Stream: Internet Engineering Task Force (IETF)
RFC: 9619
Updates: 1035
Category: Standards Track
Published: July 2024
ISSN: 2070-1721
Authors: R. Bellis *ISC* J. Abley *Cloudflare*

RFC 9619
In the DNS, QDCOUNT Is (Usually) One

Abstract

This document updates RFC 1035 by constraining the allowed value of the QDCOUNT parameter in DNS messages with OPCODE = 0 (QUERY) to a maximum of one, and it specifies the required behavior when values that are not allowed are encountered.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9619.

Copyright Notice

Table of Contents

1. Introduction

The DNS protocol [RFC1034] [RFC1035] includes a parameter QDCOUNT in the DNS message header whose value is specified to mean the number of questions in the Question section of a DNS message.

In a general sense, it seems perfectly plausible for the QDCOUNT parameter, an unsigned 16-bit value, to take a considerable range of values. However, in the specific case of messages that encode DNS queries and responses (messages with OPCODE = 0), there are other limitations inherent in the protocol that constrain values of QDCOUNT to be either 0 or 1. In particular, several parameters specified for DNS response messages such as AA and RCODE have no defined meaning when the message contains multiple queries as there is no way to signal which question those parameters relate to.

In this document, we briefly survey the existing written DNS specification; provide a description of the semantic and practical requirements for DNS queries that naturally constrain the allowable values of QDCOUNT; and update the DNS base specification to clarify the allowable values of the QDCODE parameter in the specific case of DNS messages with OPCODE = 0.

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. QDCOUNT Is (Usually) One

A brief summary of the guidance provided in the existing DNS specification ([RFC1035] and many other documents) for the use of QDCOUNT can be found in Appendix A. While the specification is clear in many cases, there is some ambiguity in the specific case of OPCODE = 0, which this document aims to eliminate.

4. Updates to RFC 1035

A DNS message with OPCODE = 0 **MUST NOT** include a QDCOUNT parameter whose value is greater than 1. It follows that the Question section of a DNS message with OPCODE = 0 **MUST NOT** contain more than one question.

A DNS message with OPCODE = 0 and QDCOUNT > 1 **MUST** be treated as an incorrectly formatted message. The value of the RCODE parameter in the response message **MUST** be set to 1 (FORMERR).

Middleboxes (e.g., firewalls) that process DNS messages in order to eliminate unwanted traffic **SHOULD** treat messages with OPCODE = 0 and QDCOUNT > 1 as malformed traffic and return a FORMERR response as described above. Such firewalls **MUST NOT** treat messages with OPCODE = 0 and QDCOUNT = 0 as malformed. See Section 4 of [RFC8906] for further guidance.

5. Security Considerations

This document clarifies the DNS specification [RFC1035] and aims to improve interoperability between different DNS implementations. In general, the elimination of ambiguity seems well-aligned with security hygiene.

6. IANA Considerations

This document has no IANA actions.

7. References

7.1. Normative References

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987, <https://www.rfc-editor.org/info/rfc1034>.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/info/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/info/rfc2119>.

[RFC3425] Lawrence, D., "Obsoleting IQUERY", RFC 3425, DOI 10.17487/RFC3425, November 2002, <https://www.rfc-editor.org/info/rfc3425>.

[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/info/rfc8174>.

7.2. Informative References

[RFC1996] Vixie, P., "A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)", RFC 1996, DOI 10.17487/RFC1996, August 1996, <https://www.rfc-editor.org/info/rfc1996>.

[RFC2136] Vixie, P., Ed., Thomson, S., Rekhter, Y., and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, DOI 10.17487/RFC2136, April 1997, <https://www.rfc-editor.org/info/rfc2136>.

[RFC5936] Lewis, E. and A. Hoenes, Ed., "DNS Zone Transfer Protocol (AXFR)", RFC 5936, DOI 10.17487/RFC5936, June 2010, <https://www.rfc-editor.org/info/rfc5936>.

[RFC7873] Eastlake 3rd, D. and M. Andrews, "Domain Name System (DNS) Cookies", RFC 7873, DOI 10.17487/RFC7873, May 2016, <https://www.rfc-editor.org/info/rfc7873>.

[RFC8490] Bellis, R., Cheshire, S., Dickinson, J., Dickinson, S., Lemon, T., and T. Pusateri, "DNS Stateful Operations", RFC 8490, DOI 10.17487/RFC8490, March 2019, <https://www.rfc-editor.org/info/rfc8490>.

[RFC8906] Andrews, M. and R. Bellis, "A Common Operational Problem in DNS Servers: Failure to Communicate", BCP 231, RFC 8906, DOI 10.17487/RFC8906, September 2020, <https://www.rfc-editor.org/info/rfc8906>.

Appendix A. Guidance for the Use of QDCOUNT in the DNS Specification

The DNS specification [RFC1035] provides some guidance about the values of QDCOUNT that are appropriate in various situations. A brief summary of this guidance is collated below.

A.1. OPCODE = 0 (QUERY) and 1 (IQUERY)

[RFC1035] significantly predates the use of the normative requirement key words specified in BCP 14 [RFC2119] [RFC8174], and parts of it are consequently somewhat open to interpretation.

Section 4.1.2 ("Question section format") of [RFC1035] states the following about QDCOUNT:

> "The section contains QDCOUNT (usually 1) entries"

The only documented exceptions within [RFC1035] relate to the IQuery OpCode, where the request has "an empty question section" (QDCOUNT = 0), and the response has "zero, one, or multiple domain names for the specified resource as QNAMEs in the question section". The IQuery OpCode was obsoleted by [RFC3425].

In the absence of clearly expressed normative requirements, we rely on other text in [RFC1035] that makes use of the definite article or that implies a singular question and, by implication, QDCOUNT = 1.

For example, Section 4.1 of [RFC1035] states the following:

> "the question for the name server"

and

> "The question section contains fields that describe a question to a name server."

And per Section 4.1.1 ("Header section format") of [RFC1035]:

> "AA: Authoritative Answer - this bit is valid in responses, and specifies that the responding name server is an authority for the domain name in question section."

DNS Cookies (Section 5.4 of [RFC7873]) allow a client to receive a valid Server Cookie without sending a specific question by sending a request (QR = 0) with OPCODE = 0 and QDCOUNT = 0, with the resulting response also containing no question.

The DNS Zone Transfer Protocol (Section 2.2 of [RFC5936]) allows an authoritative server to optionally send a response message (QR = 1) to a standard Authoritative Transfer (AXFR) query (OPCODE = 0, QTYPE=252) with QDCOUNT = 0 in the second or subsequent message of a multi-message response.

A.2. OPCODE = 4 (NOTIFY)

DNS Notify [RFC1996] also lacks a clearly defined range of values for QDCOUNT. Section 3.7 states that:

> "A NOTIFY request has QDCOUNT>0"

However, all other text in the RFC discusses the <QNAME, QCLASS, QTYPE> tuple in the singular form.

A.3. OPCODE = 5 (UPDATE)

DNS Update [RFC2136] renames the QDCOUNT field to ZOCOUNT, but the value is constrained to be one by Section 2.3 ("Zone Section"):

> "All records to be updated must be in the same zone, and therefore the Zone Section is allowed to contain exactly one record."

A.4. OPCODE = 6 (DNS Stateful Operations, DSO)

DNS Stateful Operations (DSO) (OpCode 6) [RFC8490] preserves compatibility with the standard DNS 12-octet header by requiring all four of the section count values to be set to zero.

A.5. Conclusion

There is no text in [RFC1035] that describes how other parameters in the DNS message, such as AA and RCODE, should be interpreted in the case where a message includes more than one question. An originator of a query with QDCOUNT > 1 can have no expectations of how it will be processed, and the receiver of a response with QDCOUNT > 1 has no guidance for how it should be interpreted.

The allowable values of QDCOUNT seem to be clearly specified for OPCODE = 4 (NOTIFY), OPCODE = 5 (UPDATE), and OPCODE = 6 (DNS Stateful Operations, DSO). OPCODE = 1 (IQUERY) is obsolete and OPCODE = 2 (STATUS) is not specified. OPCODE = 3 is reserved.

However, the allowable values of QDCOUNT for OPCODE = 0 (QUERY) are specified in [RFC1035] without the clarity of normative language, and this looseness of language results in some ambiguity.

Acknowledgements

The clarifications in this document were prompted by questions posed by Ted Lemon, which reminded the authors of earlier, similar questions and motivated them to pick up their pens. Ondrej Sury, Warren Kumari, Peter Thomassen, Mark Andrews, Lars-Johan Liman, Jim Reid, and Niall O'Reilly provided useful feedback.

Authors' Addresses

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

Joe Abley
Cloudflare
Amsterdam
Netherlands
Phone: +31 6 45 56 36 34
Email: jabley@cloudflare.com