DNS Enterprise Anycast: From Exotic to Necessary

Johan Ihrén
Netnod

May 24, 2017

So, Who Am I and Why Do I Care About DNS?

I'm sure that many of you know about Netnod as an IX operator,

- we run IXes in **Stockholm** (and several other Swedish locations) and now also **Copenhagen**.
- it is also possible to connect to us via a large number of **Netnod Reach Partners**.

Apart from IX Stuff, there's DNS

But we also run a massive amount of DNS services around the world:

Apart from IX Stuff, there's DNS

But we also run a massive amount of DNS services around the world:

- `i.root-servers.net` since 2000-ish

Apart from IX Stuff, there's DNS

But we also run a massive amount of DNS services around the world:

- `i.root-servers.net` since 2000-ish
- DNS anycast services for lots of ccTLDs: most of Western Europe, customers all over Africa, South America and Asia (we're possibly the largest DNS operator on the Internet for ccTLDs)

Apart from IX Stuff, there's DNS

But we also run a massive amount of DNS services around the world:

- `i.root-servers.net` since 2000-ish
- DNS anycast services for lots of ccTLDs: most of Western Europe, customers all over Africa, South America and Asia (we're possibly the largest DNS operator on the Internet for ccTLDs)
- premium and standard enterprise DNS anycast designed for large numbers of zones
- . . . from a grand total of roughly 70 locations around the Internet (including Copenhagen, Stockholm and every nordic country)

. . . to some extent this may be my fault

When DNS Anycast Was Exotic

DNS used to be easy, but those days are long gone.

- we reached the point where Anycast started being used, for a few high profile zones (starting with the root)

Now DNS is of ever growing importance, and that causes all sorts of changes.

- DDOS risks and complexity in DDOS prevention stuff (RRL)
- new software choices with more and more dynamic configs
- at the same time zones must be deployed rapidly (or at least the zone owner believes so)
- and the zone data in itself is becoming more and more dynamic

What used to be a (rather boring) static service is no longer as static

When DNS Anycast Was Exotic

DNS used to be easy, but those days are long gone.

- we reached the point where Anycast started being used, for a few high profile zones (starting with the root)

Now DNS is of ever growing importance, and that causes all sorts of changes.

- DDOS risks and complexity in DDOS prevention stuff (RRL)
- new software choices with more and more dynamic configs
- at the same time zones must be deployed rapidly (or at least the zone owner believes so)
- and the zone data in itself is becoming more and more dynamic

What used to be a (rather boring) static service is no longer as static

- nor as boring. . .

Let's look at what is changing in slightly more detail.

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, and this is a problem

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

Sidebar: DDOS, DDOS, DDOS

However, important as the DDOS threat is, I think that it is important not to make too much of it.

- i.e. we, as a community, should avoid falling into the trap of trying to make the argument that every DNS zone on the Internet is going to be attacked all the time.
- . . . that is just not going to happen

There are also other forces at play in the market

- primarily economic drivers

. . . and this may turn out to actually be more important.

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.

- it is clear that being able to script entire new functions that modify the server behaviour. . . will be used in creative ways
- the old assumption that name server behaviour can be understood from the "config file" is breaking down

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

- the days of manual hacking `named.conf` are over
- 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 define 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:

- responses based on geography, load or some other parameter, 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

The Requirement For an SLA

Furthermore, slowly but surely, the number of customers that

- have requirements on time-to-resolution of problems,
- have requirements on capacity and overprovisioning levels,
- have requirements on service levels,
- etc,

are increasing.
SLA requirements are difficult to deal with in a professional way when running a best effort service in a corner

- dependent on staff that often has a gazillion other responsibilitites in addition to DNS

DNS very rarely is a profit center, which makes it hard to staff up.

Outsource Some Zones!

The solution is of course to outsource the zones that have SLA requirements (or they will go elsewhere for DNS service on their own).

- the problem with this is that in a zero margin business it is not easy to justify the time required to segment the customer base into:
  - "**premium**" customers (that require quality service, SLAs, etc, and are prepared to pay for it)
  - "**standard**" customers (who will always go for the cheapest, preferably zero-cost, alternative)

So the problem is usually deferred.

Price Erosion To The Rescue!

Because of the massive rollout of anycast services we're seeing price erosion among the commercial services.

- while the cost of "running your own infrastructure" is increasing

There are always new threats. Apart from DDOS threats the software vulnerability threats are a major concern.

- software vulnerabilities: the gift that keeps on giving :-)

And, again, DNS is not a profit center in most cases.

Price Erosion, cont'd

The price erosion is reaching a price point where it is more cost effective to just outsource the entire portfolio of customer zones, regardless of whether they are

- **premium** zones (that would be willing to pay)
- or **standard** zones (that would not)

to an external provider (able to run on a thinner margin due to higher volume).

- will there be a waterfall effect?
- not unlikely that most zones in the public DNS are migrated to the large DNS service providers in relatively short time

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 getting close to that point.

And then DNS Anycast Becomes Necessary

When this happens, it will be anycast service for every DNS zone, including the one only used for your dog's fan mail.

- no business case for unicast as a commercial service

At this point:

- 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

Disadvantages of DNS Anycast Becoming Necessary

- smaller providers will be edged out of the market
- the cost (to remaining providers) of moving all the data for millions of zones of minor importance to lots of servers around the world will be impossible to recover
- typical problem definitions will change from
  - "how to I configure BIND9 to . . . " (or "gaa! time to upgrade BIND9, again, and urgently. . . ")

  to
  - "does the the API from DNS provider XXX support the feature YYY?"
- one source of problems (configuring and operating nameservers) will be replaced by another (integration of the various DNS provider APIs)
  - this will require a mostly new skill set in the community

Does DNS-As-A-Service Cause Risks 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.

- 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

The DNS Problem (for the registrar/hosting/etc company)

The "DNS problem" (or "DNS question") for a hosting company, a registrar, or similar, is in most cases about to shift from

- being about what software platform to use on their name servers,
- what new vulnerabilities to worry about,
- configuration management, etc

and largely instead switch over to primarily be about

- different APIs provided by the DNS service providers,
- the SLAs they're offering,
- at what price point,
- lock-in effects of adapting systems to someone else's API, etc

The DNS Problem (for the DNS service provider)

More and more zones, more and more DDOS attacks and continued price erosion is not an ideal mix.

- aggressive automation of everything that can be automated is necessary,
- anycast services must evolve significantly to deal with a situation where they define the base-line

We will see a widening spectrum of services available via the provisioning APIs to allow the customers to pick and choose according to their needs and requirements.

- the old, static, anycast service that was just a standard slave server cloned into many locations will no longer be sufficient

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
   - 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, but customers won't care, no longer their problem
   - DNS will continue to become an ever more complex service
   - the market forces will ensure that within a few years time very few of you will run public authoritative (or recursive) servers
2. DNS is becoming a more professionalised service
   - with a smaller number of large scale providers
   - and an increasing dependence on closed source implementations
3. DNS consulting will increasingly consist of API integration work

DNS Anycast Services For The Enterprise Market

- After many years of providing DNS Anycast Services for the root zone and a large number of major ccTLDs, Netnod is now also providing the same set of services to the Enterprise market
  - . . . but with a completely new provisioning infrastructure to be able to cater to very large numbers of small zones
  - . . . rather than just a single (large) zone (the typical case for a ccTLD customer)
- In the Northern European region we believe that we are already able to provide a significantly better DNS service at a lower cost than other DNS providers
  - as we continue our rollout the same will be true for an increasing number of markets