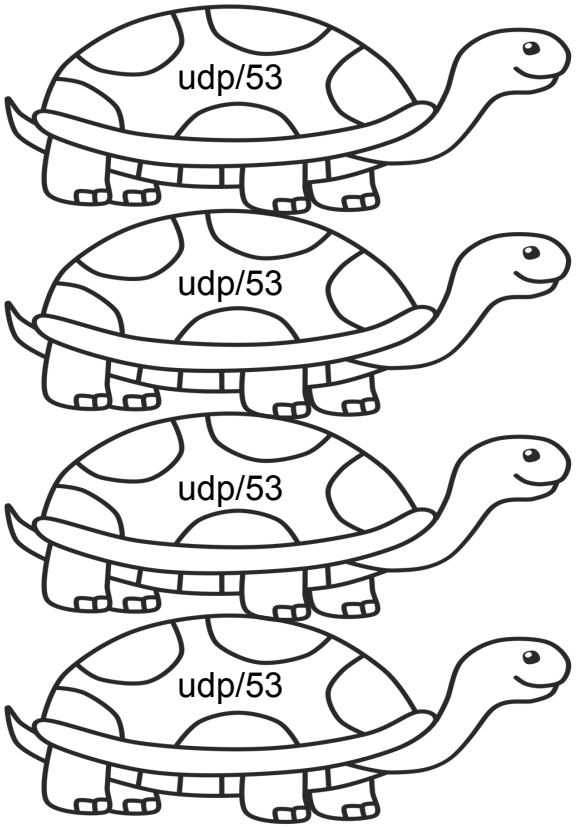
DELEGations++

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

NANOG 90 – Charlotte, NC, USA | 13 Feb 2024

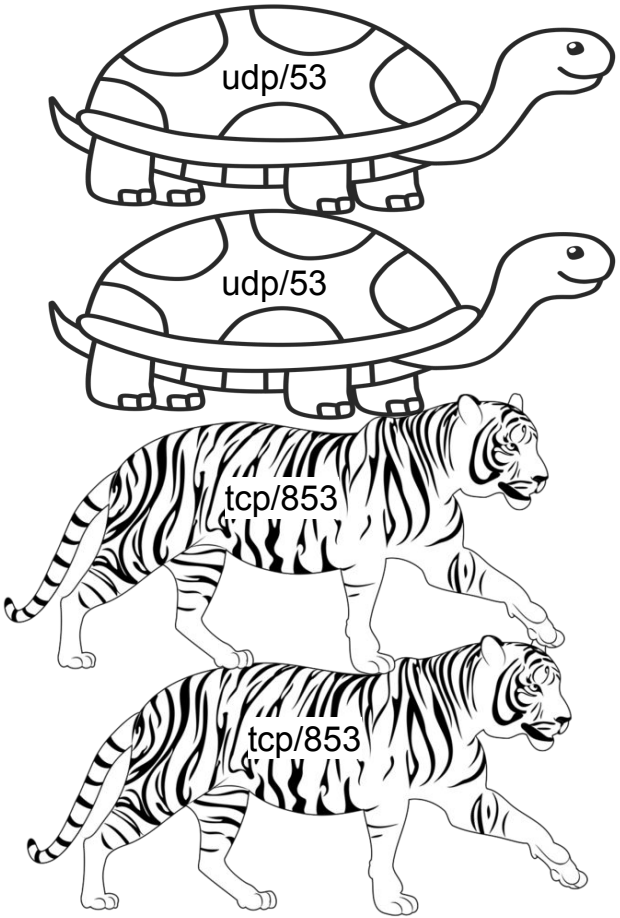


.

uk.

co.uk.

example.co.uk.



.

uk.

co.uk.

example.co.uk.

Introducing DELEG

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

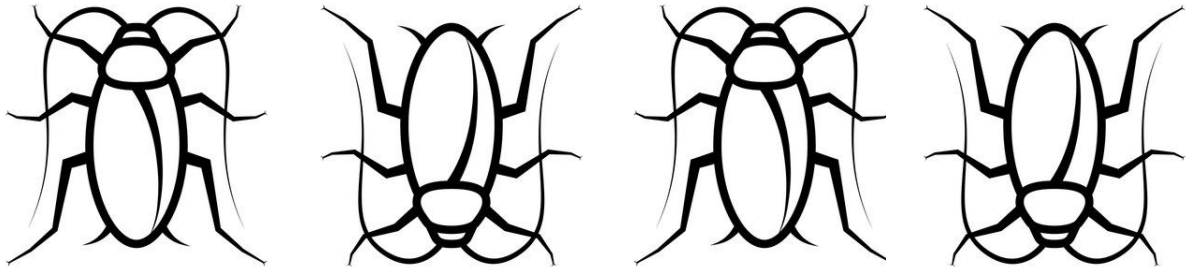
But first, a clarification on metaphor…

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

(PS: it was really BGP.)

A brief history

Petr Špaček convened a brainstorming session at the November 2023 IETF Hackathon. The goal: Wish Big on DNS evolution.

Maybe even a whole new protocol! 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.

How could we easily let resolvers know that they can switch to A New Way of doing things? EDNS option negotiation? Globally scoped special names?

Enter DELEG

We re-invented Tim April's NS2 proposal from 2020, modeled on the new Service Bind (SVCB) record. Here is how DELEG in its simplest form *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
```

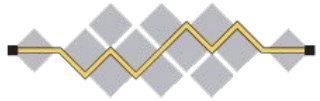
Lots of ideas in the BHAG list

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



Core definition submitted: draft-dnsop-deleg-00
Registry/Registrar protocol support: draft-brown-epp-deleg-00

Discussion on the core proposal active in the dnsop working group
Virtual interim, with minutes, was held on 30 Jan 2024

Birds-of-a-Feather at IETF 119 in Brisbane

Document development: 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

Issue comments and pull requests welcome!

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

Vandan Adhvaryu, Roy Arends, 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 this even the right approach? The DNS Camel rears its unruly head.
- Test more legacy resolvers for compatible behavior
  - Already confirmed BIND, Knot, PowerDNS and Unbound
  - Also works with major open resolvers: Cloudflare, Google, Quad9
  - What about djbdns, MaraDNS, Technitium, others … ?
  - Does any of this matter for DNS forwarders?
- Should do53 be explicitly required when desired via DELEG?
- Should there be any conditions for returning or eliding DELEG?
  - Initial testing suggests it isn't necessary, but what if a broken legacy resolver is found?
- 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

Qs and Comms?