Network Working Group
Internet-Draft
Intended status: Informational
Expires: 7 January 2026

T. Jensen
6 July 2025

Do Not Accommodate Classic DNS over UDP
draft-tojens-dnsop-do-not-accommodate-udp53-00

Abstract

Protocols that rely on Classic DNS have to account for considerations that only apply to UDP, such as message fragmentation. However, DNS implementations are already required to support both TCP and UDP, and using TCP would alleviate these considerations. This document specifies that new protocols with a dependency on Classic DNS do not need to account for the limitations of Classic DNS over UDP and can instead expect implementations to use Classic DNS over TCP.

Table of Contents

1. Introduction

Many uses of the DNS require message sizes larger than common path MTUs. This poses problems for Classic DNS over UDP by requiring peers to handle message fragmentation. This is usually addressed by requiring peers to set the trucation bit and repeat the query using Classic DNS over TCP, which wastes a round trip, introducing delay in the network traffic that depends on the DNS data retrieval.

However, there are also worse implications, such as requiring IoT devices to do polling Section 3.1 of [RFC9726], additional recommendations for avoiding IP fragmentation [RFC9715] placing transport-like burdens on DNS implementors, and normative requirements that exist only to deter the attack described in the DNS threat analysis [RFC3833], such as having to consciously control source port selection when initializing a DNS resolver with priming queries [RFC9609].

These complications can be avoided by assuming Classic DNS over TCP is the only form of Classic DNS that new protocols need to accommodate. The Implementation Requirements for Classic DNS over TCP [RFC7766] already require DNS implementations to support Classic DNS over TCP wherever they support Classic DNS over UDP and to treat TCP as a first-class transport rather than only a fallback option from UDP. Therefore, it is safe to require protocols to assume Classic DNS is always available over TCP without some specific scenario limitations being defined.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Terminology

This document reuses terms defined in DNS Terminology [RFC9499], including "Classic DNS".

4. Requirements for new protocols

This document does not directly define new normative requirements for DNS implementations. Instead, it defines requirements that apply to new documents produced by the IETF.

Authors of new IETF documents SHOULD NOT add normative requirements that are only necessary to accommodate Classic DNS over UDP that are not necessary to accommodate Classic DNS over TCP without sufficient explaination for why UDP is a preferable transport to TCP (which would deviate from the Implementation Requirements for Classic DNS over TCP [RFC7766]).

Authors of new IETF documents SHOULD direct implementations to use Classic DNS over TCP first by default instead of Classic DNS over UDP if the document defines any usage of Classic DNS that is expected to need message truncation. This will avoid a wasted round trip to switch from UDP to TCP. This requirement does not in any way affect preference between Classic DNS and encrypted DNS.

5. Security Considerations

Discouraging protocols from accommodating Classic DNS over UDP provides a non-zero security benefit by defending against the attack described in the DNS threat analysis Section 2.2 of [RFC3833].

Increasing usage of Classic DNS using TCP will increase maintained state, but this is not concerning because encrypted DNS protocols already require connection maintenance and usage of Classic DNS over TCP is already common due to increasing message sizes.

6. IANA Considerations

This document has no IANA actions.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC3833] Atkins, D. and R. Austein, "Threat Analysis of the Domain Name System (DNS)", RFC 3833, DOI 10.17487/RFC3833, August 2004, <https://www.rfc-editor.org/rfc/rfc3833>.

[RFC7766] Dickinson, J., Dickinson, S., Bellis, R., Mankin, A., and D. Wessels, "DNS Transport over TCP - Implementation Requirements", RFC 7766, DOI 10.17487/RFC7766, March 2016, <https://www.rfc-editor.org/rfc/rfc7766>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC9499] Hoffman, P. and K. Fujiwara, "DNS Terminology", BCP 219, RFC 9499, DOI 10.17487/RFC9499, March 2024, <https://www.rfc-editor.org/rfc/rfc9499>.

7.2. Informative References

[RFC9609] Koch, P., Larson, M., and P. Hoffman, "Initializing a DNS Resolver with Priming Queries", BCP 209, RFC 9609, DOI 10.17487/RFC9609, February 2025, <https://www.rfc-editor.org/rfc/rfc9609>.

[RFC9715] Fujiwara, K. and P. Vixie, "IP Fragmentation Avoidance in DNS over UDP", RFC 9715, DOI 10.17487/RFC9715, January 2025, <https://www.rfc-editor.org/rfc/rfc9715>.

[RFC9726] Richardson, M. and W. Pan, "Operational Considerations for Use of DNS in Internet of Things (IoT) Devices", BCP 241, RFC 9726, DOI 10.17487/RFC9726, March 2025, <https://www.rfc-editor.org/rfc/rfc9726>.

Acknowledgments

Many thanks for constructive feedback on this document to TBD.

Author’s Address

Tommy Jensen
Email: tojens.ietf@gmail.com