SIDN
Your world. Our domain.
Local Anycast at SIDN

Marco Davids

Joint 38th CENTR Technical / 12th CENTR R&D workshop
Moscow (RU) - May 30\textsuperscript{rd} 2018
Registry for .nl ccTLD

- And a number of other things (.aw, .politie, .amsterdam)

https://www.sidn.nl/

5 8 0 6 9 7 1
.nl domain names

3 0 2 4 2 5 2
DNSSEC .nl domain names

(as per may 9th 2018)
Vacancies:
• 1 x Machine Learning Engineer
• 2 x Research Engineers on Emerging Internet Architectures

https://www.sidnlabs.nl/over-sidnlabs
Botnets / DDoS
Why we care
Why we care
The Solution: DNS global anycast

- Just a clever ‘network hack’ to provide (a lot of) resilience.
  - And better performance (shorter RTT’s)
- Works with BGP
- Well understood solution, deployed in many places
  - The DNS root servers
  - 1.1.1.1, 8.8.8.8, 9.9.9.9, 64.6.64.6, OpenDNS and more
- Originally only in UDP environments
  - But proven in TCP environments as well (i.e. CloudFlare)
DNS global anycast (in a nutshell)

The unicast situation
(simplified, so one server, only IPv4, etc.)
DNS global anycast

The anycast situation
DNS global anycast

What routers ‘think’
DNS global anycast

What the situation is really like...
DNS global anycast

And if an instance goes down...
Problem solved...?
Problem solved, or...?
Main cause: (insecure) IoT devices
Main cause: (insecure) IoT devices
Main cause: Record breaking DDoS attacks
A rat race we can’t win.
Paradigm shift

It is better to remain available for some than to be not available at all.

---

(All resolvers are equal, but some resolvers are more equal than others)
Additional approach: DNS *local* anycast

- In essence the same principle as global anycast
- But with a deliberately *restricted catchment*.
- Dedicated instances for exclusive use by (big) ISP’s
  - Focus on Netherlands
  - Must have reasonable abuse response capacities
  - Must comply to certain requirements (like BCP38 and IPv6)
- Nothing more, nothing less (basically)

<table>
<thead>
<tr>
<th>Goals</th>
<th>Non Goals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resilience (win the rat race)</td>
<td>Latency (in contrast to global anycast)</td>
</tr>
<tr>
<td>Availability (at least for our most important users)</td>
<td>Bandwidth (DNS doesn’t consume that much, yet)</td>
</tr>
</tbody>
</table>
DNS local anycast

- **AS100** - Client A
- **AS200**
- **AS300**
- **AS400**
- **AS500**
- **AS600**
- **AS700**

**Nameservers:**
- **NS1a** 194.0.28.53
- **NS1b** 194.0.28.53

**Networks:**
- Client A
- Client B

**AS700**
- No export
- X

**Route:**
- Client A to AS100, then to AS200 or AS300, then to AS400 or AS500, then to AS600, then to AS700.

**Route:**
- Client B to AS100, then to AS200 or AS300, then to AS400 or AS500, then to AS600, then to AS700.
DNS local anycast

client A

AS100

AS200

AS300

AS400

AS500

AS600

AS700

NS1a
194.0.28.53

NS1b
194.0.28.53

client B
DNS local anycast

AS100 - AS100
AS200 - AS200
AS300 - AS300
AS400 - AS400
AS500 - AS500
AS600 - AS600
AS700 - AS700

NS1a - 194.0.28.53
NS1b - 194.0.28.53

client B
DNS local anycast
DNS local anycast – incident at AMS-IX
DNS local anycast – incident at AMS-IX
DNS local anycast – incident at AMS-IX
DNS local anycast – incident at AMS-IX
DNS local anycast – conclusion

It actually works!

• For multiple TLD’s
  • .amsterdam, .aw, .politie
DNS local anycast – ‘business model’

For mutual benefit:
• ISP / datacentre provides bandwidth, rack space, power and sometimes ‘remote hands’
• SIDN provides equipment, operations and the service
DNS local anycast – current situation

• Local presence at 8 sites at ISP’s
• One shared node (will explain later)
• ~ >80% of Dutch consumers “covered”
DNS local anycast - management

AS100

AS200

AS300

AS400

AS500

AS600

AS700

NS1a

194.0.28.53

NS1b

194.0.28.53

SIDN
DNS local anycast - management

AS100
AS200
AS300
AS400
AS500
AS600
AS700
NS1a
NS1b
SIDN
AS100
AS200
AS300
AS400
AS500
AS600
AS700
NS1a
NS1b
DNS local anycast – management (via VPN’s)

- SIDN
- AS100
- AS200
- AS300
- AS300
- AS400
- AS500
- AS600
- AS700
- NS1a 194.0.28.53 from AS300
- NS1b 194.0.28.53
- NS1a 195.51.100.1 from AS300
- 203.0.113.1 from AS600
- 194.0.28.53
- 195.51.100.1
DNS local anycast – management (via VPN’s)
DNS local anycast – lessons learned

Setup is overdone.

- Dell server, 32 Gig RAM, 1U
- Fancy Juniper EX switch for BGP, 1U
- Separate Juniper SRX switch for VPN, 1U
- A bit too much for only 50 qps...
DNS local anycast – lessons learned

Also...

- 'Legal challenges’
- ‘Persuasion challenges’, or getting in touch with the right people
- ‘Not-in-scope challenges’ (they want us, we don’t really want them)
- It’s quite a bit of work to setup and maintain
- Monitoring requires special attention
- So does tuning and tweaking
  - Like making sure partners keep it local and don’t export the route
DNS local anycast – lessons learned

Also...

• 'Legal' challenges
• Persuasion challenges, or getting in touch with the right people
• Not in scope challenges (they want us, we don’t really want them)

So we made a ‘shared’ local anycast node
DNS local anycast – Shared node

- Not with an ISP, but located at an IX
- No exclusive use by one party,
- but used by several, carefully selected peers
  - We may cut them off if they cause too much problems for others
- Works well for smaller parties, or for the other mentioned challenges
DNS local anycast – Future work

- Maybe a simple front-end and (hidden) big back-end?
  - DNSdist or CoreDNS forward/proxy and cache plugin maybe?
DNS local anycast – Future work

- **Anycast-in-a-box**
  - Single server with BGP (BIRD), DNS (i.e. BIND), VPN (i.e. FreeS/WAN)
  - Can be virtualized (including a Juniper vMX for instance)
Risk analysis of the .nl BGP (anycast) infrastructure

This project involves assessing how the failure of certain parts of the Internet would affect the availability of the .nl domain and subordinate second-level domain names. For example, what impact would the failure of a major Tier-1 provider have? And how many .nl domain names would be rendered unreachable by the non-availability of a given Autonomous System Number (ASN)?

Anycast vs. DDoS:
Evaluating the November 2015 Root DNS Event (extended)

USC/ISI Technical Report ISI-TR-2016-709b
May 2016, updated September 2016

Giovane C. M. Moura1, Ricardo de O. Schmidt2, John Heidemann3
Wouter B. de Vries2, Moritz Müller1,2, Christian Hesselman1
1: SIDN Labs 2: University of Twente 3: USC/Information Sciences Institute

Faster: Broad and Load-Aware Anycast Mapping

ISI-TR-719 24 May 2017

Pieter-Tjerk de Boer1, Wesley Hardacker3
Aiko Pras1, Giovanni De Michieli Zorzi2, Moritz Müller1,2
1: University of Twente 2: SIDN Labs 3: USC/Information Sciences Institute

Recommendations for Engineering Authority DNS Servers

Giovane Moura1, Ricardo Schmidt1,2, Moritz Müller1,2, Wouter B. de Vries2, and John Heidemann3
1SIDN Labs, 2University of Twente,
3University of Southern California/Information Sciences Institute

IEPC Meeting @ IETF101
March 18th, 2018
London, UK
Thank You!