

Avoid Large Records with a Wildcard Owner Name

draft-avoid-large-wildcard-records-00

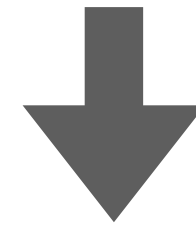
Peng Zuo (CNNIC)
Joe Abley (Cloudflare)
Zhiwei Yan (CNNIC)

Presenter: Bashan Zuo (CNNIC)

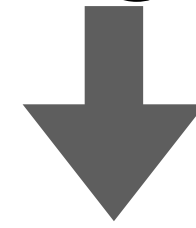
IETF 125, Shenzhen
Mar 16, 2026

Problem

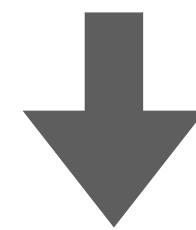
DNS does not have explicit size limit for TXT records.



Operators can publish large TXT under wildcard names.



Queries can keep triggering large responses.



High bandwidth cost and operational concerns.

Goal:

NOT to define a strict limit for TXT records, but to provide operational guidance on how limit should be applied.

Possible Attack Sources

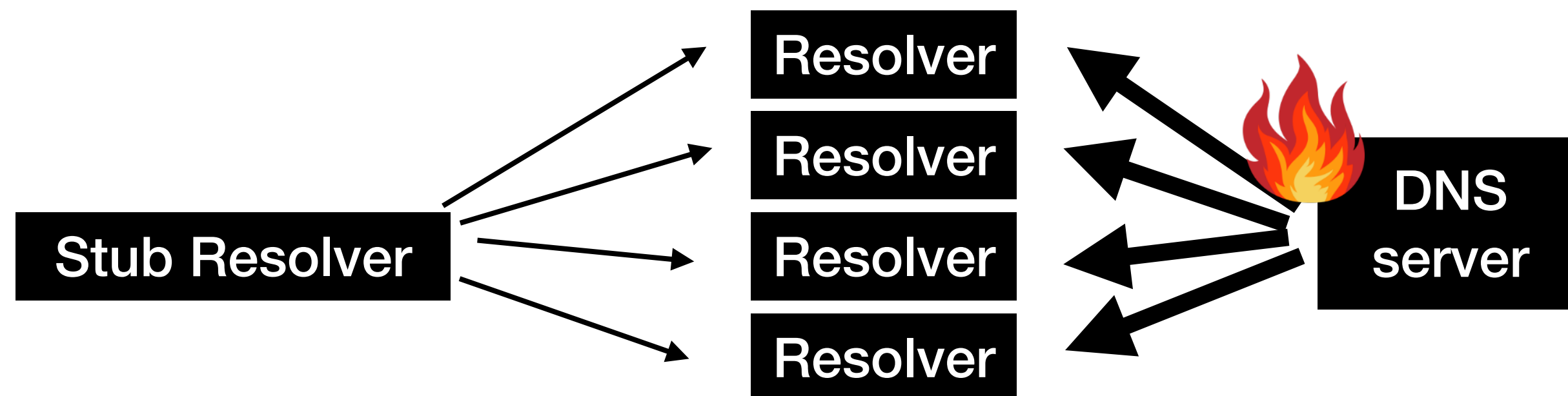
Queries can be sent through public resolvers or from compromised hosts

- Many public resolvers available (53open + TCP + recursive)
- Botnet

Queries can be triggered from a webpage using JavaScript and DoH

- Web ad campaign \ Embedded JavaScript \ DoH API
- `fetch("https://dns.google/resolve?name={random}.vimtim.com&type=TXT")`

Other protocols ?



Potential Impacts

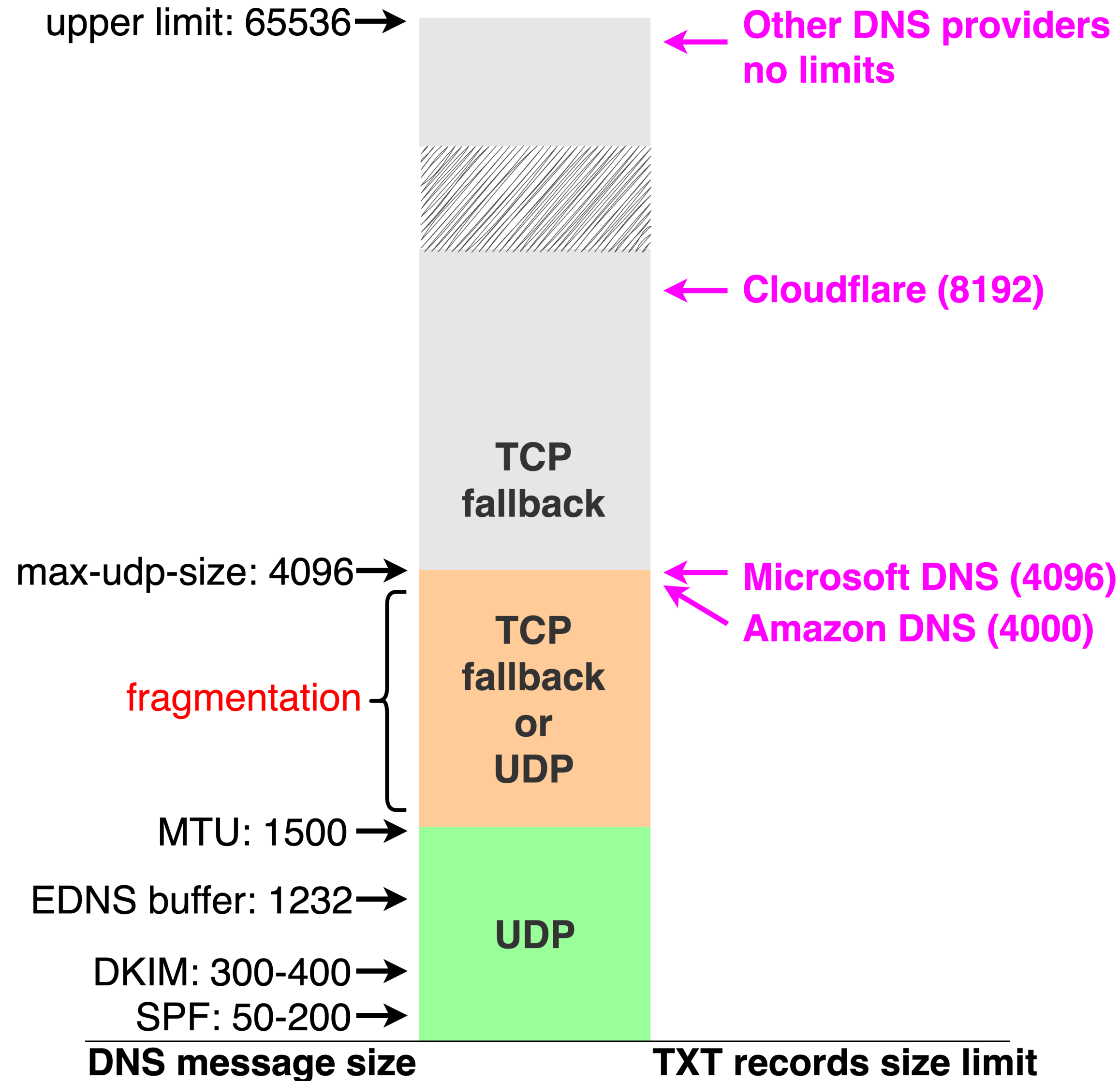
If a DNS server keeps receiving queries that require large responses

- TCP fallback
 - Connection overhead
 - Connections may be exhausted
- Outbound bandwidth on authoritative servers
 - Bandwidth = QPS x Response Size
 - $50,000 \times 65,536 \approx 21 \text{ Gbps}$
- Resolver cache memory pressure
 - Large responses are cached with long TTLs

| Response Size (bytes) | Attacker Upstream (Case A / Case B) | Authoritative Outbound (Case A / Case B) | Resolver Total (Case A / Case B) |
|-----------------------|-------------------------------------|--|----------------------------------|
| 65,535 | 0.480 Mbps / 24.0 Mbps | 524.3 Mbps / 21.0 Gbps | 525.2 Mbps / 21.1 Gbps |
| 8,192 | 0.480 Mbps / 24.0 Mbps | 65.5 Mbps / 2.62 Gbps | 66.5 Mbps / 2.66 Gbps |
| 4,096 | 0.480 Mbps / 24.0 Mbps | 32.8 Mbps / 1.3 Gbps | 33.7 Mbps / 1.35 Gbps |
| 1,024 | 0.480 Mbps / 24.0 Mbps | 8.2 Mbps / 0.32 Gbps | 9.1 Mbps / 0.37 Gbps |
| 512 | 0.480 Mbps / 24.0 Mbps | 4.1 Mbps / 0.16 Gbps | 5.1 Mbps / 0.21 Gbps |

slower response times in shared hosting environments

What can they do in practice ?

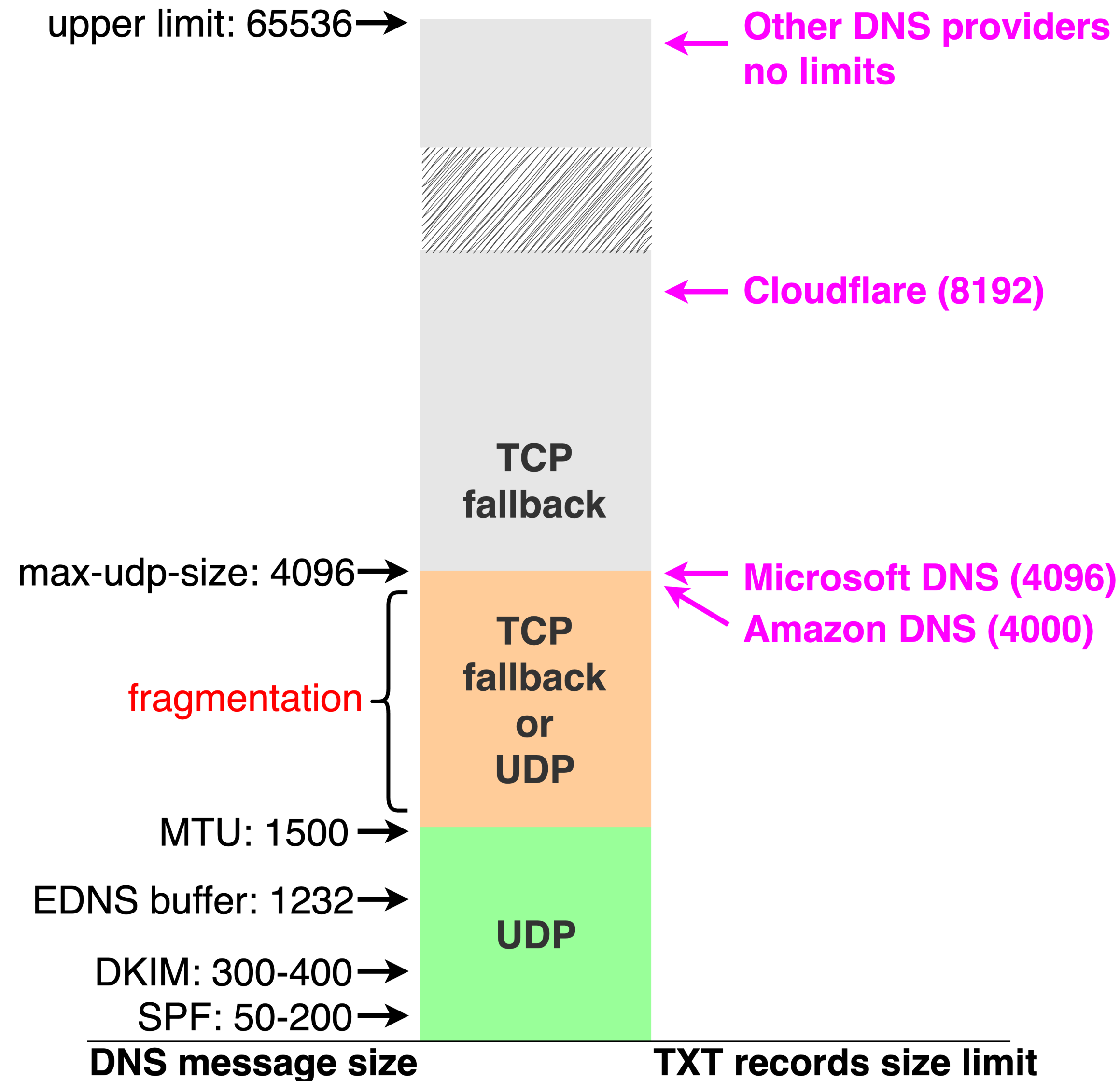


Most of them don't have limits on TXT records

- Cloudflare 8,192 bytes
- Microsoft 4,096 bytes
- Amazon 4,000 bytes
- GoDaddy **no explicit limits**
- Namecheap **no explicit limits**
- DNSPod **no explicit limits**
- Linode **no explicit limits**
- AliDNS **no explicit limits**
 - return smaller (<4,000 bytes)

.....

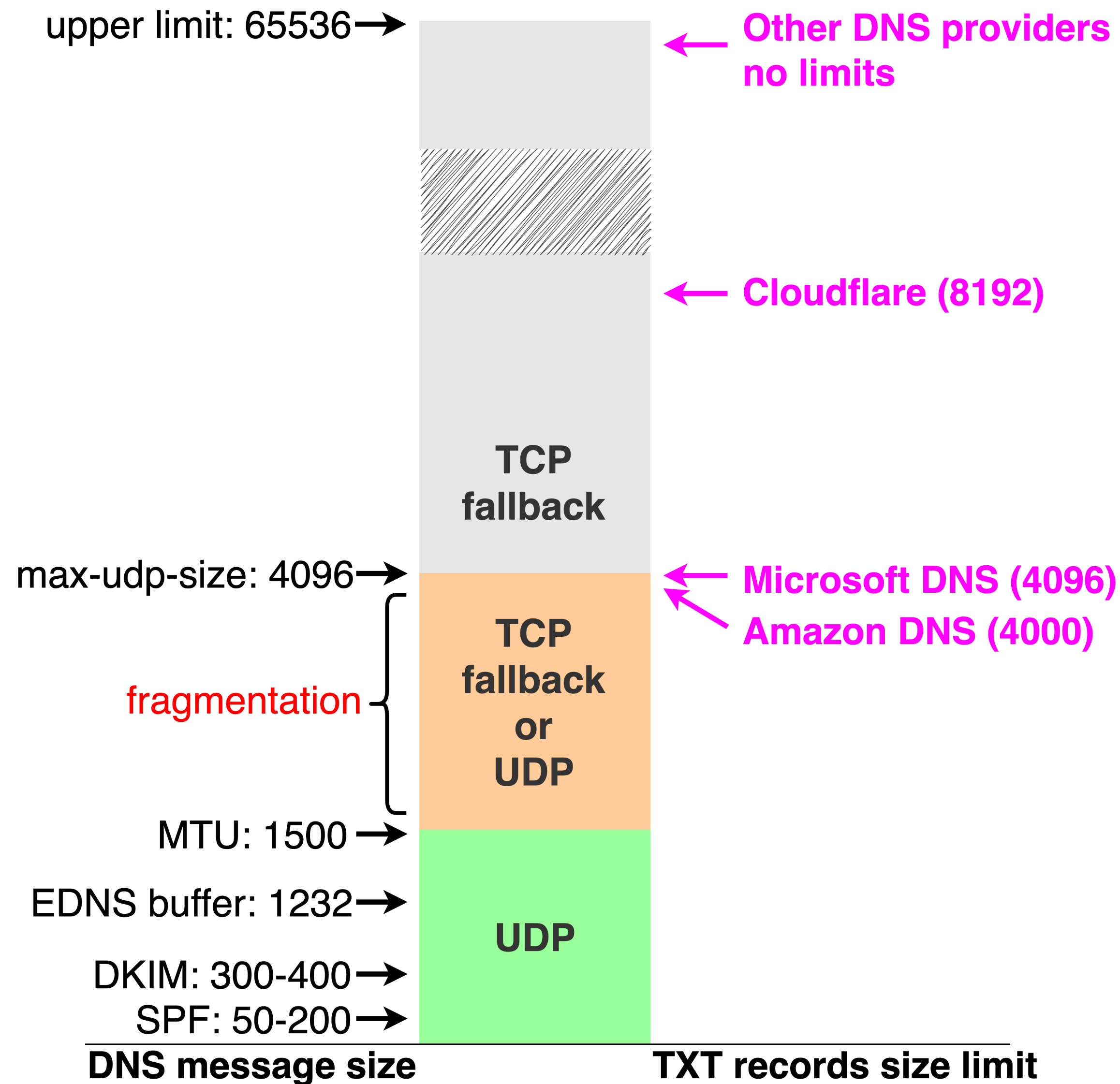
We let them know



We reached out to several DNS providers...

- Global providers
 - Domestic providers
-
- **Some of them updated their policies for large records:**
 - Set limits
 - Return smaller responses
 - Apply rate limiting for queries over TCP
 - **Others don't seem to care or don't see it as a problem.**

Proposed Operational Recommendations



- 1) What's the minimal size requirement ?
- 2) How large is too large ?

Operational guidance | ~~strict limits~~

- something to follow
- exact limit can depends ...

Avoid large TXT records either by: Refusing to accept oversized records

- presumably < 4096 bytes ?

Or by returning smaller responses

- if they don't want explicit limit

Next

Some established practice

- RFC 7208: SPF for Authorizing Use of Domains in Email
- RFC 8482: Providing Minimal-Sized Responses to DNS Queries That Have QTYPE=ANY
- RFC 9842: Compact Denial of Existence in DNSSEC
- draft-fujiwara-dnsop-dns-upper-limit-values-05

This draft follows the similar idea ...

Next

Is this large record issue worth documenting?

- As a BCP?
- As part of another document?
- Or is it not necessary?

Thanks