DNS flag day 2019 and beyond

https://dnsflagday.net

Libor Peltan • libor.peltan@nic.cz • 2019-06-03

Developer of Knot DNS, open-source authoritative DNS server

DNS is complex

RFC 1034, 1035, 1101, 1464, 1536, 1591, 1712, 1912, 1982, 1995, 1996, 2136, 2181, 2219, 2230, 2308, 2317, 2606, 2671, 2782, 2845, 2915, 3110, 3225, 3258, 3363, 3425, 3492, 3597, 3675, 4025, 4033, 4034, 4035, 4343, 4408, 4470, 4471, 4509, 4592, 4635, 4986, 5001, 5011, 5155, 5358, 5625, 5702, 5890, 5933, 5966, 6014, 6394, 6605, 6672, 6762, 6781, 6840, 6891, 7129, 7314, 7344, 7583, 7646, 7719, 7766, 7858, 7871, 7873, 8078, 8080, 8109, 8198, and many more (200+)

Workarounds in DNS software

- Added long ago to improve compatibility
- No motivation for non-compliant players to fix
- The costs are on the bill of major vendors:
  - Maintenance of ugly source code
  - Inefficient operation: user observes lagging DNS
  - Hurdles in implementing new DNS features

Non-compliant authoritative servers

- Custom DNS implementations
- Old abandoned versions
- Bad firewalls

Remove workaround?

- Users will blame the resolver
- Resolvers' vendors must cooperate
- Shift the fixing costs to non-compliant parties

First DNS flag day

- EDNS is an extension to DNS protocol to allow i.a. >512 bytes answers
- Every authoritative DNS server must respond to EDNS query
  - valid EDNS response
  - indicate with FORMERR

EDNS is here since 1999

RFC 1034, 1035, 1101, 1464, 1536, 1591,
1712, 1912, 1982, 1995, 1996, 2136, 2181,
2219, 2230, 2308, 2317, 2606, 2671, 2782,
2845, 2915, 3110, 3225, 3258, 3363, 3425,
3492, 3597, 3675, 4025, 4033, 4034, 4035,
4343, 4408, 4470, 4471, 4509, 4592, 4635,
4986, 5001, 5011, 5155, 5358, 5625, 5702,
5890, 5933, 5966, 6014, 6394, 6605, 6672,
6762, 6781, 6840, 6891, 7129, 7314, 7344,
7583, 7646, 7719, 7766, 7858, 7871, 7873,
8078, 8080, 8109, 8198, and many more (200+)

First DNS flag day

- **February 2019**
- New releases of DNS resolvers from
  - CZ.NIC, ISC, NLnet Labs, PowerDNS
- Public DNS recursors
  - Google, Quad 9, Cloudflare, ...
- **DNS servers which do not respond at all to EDNS queries are treated as *dead***

First DNS flag day

- Lot of fear, media articles
- Many operators fixed things
- Remaining broken domains are mostly unused
- Good cooperation among internet community
- Communication to operators can improve

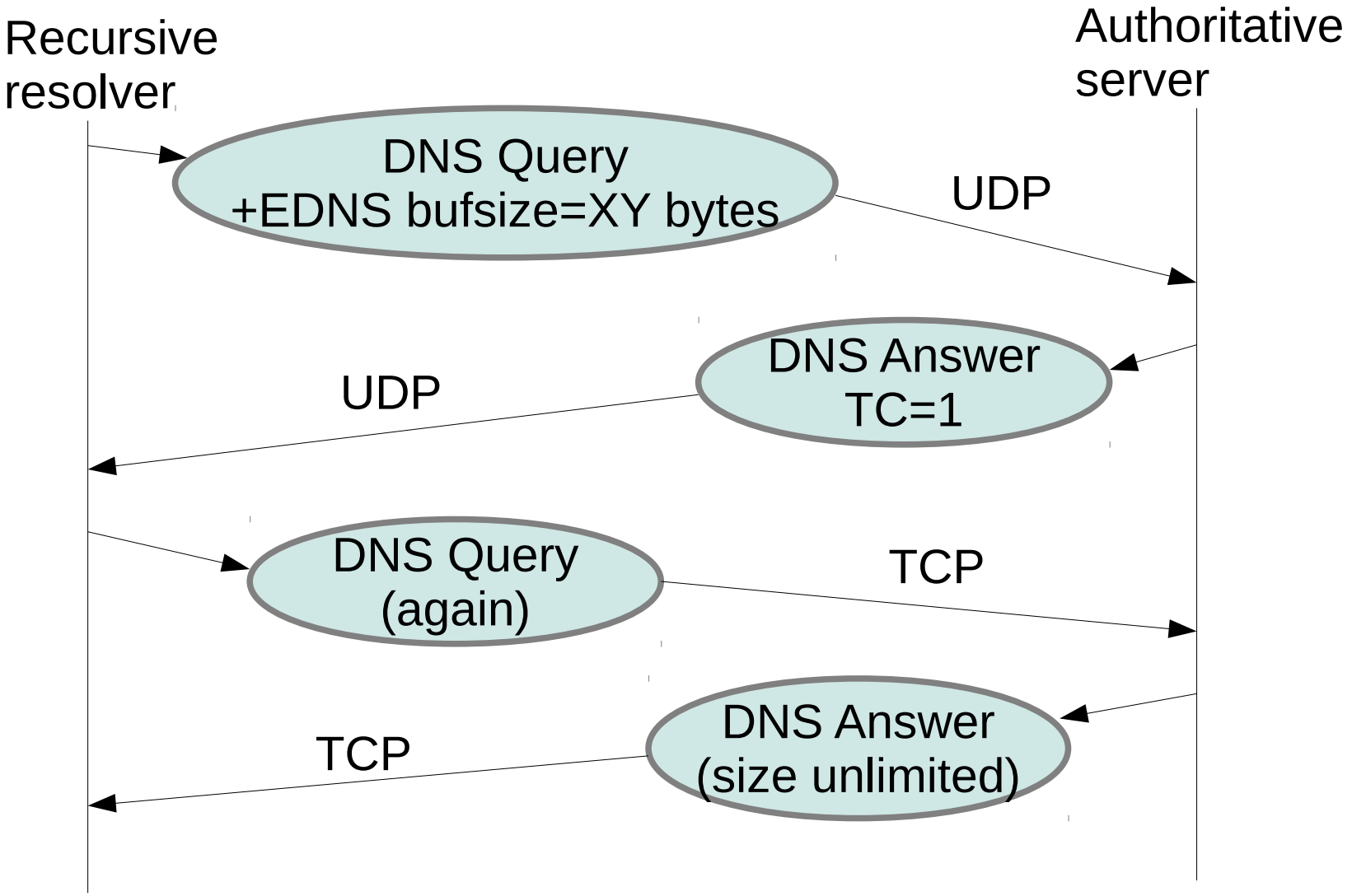
Test your domain

https://dnsflagday.net/2019

Second DNS flag day

- Planning in progress
- 2020 (Feb? Jun? Oct?)
- **DNS UDP to TCP fallback must work**

DNS UDP to TCP fallback



DNS UDP to TCP fallback

RFC 1034, 1035, 1101, 1464, 1536, 1591,
1712, 1912, 1982, 1995, 1996, 2136, 2181,
2219, 2230, 2308, 2317, 2606, 2671, 2782,
2845, 2915, 3110, 3225, 3258, 3363, 3425,
3492, 3597, 3675, 4025, 4033, 4034, 4035,
4343, 4408, 4470, 4471, 4509, 4592, 4635,
4986, 5001, 5011, 5155, 5358, 5625, 5702,
5890, 5933, 5966, 6014, 6394, 6605, 6672,
6762, 6781, 6840, 6891, 7129, 7314, 7344,
7583, 7646, 7719, 7766, 7858, 7871, 7873,
8078, 8080, 8109, 8198, and many more (200+)

DNS over TCP use-cases

- Reliability for large aswers (e.g. DNSSEC)
- Answer size bigger than bufsize
- Mitigation of DoS Amplification
  - Outgoing Response Rate Limiting
- Ensure answer origin
  - DNSSEC secure delegation bootstrap
  - CA domain validation

Second DNS flag day

- Authoritative server must honor EDNS bufsize
- Authoritative server must answer with TC=1
- Authoritative server must implement TCP
- Recursive resolver shall re-query over TCP
- Firewall must not block TCP port 53

The Plan

- By default, resolvers will set bufsize = ~1220
- Thus no fragmentation for DNS over UDP

What you shall do

- Use reasonably recent version of any mainstream DNS software implementaion
- Configure firewalls to allow any kind of correct DNS traffic, including EDNS, TCP, etc.
- Watch https://dnsflagday.net for news and tests