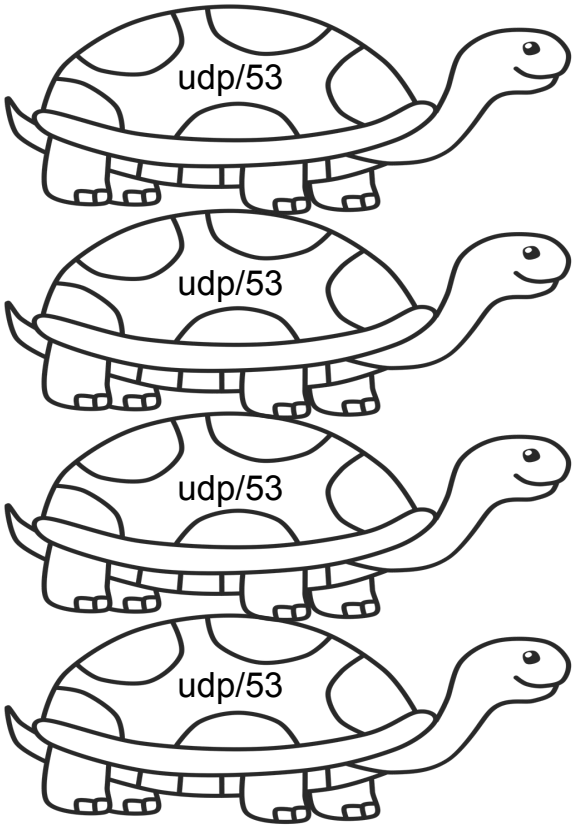
DELEGations++

Tim April, **David Lawrence**, Petr Špaček, Ralf Weber

RIPE 87 – Rome,Italy | dns-wg | 29 Nov 2023

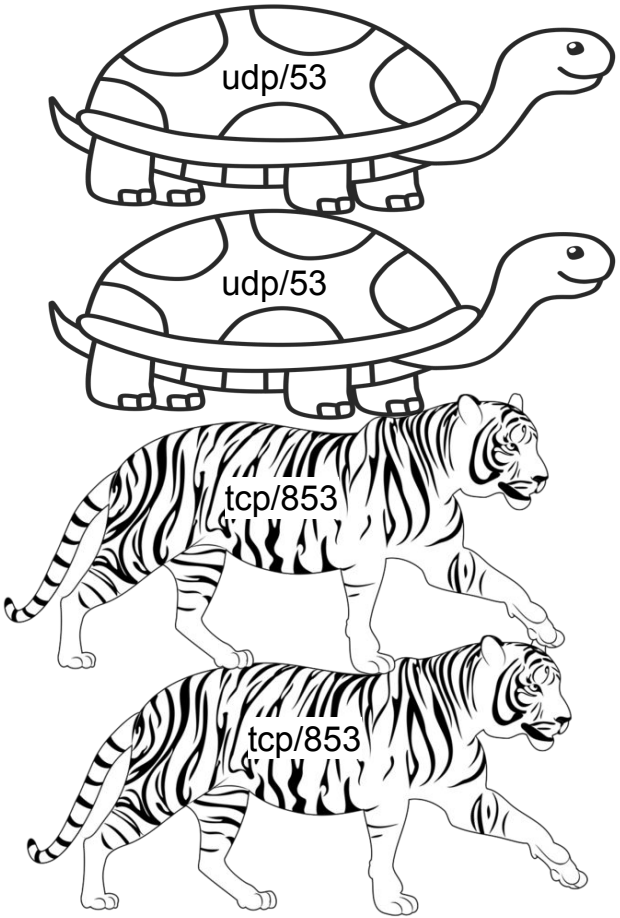


.

uk.

co.uk.

example.co.uk.



.

uk.

co.uk.

example.co.uk.

Introducing DELEG

example.com. 86400 IN DELEG 1 ns1.example.com. *SvcParams*

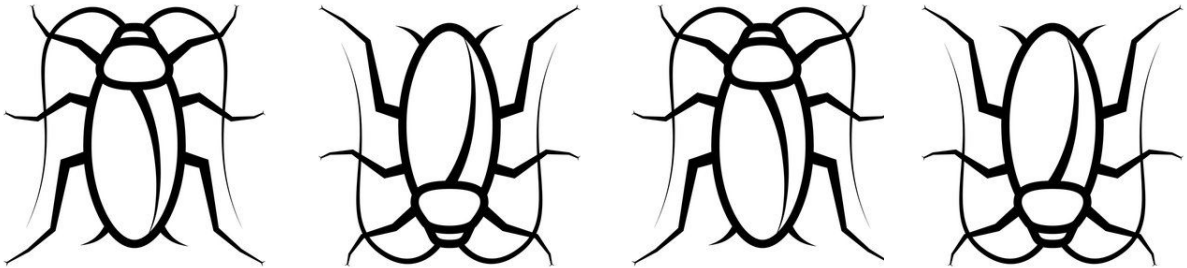
But first, a clarification on metaphor…

The turtle versus tiger comparison is admittedly unfair.

The Domain Name System has been one of the most successful, decades-old Internet protocols.

It lies at the start of a gazillion* connections.

Adaptable, efficient, and far more resilient than “It Was The DNS” memes would have you believe, but …



… yecch

*real number, totally supported by actual research

A brief history

Petr Špaček convened a brainstorming session at the recent Prague Hackathon.

The goal: Wish Big on DNS evolution
Maybe even a whole new protocol!
What the suits would call a “BHAG”

Quickly coalesced on a core idea:

For any BHAG to succeed, it needs
Low-friction incremental deployability
AND
It cannot break the legacy DNS

So, how could we easily let resolvers know that they can switch to A New Way of doing things?

So, DELEG

We re-invented Tim April's NS2 proposal from 2020, modeled on the new Service Bind (SVCB) record. Here is its simplest form as it *might* appear in a delegation response:

```
; <<>> DiG <<>> example.com @f.gtld-servers.com
;...
;; AUTHORITY SECTION:
example.com.          172800  IN     NS     ns1.example.com
example.com.          172800  IN     NS     ns2.example.com
example.com.          86400   IN     DS     370 13 2 BE735995...
example.com.          172800  IN     DELEG  1 ns1.example.com (
                      ipv4hint=192.0.2.1 ipv6hint=2001:DB8:abcd::1 )
example.com.          172800  IN     DELEG  1 ns2.example.com (
                      ipv4hint=198.51.100.1 ipv6hint=2001:DB8:1234::1 )

;; ADDITIONAL SECTION:
ns1.example.com       86400   IN     A      192.0.2.1
ns1.example.com       86400   IN     AAAA   2001:DB8:abcd::1
ns2.example.com       86400   IN     A   198.51.100.1
ns2.example.com       86400   IN     AAAA   2001:DB8:1234::1
```

DELEG’s key features

- Opportunistic discovery, during normal resolution flow
- Transparent to legacy resolvers
- Extensible with key=value pairs
- Parent-side record ONLY
- Minimal implementation for authority servers
- No special/additional processing by authority
- Indirection for operations management
- Allows legacy DNS in sub-delegations

Indirection?

Yes, like SVCB's AliasMode, using a special priority of 0.

```
; .com zone
example.com.  86400  IN DELEG  0 config2.example.
example.com.  86400  IN RRSIG  DELEG 8 2 86400 20231203063732 …

; .example zone
config2.example. 3600    IN SVCB 1 . (
                ipv4hint=192.0.2.1,198.51.100.1
                ipv6hint=2001:DB8:1234::1,2001:DB8:abcd::1
                ds="53059 8 2 F43A22…" )
```

Operators will be able to change delegation information without additional registrar interaction by customers. Notably, DS key data can be updated and the signature chain maintained through the operator's DS. It will also enable …

Alternative transports, now more accessible

DoH, DoT, DoQ have all been standardized, but

HOW DO YOU FIND THE SERVERS?

¯_(ツ)_/¯

Currently: additional configuration from out-of-band information, or additional lookups

Soon:

```
example.com. 86400 IN DELEG 1 ns1.example.net. (
    alpn=dot tlsa="3 0 0 2dc74f…" )
```

To infinity and beyond!

```
example.com. 86400 IN DELEG 1 ns1.example.net dnsproto=2
```

Lots of ideas in the BHAG list

Many would benefit by being unshackled from the constraints of Legacy DNS

Imagine:
a new wire format

better zone synchronization

a fully-secured DNS PUSH that you could trust across domains

Proposal to the IETF imminently

https://github.com/fl1ger/deleg.git

draft-dnsop-deleg.md – Core definition

draft-dnsop-deleg-transport.md – Alternative transport layers

draft-dnsop-deleg-dnssec.md – Secure indirect delegation

We'll also need an EPP draft for the regext group,
documenting the registry/registrar update path

Initial support from a broad cross-section of the DNS community

Vandan Adhvaryu, Tim April, David Blacka, Manu Bretelle,
Vladimír Čunát, Klaus Darilion, Peter van Dijk,
Christian Elmerot, Philip Homburg, Shumon Huque,
Shane Kerr, David Lawrence, Ed Lewis,
George Michaelson, Erik Nygren, Libor Peltan,
Ben Schwartz, Petr Špaček, Jan Včelák, Ralf Weber

Also socialized outside the DNS sphere, with notable interest from web folks

Still need to test and discuss

- Is the assertion about legacy resolvers ignoring it accurate?
  - Believed to be true about BIND, Knot, PowerDNS and Unbound, yet still needs confirmation
  - What about djbdns, MaraDNS, Technitium, others … ?
  - How do existing forwarders/validators handle it?
- Should do53 be explicitly required when desired via DELEG?
- Any conditions for returning or eliding DELEG?
  - Only if, eg, rd=0 + EDNS(0)?
  - Except when qtype=DELEG, or qtype=ANY depending on ANY policy?
- Allow sideways delegation when parent doesn't implement?
  - Some TLDs are notoriously slow with any DNS development
  - Could be something like a SVCB in auth for queries received on port 53?
- Usual bike shedding.

The Why Game, courtesy of my family

Why are you going to Italy?
To give a talk.
Why?
To promote a new way for the DNS to work.
Why?
We want to make the Internet work better.
Why?
For the betterment of humanity!

Okay, The Why Game eventually ends in nonsense.

Or not, because the work you all do is used by hundreds of millions of people every single day.
Jury is still out on whether this whole Internet thing was really a good idea or not, though.

Qs and Comms?