Workgroup: DNSSD
Internet-Draft:
draft-ietf-dnssd-multi-qtypes-02
Published: 10 June 2024
Intended Status: Standards Track
Expires: 12 December 2024
Authors: R. Bellis
ISC

DNS Multiple QTYPEs

Abstract

This document specifies a method for a DNS client to request additional DNS record types to be delivered alongside the primary record type specified in the question section of a DNS query.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://dnssd-wg.github.io/draft-ietf-dnssd-multi-qtypes/draft-ietf-dnssd-multi-qtypes.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-dnssd-multi-qtypes/.

Discussion of this document takes place on the DNSSD Working Group mailing list (mailto:dnssd@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/dnssd/. Subscribe at https://www.ietf.org/mailman/listinfo/dnssd/.

Source for this draft and an issue tracker can be found at https://github.com/dnssd-wg/draft-ietf-dnssd-multi-qtypes.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 12 December 2024.

Table of Contents

1. Introduction

A commonly requested DNS [RFC1035] feature is the ability to receive multiple related resource records (RRs) in a single DNS response.

For example, it may be desirable to receive the A, AAAA and HTTPS records for a domain name together, rather than having to issue multiple queries.

The DNS wire protocol in theory supported having multiple questions in a single packet, but in practise this does not work. In [I-D.draft-ietf-dnsop-qdcount-is-one], [RFC1035] is updated to only permit a single question in a QUERY (OpCode == 0) request.

Sending QTYPE=ANY does not guarantee that all RRsets will be returned. [RFC8482] specifies that responders may return a single RRset of their choosing.

This document provides a solution for those cases where only the QTYPE varies by specifying a new option for the Extension Mechanisms for DNS (EDNS [RFC6891]) that contains an additional list of QTYPE values that the client wishes to receive in addition to the single QTYPE appearing in the question section. A different EDNS option is used in response packets as protection against DNS middleboxes that echo EDNS options verbatim.

The specification described herein is applicable both for queries from a stub resolver to recursive servers, and from recursive resolvers to authoritative servers.

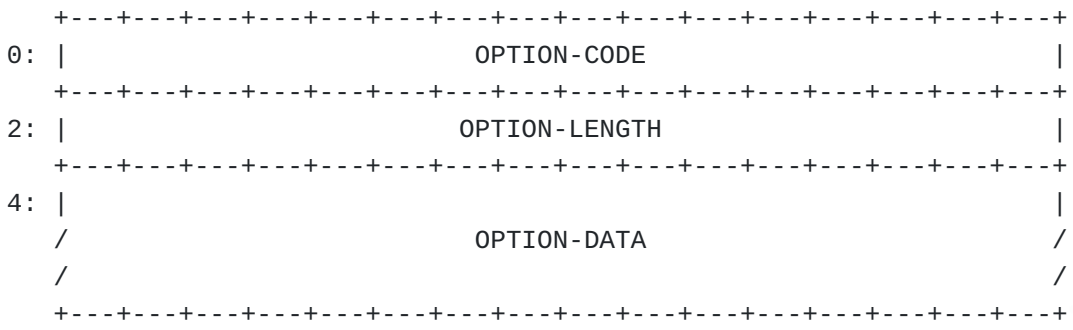
2. Terminology used in this document

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. Description

3.1. Multiple QTYPE EDNS Options Format

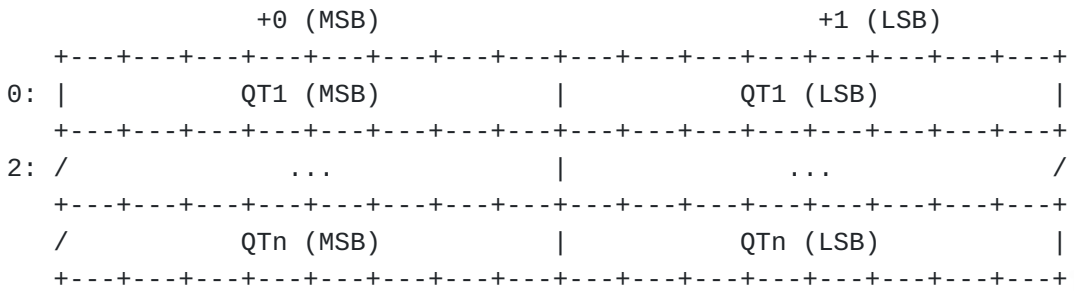
The overall format of an EDNS option is shown for reference below, per [RFC6891], followed by the option specific data:



OPTION-CODE: MQTYPE-Query (TBD1) in queries and MQTYPE-Response (TBD2) in responses.

OPTION-LENGTH: Size (in octets) of OPTION-DATA.

OPTION-DATA: Option specific, as below:



QT: a (potentially empty) list of 2 byte fields (QTx) in network order (MSB first) each specifying a DNS RR type. The RR types **MUST** be for real resource records, and **MUST NOT** refer to pseudo RR types such as "OPT", "IXFR", "TSIG", "*", etc.

3.2. Server Response Generation

A conforming server that receives an MQTYPE-Query option in a query **MUST** return an MQTYPE-Response option in its response. A server that receives an MQTYPE-Response option in a query **MUST** return a FORMERR response.

On receipt of a valid MQTYPE-Query option the server **SHOULD** attempt to return any resource records known to it that match the additional (QNAME, QTx, QCLASS) tuples. These records **MUST** be returned in the Answer Section of the response, but the answer for the primary QTYPE from the Question Section **MUST** be included first.

If any invalid QTx is received in the query (e.g. one corresponding to a meta-RR) the server **MUST** return a FORMERR response.

For any particular QTx in the query, if the server provides additional answers, or has knowledge that the RR type does not exist for that QNAME (a "negative answer"), it **MUST** include that QTx value in the list of QTYPEs in its MQTYPE-Response option. If the server does not provide an answer (whether positive or negative) for that QTx then that value **MUST** be omitted from the list of QTYPEs in it MQTYPE-Response option.

A negative answer is therefore indicated by the combination of the presence of a QTx value in the Multiple QTYPE Option and the absence of a matching record in the Answer Section. This is necessary (in the absence of DNSSEC) to differentiate between absence of the record from the zone and absence of the record from the response.

A server that is authoritative for the specified QNAME on receipt of a Multiple QTYPE Option **MUST** attempt to return all specified RR types except where that would result in truncation or a risk of a significant DNS amplification attack in which case it **MAY** omit some (or all) of the records for the additional RR types.

A caching recursive server receiving a Multiple QTYPE Option query **SHOULD** attempt to fill its positive and negative caches with all of the specified RR types before returning its response to the client. It **MAY** limit itself to a smaller subset of the specified RR types if the processing overhead to fill its caches is too great or if there is a risk of a significant DNS amplification attack.

While this document specifies no limit on the number of QTx values that may be specified, the author anticipates that server implementations will provide configuration settings to constrain the response sizes.

3.2.1. DNSSEC

If the DNS client sets the "DNSSEC OK" (DO) bit in the query then the server **MUST** also return the related DNSSEC records that would have been returned in a standalone query for the same QTYPE.

A negative answer from a signed zone **MUST** contain the appropriate authenticated denial of existence records, per [RFC4034] and [RFC5155].

In a signed zone there is a theoretical risk of valid signatures for one RR type and invalid signatures for another. This is the only case known to the author where the response code for any particular QNAME may be inconsistent across different RR types.

Should a validating resolver produce NOERROR for some RR types and SERVFAIL for others it **MUST** omit the RR types that failed to validate from its response and from the QTx fields on the Multiple QTYPE option.

3.3. Client Response Processing

Recursive resolvers **MAY** use this method to obtain multiple records from an authoritative server. For the purposes of Section 5.4.1 of [RFC2181] any authoritative answers received **MUST** be ranked the same as the answer for the primary question.

If the response to a query containing an MQTYPE-Query option does not contain an MQTYPE-Response option, or if it erroneously contains an MQTYPE-Query option, the client **MUST** treat the response as if this option is unsupported by the server and **SHOULD** process the response as if the MQTYPE-Query option had not been used.

The client **SHOULD** subsequently initiate standalone queries (i.e. without using the MQTYPE-Query option) for any QTx value that did not generate a negative answer.

4. Security Considerations

The method documented here does not change any of the security properties of the DNS protocol itself.

It should however be noted that this method does increase the potential amplification factor when the DNS protocol is used as a vector for a denial of service attack.

5. IANA Considerations

NB: to be rewritten once assignments have been made.

IANA is requested to assign two new values (TBD1 and TBD2) in the DNS EDNS0 Option Codes registry for MQTYPE-Query and MQTYPE-Response. They should be consecutive, with the -Query option being an even number.

6. References

6.1. Normative References

[I-D.draft-ietf-dnsop-qdcount-is-one] Bellis, R. and J. Abley, "In the DNS, QDCOUNT is (usually) One", Work in Progress, Internet-Draft, draft-ietf-dnsop-qdcount-is-one-03, 29 May 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-qdcount-is-one-03>.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/rfc/rfc1035>.

[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>.

[RFC2181] Elz, R. and R. Bush, "Clarifications to the DNS Specification", RFC 2181, DOI 10.17487/RFC2181, July 1997, <https://www.rfc-editor.org/rfc/rfc2181>.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, DOI 10.17487/RFC4034, March 2005, <https://www.rfc-editor.org/rfc/rfc4034>.

[RFC5155] Laurie, B., Sisson, G., Arends, R., and D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence", RFC 5155, DOI 10.17487/RFC5155, March 2008, <https://www.rfc-editor.org/rfc/rfc5155>.

[RFC6891] Damas, J., Graff, M., and P. Vixie, "Extension Mechanisms for DNS (EDNS(0))", STD 75, RFC 6891, DOI 10.17487/RFC6891, April 2013, <https://www.rfc-editor.org/rfc/rfc6891>.

[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>.

6.2. Informative References

[RFC8482] Abley, J., Gudmundsson, O., Majkowski, M., and E. Hunt, "Providing Minimal-Sized Responses to DNS Queries That Have QTYPE=ANY", RFC 8482, DOI 10.17487/RFC8482, January 2019, <https://www.rfc-editor.org/rfc/rfc8482>.

Acknowledgements

The author wishes to thank the following for their feedback and reviews during the initial development of this document: Michael Graff, Olafur Gudmundsson, Matthijs Mekking, and Paul Vixie.

In addition the author wishes to thank the following for subsequent review during discussion in the DNSSD Working Group: Chris Box, Stuart Cheshire, Esko Dijk, Ted Lemon, and David Schinazi.

Author's Address

Ray Bellis
Internet Systems Consortium, Inc.
PO Box 360
Newmarket, NH 03857
United States of America

Phone: +1 650 423 1300
Email: ray@isc.org