DNS Flag Days’ Impact and Future Steps

Töma Gavrichenkov
Disclaimer #1.

• I am in no part responsible for the 2019 DNS Flag Day planning.
Disclaimer #1.

• I am in no part responsible for the 2019 DNS Flag Day planning.

• I will be *sort of, slightly,* responsible for the 2020 DNS Flag Day as a community member, but I haven’t been really active in that matter yet (and I’ll explain why).

• Therefore, I only represent my own view. Your mileage may vary.
Disclaimer #2.
Disclaimer #2.

I DO NOT WORK FOR TOYOTA
Disclaimer #2.

I DO NOT WORK FOR TOYOTA

• Therefore, what goes next is not an advertisement

• It is just an act of appreciation of some of the finest tech in the world
A 2019 Toyota Hilux. Runs just fine.
Another 2006 Toyota Hilux. Tactic combat vehicle. Runs just fine.
In 2003, Top Gear bought this 1987 Hilux and tried hard to kill it.
They ended up with this:
They ended up with this:

Runs just fine.
They ended up with this:

Runs just fine. Wanna ride this car?
DNS standard nowadays

Source: https://powerdns.org/dns-camel/

- 100-300 RFCs
- 2,000 to 4,000 pages of text, depending on your material preference
- Hundreds of legacy code someone has to support
- A bunch of new features appears every passing year
DNS standard nowadays

- Over years, the industry has been trying hard to kill the "Toyota" of DNS. Just as Top Gear did.

- Open source DNS software vendors, as well as the infrastructure providers, have to support all that mess today, but they don’t get paid to do that.

- There’s a number of more interesting hobbies than to support a list of legacy features.
Hi there all,

To obsolete DLV I was using the Option 2 of the "Designating RFCs as Historic" process – this involves copying the text of the supporting draft into the "status–change" document, and then making the supporting draft as Dead.

Unfortunately I missed something obvious --
draft-ietf-dnsop-obsolete-dlv also updates RFC 6698 and RFC 6840; by copying the text into the status–change document, there is nothing left to actually *do* the updates. So, with apologies to the authors / WG, can you please resubmit draft-ietf-dnsop-obsolete-dlv with:

1: RFC 6698, RFC 6840 listed in the "Updates" header
2: Update the abstract to say "This document updates RFC 6698 by..."
Thanks Warren.

What I've been told is "the IETF doesn't mark enough documents Historic to standardize the workflow".

Poor Camel

Tim
Thanks Warren.

What I've been told is "the IETF doesn't mark enough documents Historic to standardize the workflow".

Poor Camel

Tim

Or, poor Toyota.
A DNS Flag Day

— An attempt to resurrect the Toyota.

2019: EDNS0 support mandatory
Imagine there are planes you cannot take baggage into
Imagine there are planes you cannot take baggage into. Now imagine you cannot know that in advance.
A DNS Flag Day

— An attempt to resurrect the Toyota.

2019: EDNS0 support mandatory
  • Non-compliant servers would become inoperative
  • Non-compliant firewalls would become inoperative
  • All this happens eventually
A DNS Flag Day

— An attempt to resurrect the Toyota.

2019: EDNS0 support mandatory
• Non-compliant servers would become inoperative
• Non-compliant firewalls would become inoperative
• All this happens eventually

The ultimate effect of the Flag Day was negligible.
### 2019: $T_0$ - 3 months: clusters of breakage

<table>
<thead>
<tr>
<th>provider domain</th>
<th>breakage</th>
<th># broken</th>
</tr>
</thead>
<tbody>
<tr>
<td>hichina.com.</td>
<td>35.78 %</td>
<td>469 611</td>
</tr>
<tr>
<td>dnspod.com.</td>
<td>25.66 %</td>
<td>336 797</td>
</tr>
<tr>
<td>myhostadmin.net.</td>
<td>5.04 %</td>
<td>66 208</td>
</tr>
<tr>
<td>xincache.com.</td>
<td>4.82 %</td>
<td>63 246</td>
</tr>
<tr>
<td>dnspod.net.</td>
<td>3.27 %</td>
<td>42 881</td>
</tr>
<tr>
<td>dnsdun.net.</td>
<td>2.85 %</td>
<td>37 435</td>
</tr>
<tr>
<td>gmoserver.jp.</td>
<td>2.71 %</td>
<td>35 595</td>
</tr>
<tr>
<td>registrar-servers.com.</td>
<td>1.64 %</td>
<td>21 533</td>
</tr>
<tr>
<td>alidns.com.</td>
<td>1.63 %</td>
<td>21 369</td>
</tr>
<tr>
<td>metaregistrar.nl.</td>
<td>1.20 %</td>
<td>15 762</td>
</tr>
</tbody>
</table>

$\sum$ 85%  

$\sum$ 66%  

Source: [https://ripe78.ripe.net/presentations/53-plenary.pdf](https://ripe78.ripe.net/presentations/53-plenary.pdf)
Well.

- If we dive into the impact, it turns out only a marginal portion of niche players are affected.
- This is an incentive to shift the operational costs from compliant players to non-compliant ones!
- Therefore, there’s an incentive to move on.
2019 Flag Day

Was not (sorry) a broad community move.

Rather, a desperate shootout from the ones who have to carry the burden of legacy for free.
2020 Flag Day

Is now the community event!

• Organized by OARC
• Already a topic (expect more)
• A list of supporters
• No particular date yet
2020 Flag Day

The goal: fix the DNS fragmentation.

- Fragmented traffic is a regular part of DDoS attacks
- IP fragments are simply not suitable for DNS
- DNS over TCP has long been there for that!
2020 Flag Day

The goal: fix the DNS fragmentation.

• Fragmented traffic is a regular part of DDoS attacks
• IP fragments are simply not suitable for DNS
• DNS over TCP has long been there for that!

The call for action:
limit the EDNS buffer size to 1232 octets today.

Make sure DNS over TCP works in your network!
202x Flag Day?..

The ultimate impact of the Flag Days:

you’re not getting your legacy DNS for free now.

With its 4,000 pages of spec,
DNS is a protocol that needs an evolution.
A dynamics.
202x Flag Day?.. 

The ultimate impact of the Flag Days:  
**you’re not getting your legacy DNS for free now.**

With its 4,000 pages of spec, 
DNS is a protocol that needs **an evolution.**  
A dynamics.

A piece of software today has a “best before” date.  
**You need to update it before expiration.**
https://dnsflagday.net/2020/