



# DNS Flag Day - 2020

Eddy Winstead, ISC

# What is Flag Day?

- A community effort to ‘clean up’ lingering interoperability issues impacting the DNS system
- Focused on compliance with established IETF standards
- A point in time at which participants remove ‘workarounds’ for non-compliant systems, allowing those to fail





# 2019 DNS Flag Day Participants



# 2019 Problem

- Lack of protocol header in fragments causes problems with middleboxes, firewalls, DPI
- Path mtu discovery doesn't work with Anycast clouds
- UDP is unsuitable for large messages, including DNSSEC
- UDP is insecure - too easy to spoof

# 2020 Solution

- honor an EDNS buffer size that will not cause fragmentation  $\approx 1220$  (exact size tbd)
- allow DNS to switch from UDP to TCP when larger buffer sizes are not enough
  - including FIREWALLS
- No change for small answers - UDP
- DNS over TCP in RFC 7766 and predecessors

# Status of the test tool

- Manual test
  - \$ dig +tcp @auth\_IP yourdomain.example.
  - \$ dig +tcp @resolver\_IP yourdomain.example.
  - \$ dig @resolver\_IP test.knot-resolver.cz. TXT

web-hosted test tool coming soon  
to [dnsflagday.net](https://dnsflagday.net)

Test your domain

Domain name (without www):

Testing completed:

isc.org: All Ok!



- This domain is perfectly ready, you do not need to worry about DNS flag day 2019.
- Your DNS administrator is doing a good job, send them a sincere thank you ;-)

technical report <https://ednscomp.isc.org/ednscomp/105386ab84>

# Updates at

- Web <https://dnsflagday.net/>
- Twitter <https://twitter.com/dnsflagday>
- Announcements: <https://lists.dns-oarc.net/mailman/listinfo/dns-announce>
- Discussion: [dns-operations@lists.dns-oarc.net](mailto:dns-operations@lists.dns-oarc.net)
- Talk to us this week

# References

- Date is TBD (February - May 2020)
- Bonica R. et al, “[IP Fragmentation Considered Fragile](https://tools.ietf.org/html/draft-bonica-intarea-frag-fragile)”, Work in Progress, July 2018. <https://tools.ietf.org/html/draft-bonica-intarea-frag-fragile>
- Huston G., “[IPv6, Large UDP Packets and the DNS](http://www.potaroo.net/ispcol/2017-08/xtn-hdrs.html)”, August 2017. [www.potaroo.net/ispcol/2017-08/xtn-hdrs.html](http://www.potaroo.net/ispcol/2017-08/xtn-hdrs.html)
- Fujiwara K., “[Measures against cache poisoning attacks using IP fragmentation in DNS](https://indico.dns-oarc.net/event/31/contributions/692/)”, May 2019. <https://indico.dns-oarc.net/event/31/contributions/692/>
- RIPE 78 Presentation on DNS Flag Day 2020, <https://ripe78.ripe.net/archives/video/28>