The Changing DNS Market: A Technical Perspective

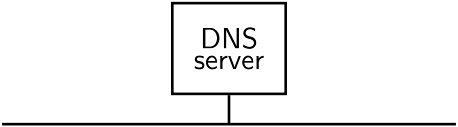
Johan Ihrén
Netnod

October 26, 2016

Once upon a time DNS was simple

In the early days, DNS was not considered a “problem” (but rather a solution)

- the only thing needed was “the DNS server”
    - of course it was both authoritative and recursive
- everyone behaved nicely (at least regarding DNS)
- for a long time there was often only one server and only one implementation



Once upon a time DNS was simple

In the early days, DNS was not considered a “problem” (but rather a solution)

- the only thing needed was “the DNS server”
  - of course it was both authoritative and recursive
- everyone behaved nicely (at least regarding DNS)
- for a long time there was often only one server and only one implementation (`BIND4.7.2beta26` if I remember correctly)

However, things went south over time:

- good guys started doing bad things (split-DNS, strange forwarding setups, policy-based responses, lots of rope everywhere)
- bad guys showed up doing bad things (also with DNS)

The major reason that DNS is becoming a “problem” is that there is not sufficient revenue to match the increasing cost of operation.

Changes

During the last few years a number of changes, some technical, some not so technical, have been propagating through the DNS community.

- DNS Anycast has become a staple technology
  - root, TLDs and also Enterprises
- DDOS attacks have become a routine issue
- Static configurations are disappearing
- More and more "behaviour modifying" features outside the DNS protocol are used to tweak responses in various ways
- System complexity is exploding

Changes: Dynamic Configurations

DNS is migrating from a static service (or set of services) that is configured via a static config file to a dynamic service that is configured in “other ways”:

- configuration via database
- configuration via APIs
- scriptable configs with CLI access to the nameserver

Interestingly, two of the most interesting new recursive servers (PDNS Recursor and Knot-DNS Resolver) provide high-level scripting of configs via built in Lua support.

- while I’m all for Lua, it is clear that being able to script entire new functions that modify the server behaviour... will be used in creative ways
- also, this breaks the old assumption that server behaviour can be understood from the “config file”. Now there’s a “running” config and a “written” config and they can be different

Changes: Emergence of “DNS APIs”

The DNS space consolidates. Fewer providers provide service for vast numbers of zones (authoritative service) or vast numbers of users (recursive service), but always with vast numbers of servers. In practice, the configuration file is disappearing

- sorry to have to break it to you, but the days of manual hacking of **`named.conf`** are over (no regrets. . .)
- today a requirement on DNS service is “API access”

What is that? Well, there are

- provisioning APIs (adding and removing zones, modifying content of zones, etc)
- stats APIs (returning statistics and sometimes pretty graphics)
- management APIs (managing servers, modifying policies, etc)

With the APIs follow new needs for authentication, etc

Changes: Behaviour From Policy, Not Zone Content

Another major change in DNS service is the increasing breakage of the assumption that the contents of the zone defines the answer that the stub resolver (i.e. the end user) should get.
There are an increasing amount of policy knobs in the authoritative space:

- geography-based responses, multiple levels of split-DNS (now also with DNSSEC), etc

And even more in the recursive area:

- RPZ (response-policy-zones)
- all sorts of local overrides that modify the response received from the authoritative servers
- loadable modules and scripting support specifically designed for reponse modification

Recent Market Changes

All of the above are mostly technical changes

- there will always be technical changes, and the good ideas propagate while the bad ideas (hopefully) die out before they spread too far.

What about market changes?

Well, there is one massive change happening right now:

The cost for anycast service has now reached a price level where it is becoming very difficult to make a business case for "DNS service"

- unless the volume is really large. . .
- . . . and the coverage is global

What will the consequences of this change be?

Market Penetration Thresholds Are Interesting Things

History is full of examples where "change" started gradually. . . but when it reached a certain threshold there was a cascade effect

- at first only a few, wealthy, families had phones. . . but when a threshold was reached everyone had to get one
- at first only geeks and university students had email. . . but when the threshold was reached everyone had to get email
- . . . cars, Internet access, credit cards, etc, etc

At some point we will reach a threshold where basically everyone

- zone owners, registrars, web and email hosting providers, etc

switch to DNS service from a dedicated DNS provider rather than fiddling with a bunch of servers on their own

- I believe that we are very close to that point

Advantages of Anycast For Everyone

- The market will inevitably become more “professional”
- The general quality of the DNS name space will increase and the number of outages and issues will decrease
- General DDOS resilience will increase (although no one with a sane mind will be willing to guarantee ability to withstand a large attack)
- Outages due to “the nameserver is broken” will mostly disappear as a source of problems
  - but other sources like broken zones, etc, obviously remain
- Previously hidden brokenness (like broken zones) is exposed

Zone Quality

On our recently launched Enterprise platform we immediately saw “broken” customer zones

- the zone transfer from the customer master to our distribution infrastructure fails, because our nameservers refuse to accept the broken zone
- that such broken zones exist at all is likely a sign of old name server software (that doesn’t do sufficient correctness verification)
- in the short run it is a problem for the customer relation

However, in the long run it is good that these broken zones get detected and fixed, as this will improve quality of the overall DNS name space

- . . . assuming, of course, that they **do** get fixed

Disadvantages of Anycast For Everyone

- Smaller providers will be edged out of the market
- The cost (to the remaining providers) of moving all the data for millions of zones of minor importance to lots of servers around the world will be. . . very difficult to recover
- The problem definition will change from “the nameserver is broken, we need to fix it” to “how do I achieve XXX via the API from DNS provider YYY?”
    - i.e. there is a change of prblem space from “community” (open source nameserver configuration) to “proprietary” (support for that particular vendor API)
- One source of problems (configuring and operating nameservers) is replaced by another (integration of the various DNS provider APIs)
    - which requires a mostly new skill set in the community

Risk Of Mono Culture? Closed Source?

DNS has a long tradition of relying on open source implementations. Most of the major implementations (BIND, NSD, etc) have always been open source.

- there is also a large “fringe” of mostly open source nameservers, with various quirks and feature.
- it is certainly a rich culture (despite the huge BIND user base)

Will a rapid migration towards professional DNS services provided by a limited number of providers change this?

- probably yes (as in some implementations will die), but not enough to make the risks of mono culture a real concern

My concern is instead the trend towards closed source implementations that implement various extensions to DNS as a means to distinguish themselves from the competition

Risks Of Consolidation Into a Small Number of Major Providers

Last weeks attack against one of the major DNS providers clearly showed one of the drawbacks of consolidation

- yesterday the discussion was which provider provided the best bang-for-the-buck…

Risks Of Consolidation Into a Small Number of Major Providers

Last weeks attack against one of the major DNS providers clearly showed one of the drawbacks of consolidation

- yesterday the discussion was which provider provided the best bang-for-the-buck...
- enter "collateral damage": large numbers of zones lost service when the attack was either targeting service for some other zone (or the provider itself)

Risks Of Consolidation Into a Small Number of Major Providers

Last weeks attack against one of the major DNS providers clearly showed one of the drawbacks of consolidation

- yesterday the discussion was which provider provided the best bang-for-the-buck. . .
- enter "collateral damage": large numbers of zones lost service when the attack was either targeting service for some other zone (or the provider itself)
- . . . today the question is whether to use two (or perhaps even more) providers instead of a single one

Fast forward to the future where your zone has DNS service from several major providers and the next scale of attacks hit all of them at the same time. . .

Some Predictions for the Future (this is so last year!)

1. The drivers for further DNS evolution remain
    - “DNS service” and “routing” is becoming more and more mixed up due to prevalent use of anycast, both for authoritative and for recursive service
    - DNS will continue to become an ever more complex service
    - with increasing complexity more and more of the “regional level” DNS service will be edged out
2. DNS is becoming a more professionalised service
    - with a smaller number of large scale providers
3. DNS consulting will remain a good field of work

Some Updated Predictions for the Future

1. The drivers for further DNS evolution remain
   - "DNS service" and "routing" is becoming more and more mixed up due to prevalent use of anycast, both for authoritative and for recursive service, but customers won't care, no longer their problem
   - DNS will continue to become an ever more complex service
   - ~~with increasing complexity more and more of the~~ the market forces will ensure that "regional level" DNS service ~~will be edged out~~ will die within five years time
2. DNS is becoming a more professionalised service
   - with a smaller number of large scale providers, resulting in increased fate sharing between zones
   - and an increasing dependence on closed source implementations
3. DNS consulting will ~~remain a good field of work~~ largely consist of API integration work
   - time for more attention on the actual DNS data?

Thank You!

Johan Ihrén
johani@netnod.se