DNS Flag Day 2020

2019-10-31 DNS-OARC, Austin, TX

Ondřej Surý <ondrej@isc.org>

2020: Motivation

- IP fragmentation often does not work
  - IP Fragmentation Considered Fragile [I-D] (expired)
  - IPv6, Large UDP Packets and the DNS (by Geoff Huston)
- If IP fragmentation works, it is not secure enough
  - Measures against cache poisoning attacks using IP fragmentation in DNS (by Kazunori Fujiwara)

UDP is unsuitable for large DNS messages

Causing operational issues around the globe

2020: Goals

- Eliminate operational issues caused by fragments
- Improve security of DNS

2020: Eliminating Fragments

- For large DNS answers switch to TCP
  - **No change for small answers - UDP**
- Existing standards
  - DNS Transport over TCP in RFC 7766 and predecessors
  - Default EDNS buffer size **1232** (= *never fragment*)
- Non-compliance on several levels
  - Authoritative servers don’t listen on TCP
  - Authoritative server don’t honor EDNS buffer size
  - Recursive clients (ignores TC=1)

2020: Advantages of TCP

- Hides IP fragmentation issues
- Harder to spoof
  - Low-throughput high-value services
    - CA domain validation
    - DNSSEC bootstrapping (CDS/CDNSKEY)
- Preparation for DNS-over-TLS (and DoH)

2020: Authoritative nameserver operators

- Honor RFC 7766 — DNS Transport over TCP
  - Answer on TCP port 53
  - Check your firewall, too!
- Set the maximum EDNS buffer size 1232 to avoid fragmentation
  - Defaults in software will reflect this
- Authoritative MUST NOT send oversized answers
  - Standard compliant software does not require changes

2020: Recursive nameserver operators

- Honor RFC 7766 — DNS Transport over TCP
  - Answer on TCP port 53
  - Check your firewall, too!
- Set the default EDNS buffer size 1232 to avoid fragmentation
  - Defaults in software will reflect this
- Resolvers MUST support fallback from UDP to TCP
  - Standard compliant software does not require changes

2020: Test Resolver Configuration

- BIND 9
  - `options { edns-udp-size 1232; };`
- Knot Resolver
  - `net.bufsize(1232)`
- PowerDNS Recursor
  - `edns-outgoing-bufsize=1232`
- Unbound
  - ```
    server:
        edns-buffer-size: 1232
    ```
    ```

2020: The Missing Pieces

- Exact date
  - 1 year from now?
- More measurements
- Communication

2020: Supporters

2020: How to participate

- Web https://dnsflagday.net/
- Twitter https://twitter.com/dnsflagday
- Announcements: https://lists.dns-oarc.net/mailman/listinfo/dns-announce
- Questions: dns-operations@lists.dns-oarc.net
- Talk to us now

Photo by Icons8 team on Unsplash

Questions?