

IETF Hackathon DNS protocol evolution

IETF 118
4–5 November 2023
Prague, Czech Republic



Hackathon Plan

- Solve assorted DNS protocol problems!
- Get smart people together ... and ... discuss!

Zone cut improvements

Notes from discussion:

Ellen Schachter

- Segment ADs/T branching on the parent side & EDNS0 extensions to propagate it
- Mapbox submitted as a DSDV/DZ record that provides:
 - NS/CL/RRSIG records for child TLDs (maps up info for ADs/T)
 - NS/CL/RRSIG follows many requirements, much PUBLISH can have independent DSKEYs
- Liberal: "I don't keep the records segregated like NS/CL/RRSIG. One record should contain the full name, address, capabilities, "N...". And if there are multiple clients, each NS can have different capabilities and properties."

Hall Walker

- Zone Cuts: We need to define what is authentication at the child and what is authentication at the parent. NS with a failure we can't let happen again. Not sure on glues, but having an IVC/RR type record would help here.
- I like the idea of delegation records. It would be nice to receive them from the parents during delegation. Child information on the PUBLISH is irrelevant.
- I very much would like something like NS2 that we had for secure delegation, but open to other technologically sound types given that they follow the above principles.

• The "tiny thoughts" of how to implement/extend EDNS to always have to handle "delegation":

- currently we expand NS+glue+sigv4 EDNS as needed
 - we need a delegation record that handles delegation names, addresses, of all PUBLISH capabilities. TLD needs, recursively EDNS
 - delegation record (or delegation record set)
- possibly (a client will) EDNS/T
- we need clearly established processes: how old update parent's delegation records?
- there are still discussions if "secure" or "secure", mapbox forced to either? In the end, keep one **glue** into EDNS (and not side-channelized outside of EDNS) for better

• One new delegation record signaling EDNS/T capability of the delegated nameservers has already been proposed in the IEDR, similar to EDNS.

• I like the idea of new query type! Or a new query CL/RRSIG? Or just an EDNS option?*

Liber Peleg

- EDNS test + zone iteration might be of value to something used elsewhere and more structured, e.g. (EDNS4,EDNS999), but in CR it keeps the current
- Change of name: Ellen Halle
- EDNS/T or EDNS/ADL: distinguishing meaning of transports
 - EDNS or EDNS/T: transports is needed when proxy compression should be used as the private transport (ADL, local site)
 - Webcams are not cameras. Open question: are there being a media browser or not
 - Much improved servers, and in particular clients, use SRV/PALM, or only/translate in somehow similar to IEEE 1905 HTTP/JSON standard
- Name now is not clear. I think it's better to change. Good question has a specific answer and a question - E.g. "Who is the A resource for www.example?". There is one AAAA record for www.example". "Who is not authentication for www.example?". This is not answering your 10k question as that's too many". These answers would also be measured more explicitly than in the DNS. E.g. in the case of "The name you asked about has some data, but no data of the type you asked about" would be a typical "NOOPRRSIG" result, not inferred from "no name code" or "no answer". "Registration authority for ns1.com" vs "Registration authority for ns1.com".

• Transport should be **EDNS**: Clients get security labels and use them when needed. DnsID is used for pricing/discovery towards auto discovery address.

- Liber: I don't like DnsID. Pricing has to be avoided by proper delegation mechanisms.

• Another point on transport: multiple compressors possible (transport-level compression/T optimization) - verification of functionality.

- Local network transport over local TLS by static receivers:
 - Liber: why not. DnsID an issue?
- Using DnsID allows message sizes increased by a lot

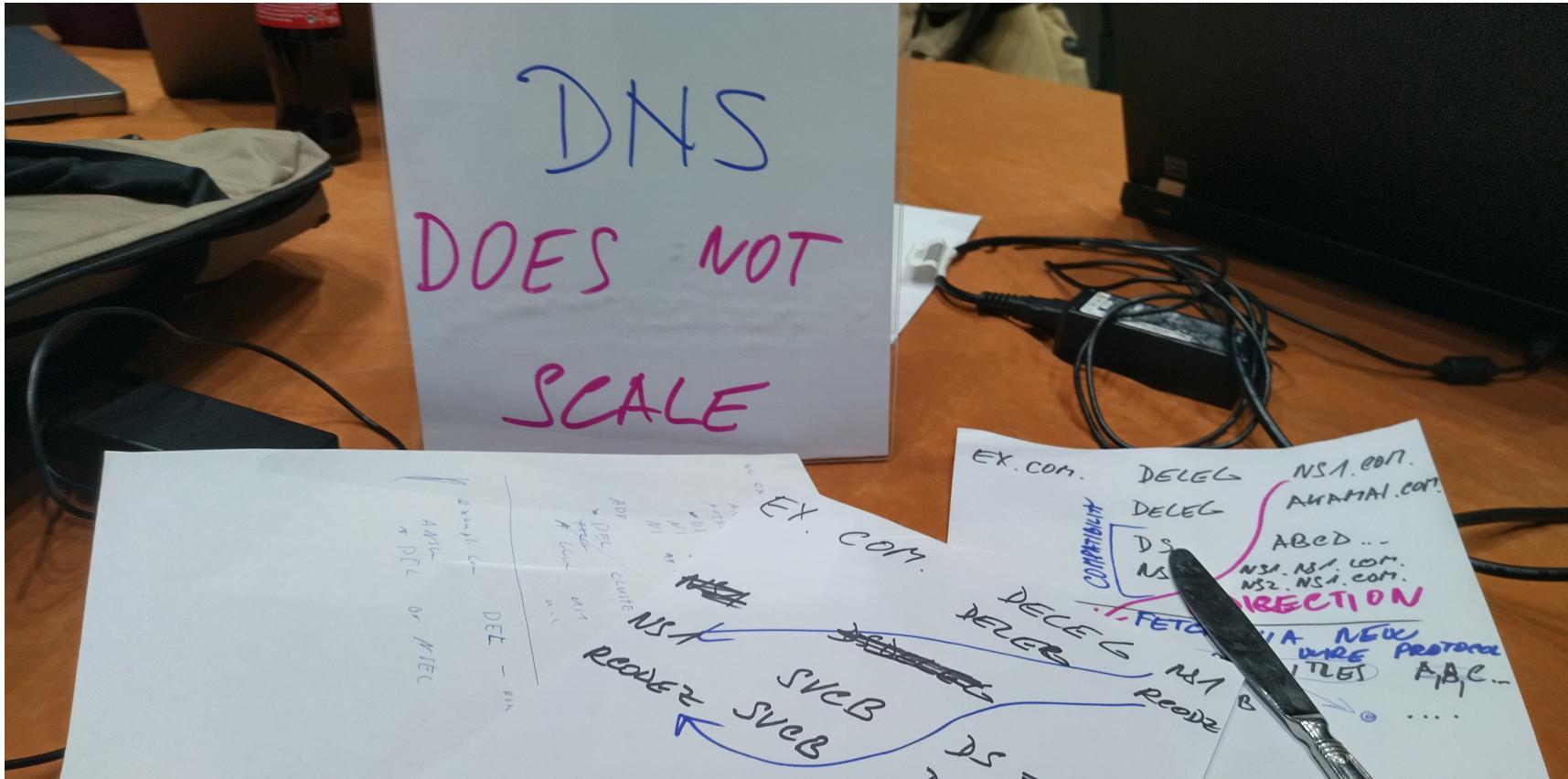
• Up (+ Mixed Label collaging)

• Only encrypted transports

• DnsID need to protect Range?

- 6 pages of problems

What got done



What got done

- RESINFO implementation for BIND
- NOTIFY for CDS/CDNSKEY scans
- "Mechanism for Diversion"
from Legacy DNS to a New DNS Protocol
 - Protocol proposal ... on a napkin – work-in-progress
 - Extension to DNS delegation mechanism
- example.com. NS nameserver.example.net.
- **example.com. DELEG configset1.example.net.**
- **configset1.example.net. SVCB ... parameters here ...**

What we learned

- We can't evolve protocol without extending **parent side** of DNS zone cut
- Backwards-compatible evolution is possible if we extend the DNS delegation

Wrap Up

Team members:

Andreas Shulze

Andrew Fregly

Christian Elmerot

David Blacka

David Lawrence

Edward Lewis

Evan Hunt

George Michaelson

Jan Včelák

Klaus Darilion

Libor Peltan

Matthijs Mekking

Mark Andrews

Petr Špaček

Ralf Weber

Shane Kerr

Shumon Huque

Tamas Csillag

Vandan Adhvaryu

Vladimír Čunát