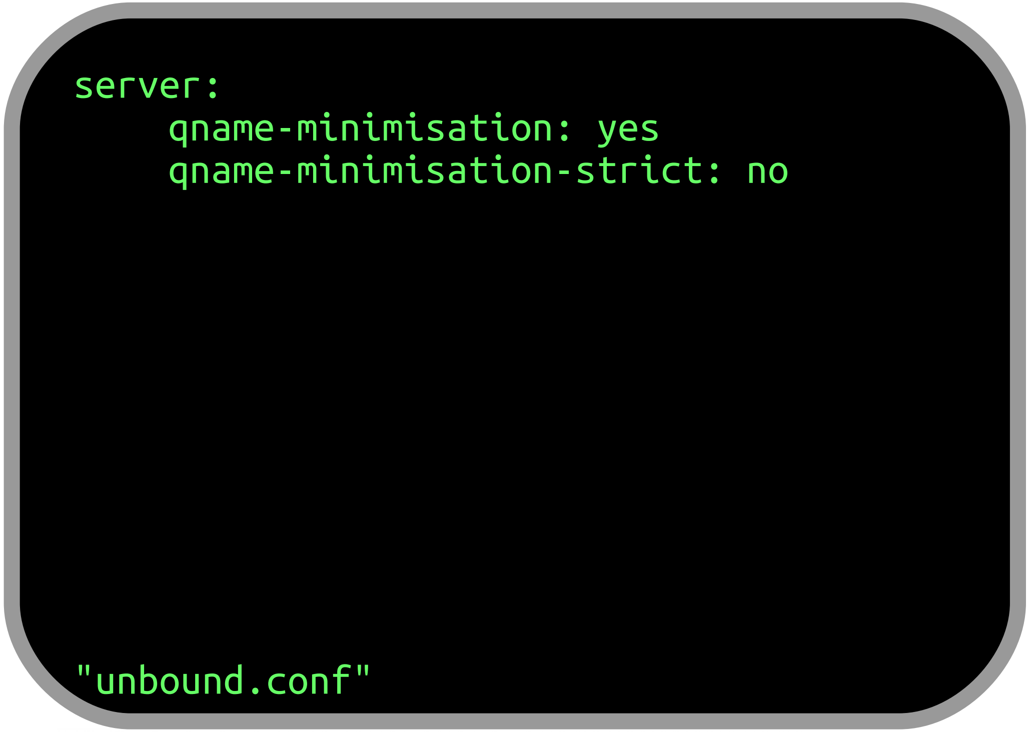
```
www.snow.nl 300 CNAME snow.nl
    snow.nl 300 A     213.154.248.153
```

```
www.snow.nl 300 CNAME snow.nl
    snow.nl 300 A     213.154.248.153
```

Privacy issues met DNS

minimaliseer data in queries – qname min

- RFC7816 - DNS Query Name Minimisation



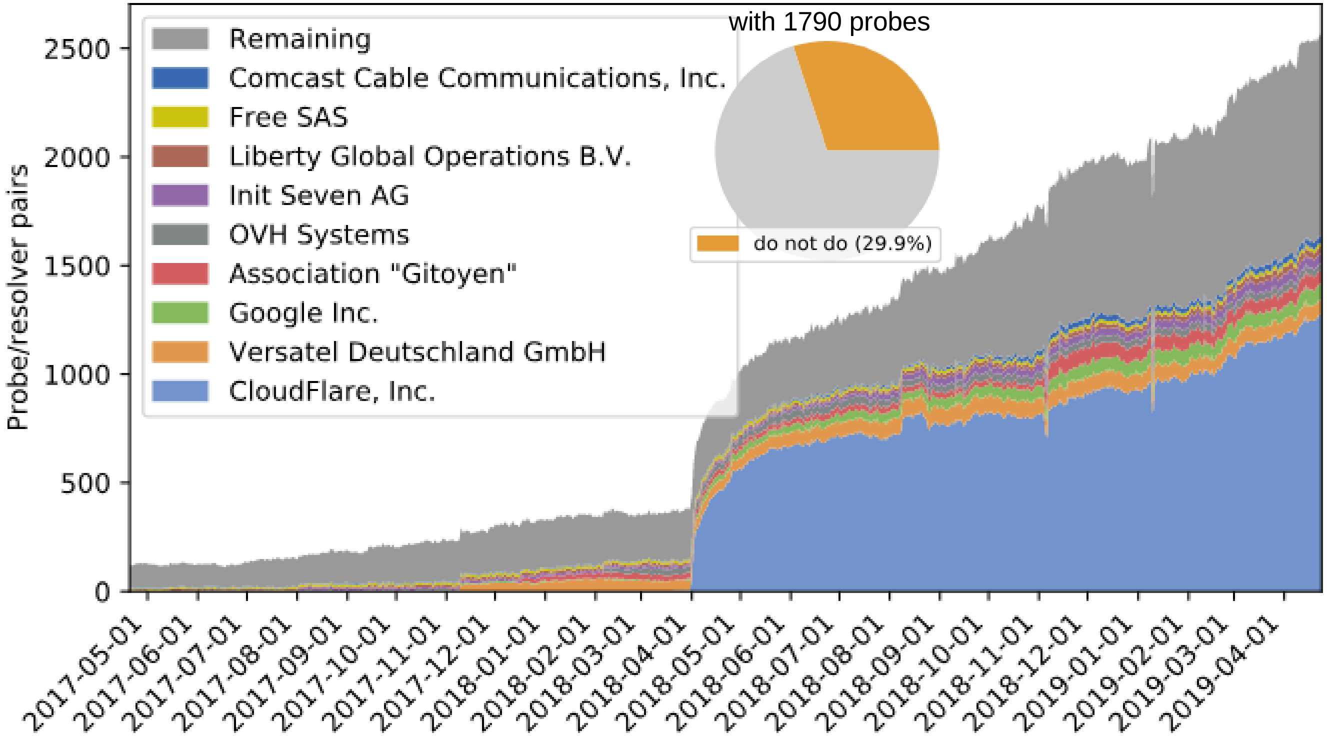
```
server:
     qname-minimisation: yes
     qname-minimisation-strict: no



"unbound.conf"
```

unbound

Privacy issues met DNS

minimaliseer data in queries – qname min

- RFC7816 - DNS Query Name Minimisation



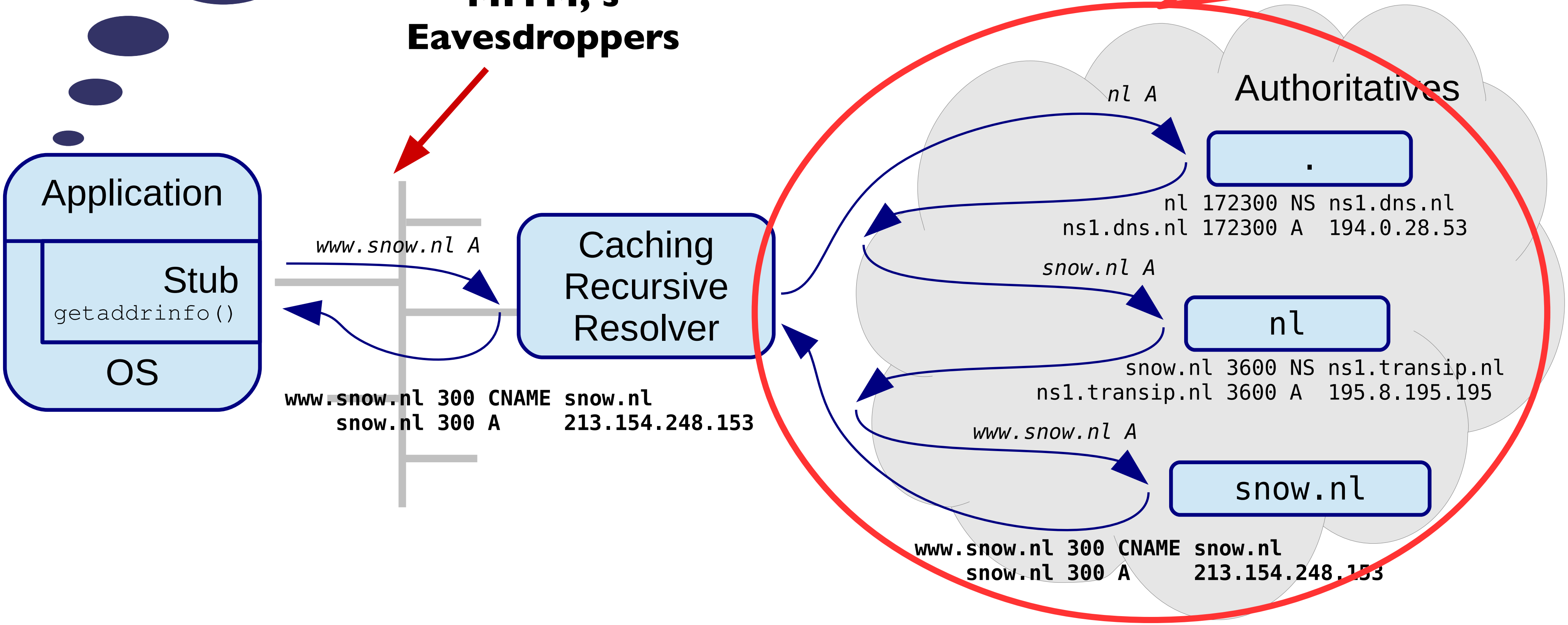
DNSThought

ITHI: 20.6% gemeten op de root

Privacy issues met DNS

Overal Encryptie

minimaliseer (data in) queries

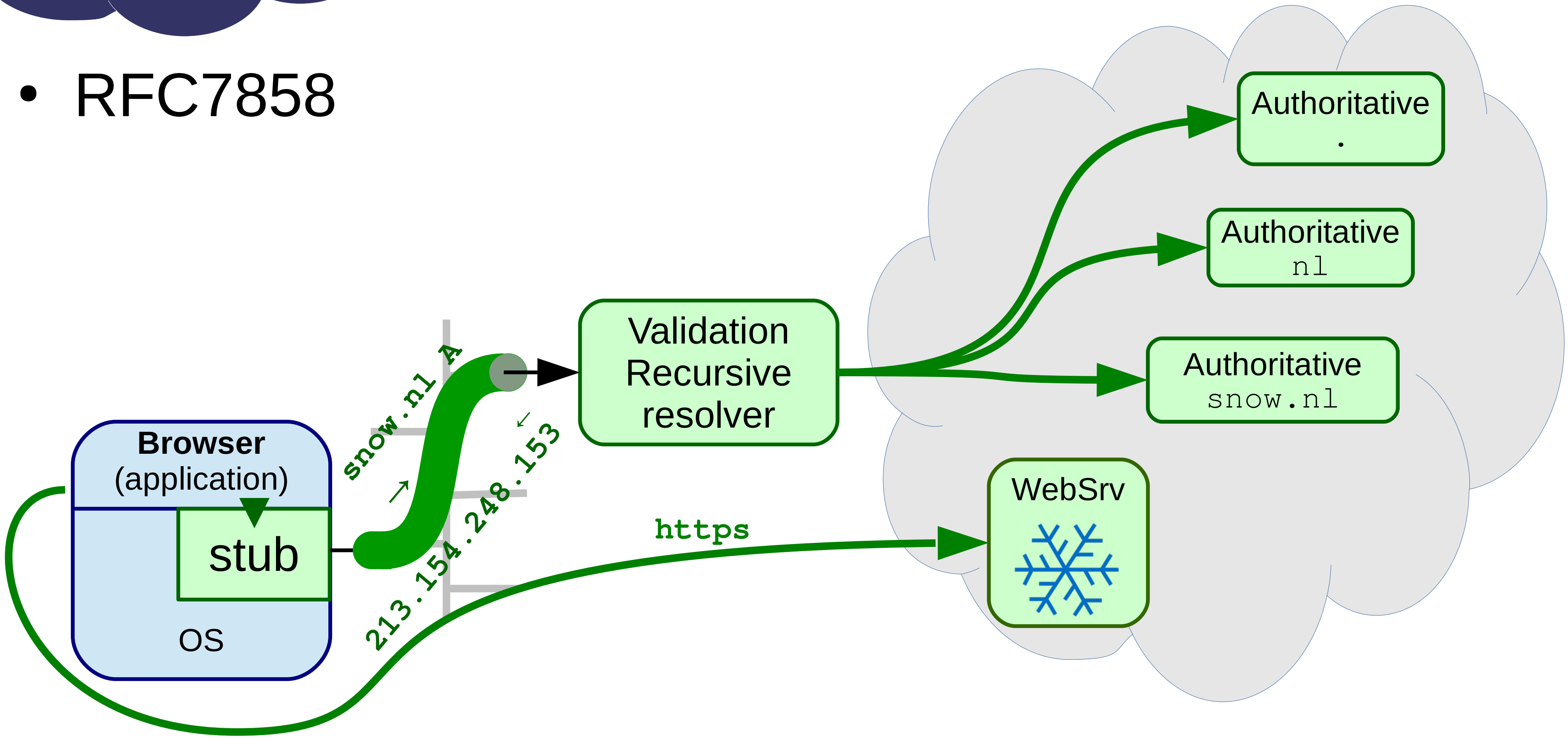

MITM, s
Eavesdroppers
Application
Stub
getaddrinfo()
OS
www.snow.nl A
www.snow.nl 300 CNAME snow.nl
snow.nl 300 A 213.154.248.153
Caching
Recursive
Resolver
Authoritatives
nl A
.
nl 172300 NS ns1.dns.nl
ns1.dns.nl 172300 A 194.0.28.53
snow.nl A
nl
snow.nl 3600 NS ns1.transip.nl
ns1.transip.nl 3600 A 195.8.195.195
www.snow.nl A
snow.nl
www.snow.nl 300 CNAME snow.nl
snow.nl 300 A 213.154.248.153

Overal Encryptie

Privacy issues met DNS

DNS over TLS (DoT)

- RFC7858

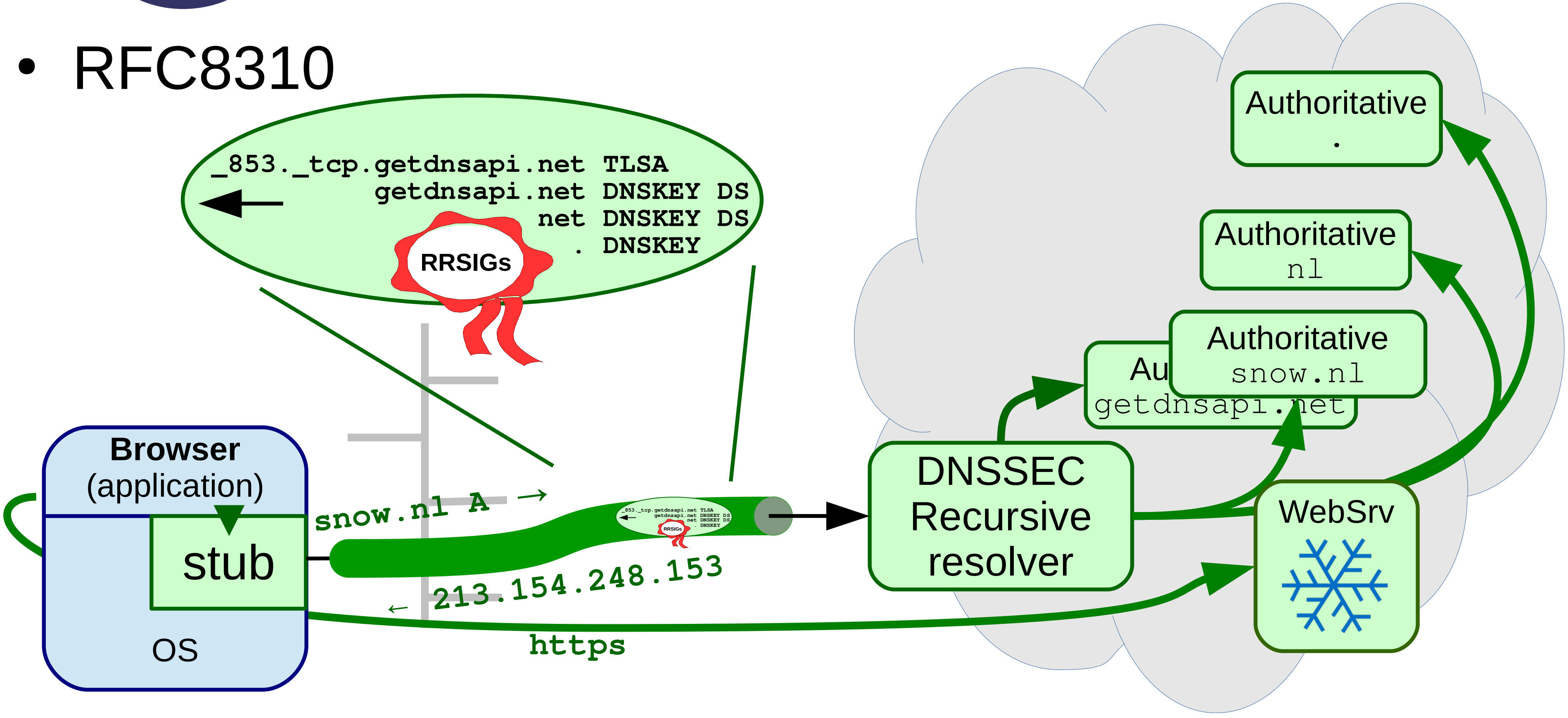


Overal Encryptie

Privacy issues met DNS

DNS over TLS (DoT)

- RFC8310



Overal Encryptie

Privacy issues met DNS

DNS over TLS (DoT)

```
server:
     tls-service-key: "privkey.pem"
     tls-service-pem: "fullchain.pem"
     tls-port: 853
```

"unbound.conf"

```
round_robin_upstreams: 1

upstream_recursive_servers:
## Quad 9
  - address_data: 9.9.9.9
    tls_auth_name: "dns.quad9.net"
## Cloudflare
  - address_data: 1.1.1.1
    tls_auth_name: "cloudflare-dns.com"
## Google
  - address_data: 8.8.8.8
   tls_auth_name: "dns.google"
```

"stubby.yml"

unbound

getdns

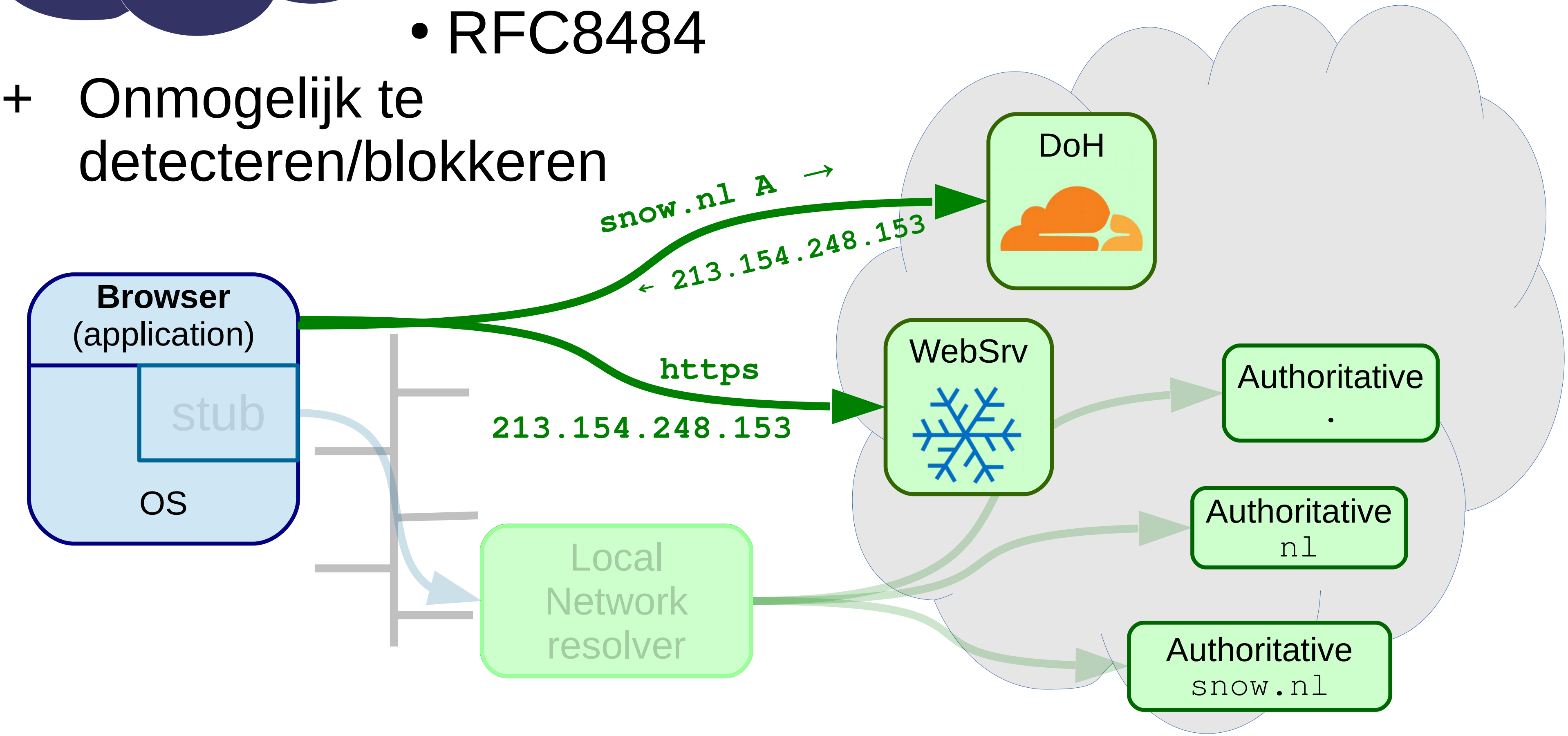
Overal Encryptie

Privacy issues met DNS

DNS over HTTPS (DoH)

- RFC8484

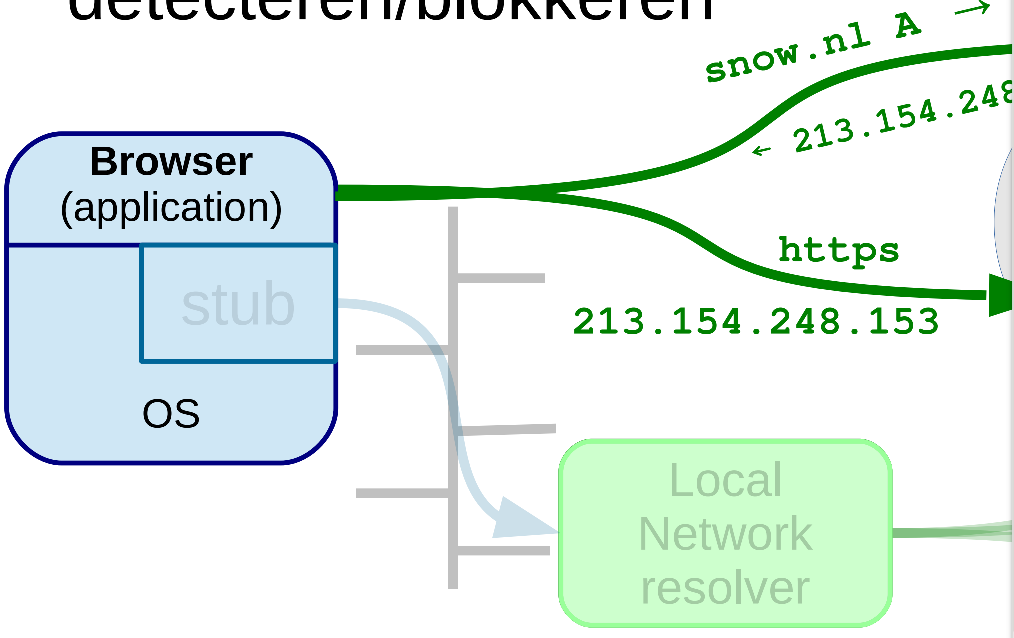
- + Onmogelijk te detecteren/blokkeren

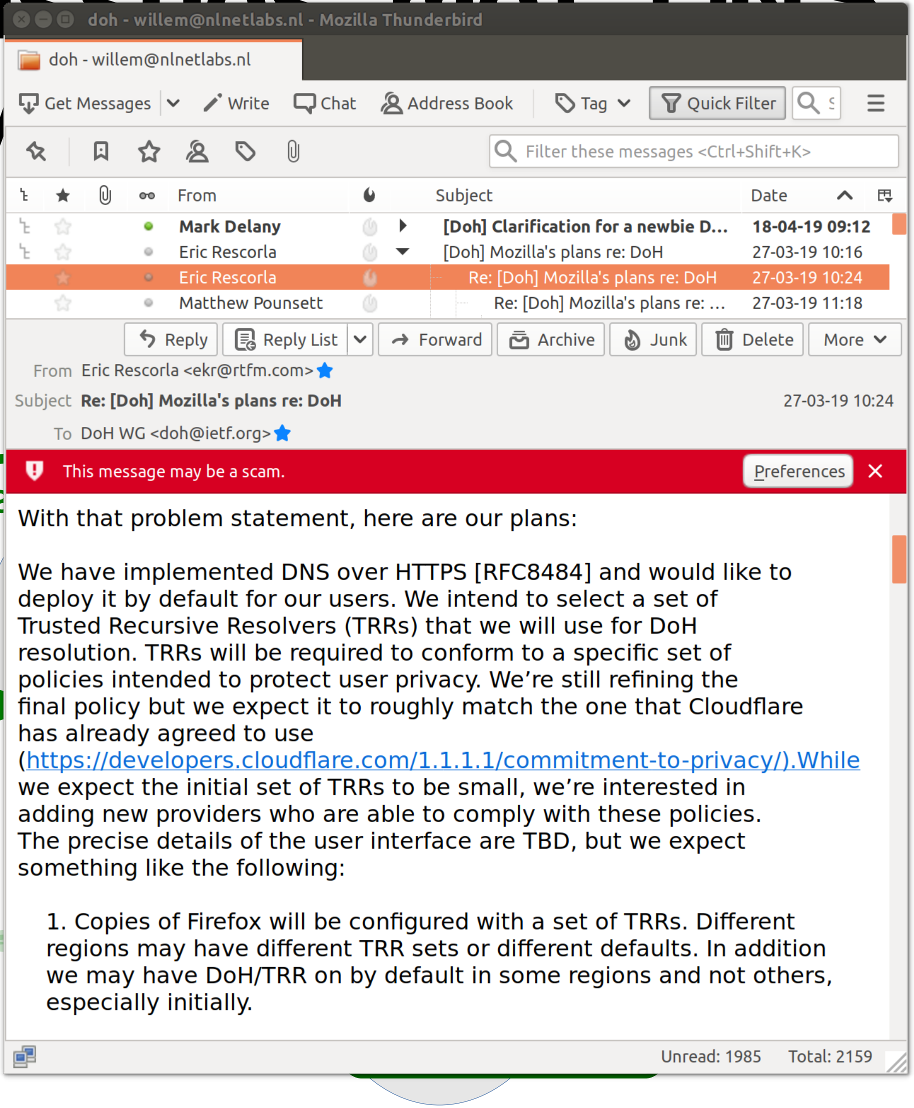


Overal Encryptie

Privacy issues met DNS
DNS ov

- RFC8484
- + Onmogelijk te detecteren/blokkeren





From	Subject	Date
Mark Delany	[Doh] Clarification for a newbie D...	18-04-19 09:12
Eric Rescorla	[Doh] Mozilla's plans re: DoH	27-03-19 10:16
Eric Rescorla	Re: [Doh] Mozilla's plans re: DoH	27-03-19 10:24
Matthew Pounsett	Re: [Doh] Mozilla's plans re: ...	27-03-19 11:18

From Eric Rescorla <ekr@rtfm.com>
Subject **Re: [Doh] Mozilla's plans re: DoH** 27-03-19 10:24
To DoH WG <doh@ietf.org>

This message may be a scam.

With that problem statement, here are our plans:

We have implemented DNS over HTTPS [RFC8484] and would like to deploy it by default for our users. We intend to select a set of Trusted Recursive Resolvers (TRRs) that we will use for DoH resolution. TRRs will be required to conform to a specific set of policies intended to protect user privacy. We're still refining the final policy but we expect it to roughly match the one that Cloudflare has already agreed to use (https://developers.cloudflare.com/1.1.1.1/commitment-to-privacy/).While we expect the initial set of TRRs to be small, we're interested in adding new providers who are able to comply with these policies. The precise details of the user interface are TBD, but we expect something like the following:

1. Copies of Firefox will be configured with a set of TRRs. Different regions may have different TRR sets or different defaults. In addition we may have DoH/TRR on by default in some regions and not others, especially initially.

Unread: 1985 Total: 2159

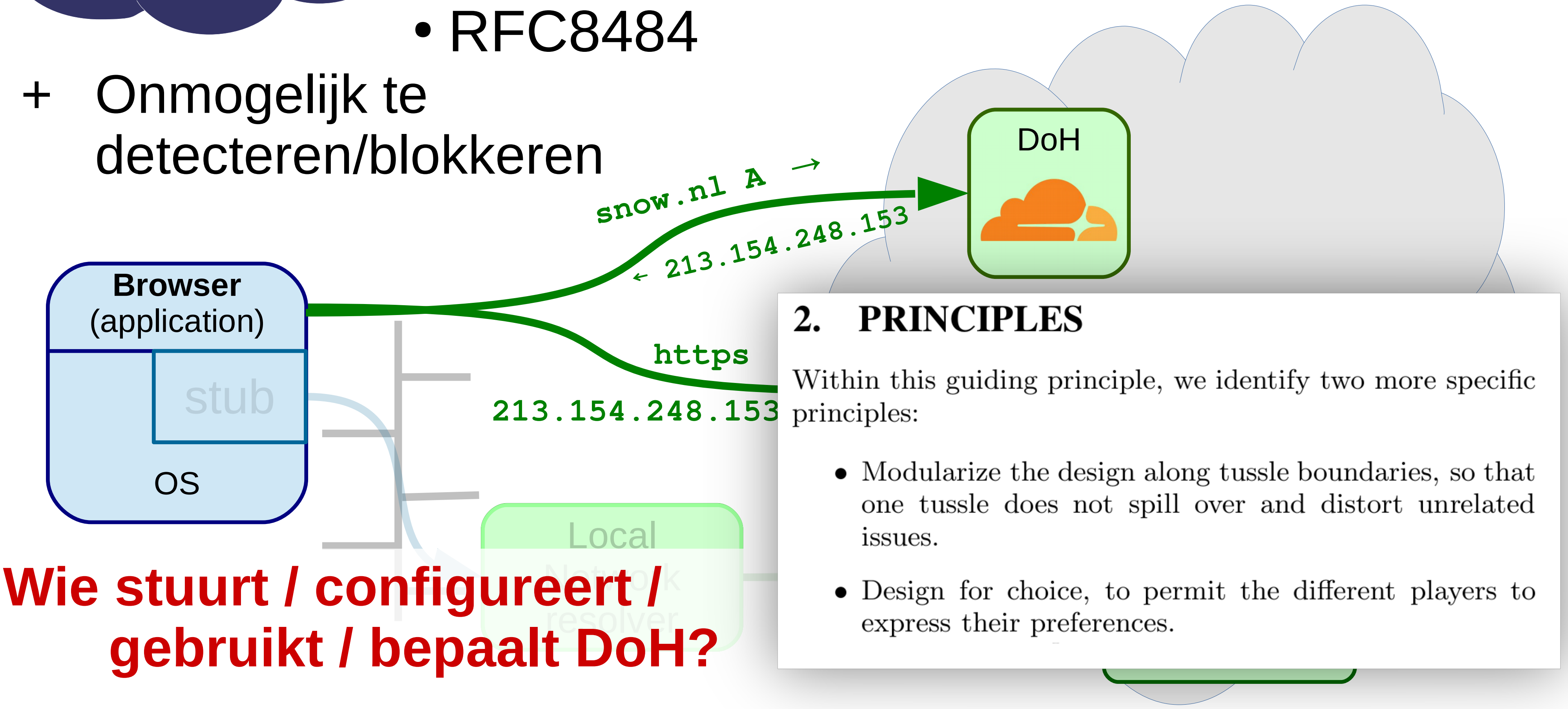
Overal Encryptie

Privacy issues met DNS

DNS over HTTPS (DoH)

- RFC8484

- + Onmogelijk te detecteren/blokkeren



2. PRINCIPLES

Within this guiding principle, we identify two more specific principles:

- Modularize the design along tussle boundaries, so that one tussle does not spill over and distort unrelated issues.
- Design for choice, to permit the different players to express their preferences.

- **Wie stuurt / configureert / gebruikt / bepaalt DoH?**

Mmm..
D'OH...
NUTS!
DONUTS
MATT GROENING