Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 22, 2016

M. Vavrusa
O. Gudmundsson
CloudFlare Inc.

March 21, 2016

# Providing AAAA records for free with QTYPE=A
# draft-vavrusa-dnsop-aaaa-for-free-00

Abstract

This document enables DNS servers to include AAAA addresses in the answer section for DNS queries with QTYPE=A in order to reduce the number of resolver round-trips during address lookups, and also provides guidance for recursive DNS servers in accepting such records.

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 http://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 September 22, 2016.

Table of Contents



## 1. Introduction

Over the years, there have been a number of attempts to extend DNS to allow multiple questions in a DNS query. While it is possible to place more than one query in the question section there is is only one RCODE for the combined answer and there are no semantics on how to set the RCODE if there are multiple questions that have different results.

### 1.1. Requirements

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

### 1.2. Terminology

The reader is assumed to be familiar with the basic DNS concepts described in [RFC1034], [RFC1035], [RFC2181] and [RFC6891]. Further DNS terminology is clarified in [RFC7719].

## 2. Motivation

The DNS specification [RFC1034] [RFC1035] doesn't provide any guidance on how to handle records in answer sections with matching QNAME, but mismatching QTYPE with the exception of CNAME and DNAME records.

The most frequently looked up types are address records, A for IPv4 addresses, and AAAA for IPv6 addresses. Stub resolvers attempt to optimize latency by issuing both queries in parallel, but both recursive and authoritative DNS servers then treat both queries independently, thus in the worst case, loss of one answer triggers requery for both. Furthermore, when client is behind an anycast resolver cluster, the two queries may go to different resolver instances. Resolvers also use queries for both record types internally when determining referral chain topology, and the loss of one answer leads either to an added round-trip if requerying, or suboptimal address selection if the recursor continues without it.

## 3. Behaviour of authoritative DNS servers

The authoritative server MAY treat a query with QTYPE=A effectively as a request for any IP address type, regardless of the address protocol with all the requirements due to [RFC1035] , [RFC4035]. Namely, the authoritative server MUST add DNSSEC signatures for any such records if the zone is signed.

However, if there is a direct answer to the original question, but no records for other address protocols, the authoritative DNS server SHOULD NOT prove their non-existence. In this respect, they are treated as additional data.

## 4. Behaviour of recursive DNS servers

The recursive resolver MAY accept RRs with TYPE=AAAA and owner equal to SNAME, therefore a direct answer to the query or matching the the final target of the CNAME chain. They MUST be treated as authoritative data as in [RFC2181], 5.4.1.

Notably, a recursive resolver MUST verify DNSSEC signatures on any such records and it MUST reject any such records if the validation fails, and the zone is not provably secure. In other words, they are subject to the same requirements as a direct answer.

A resolver SHOULD accept other IP address records even if there are no records matching the original QTYPE, given that authoritative DNS server proves non-existence of the direct answer.

## 5. Examples

### 5.1. Response to QTYPE=A with additional AAAA

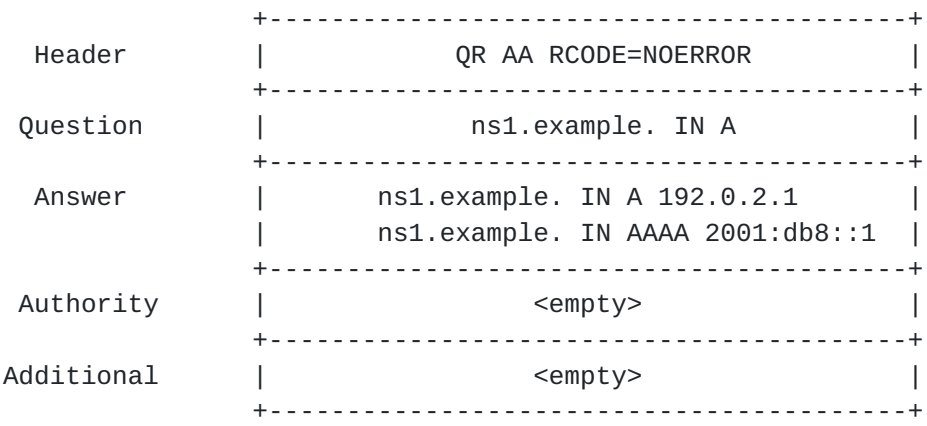


Figure 1

### 5.2. Response to QTYPE=A with missing AAAA

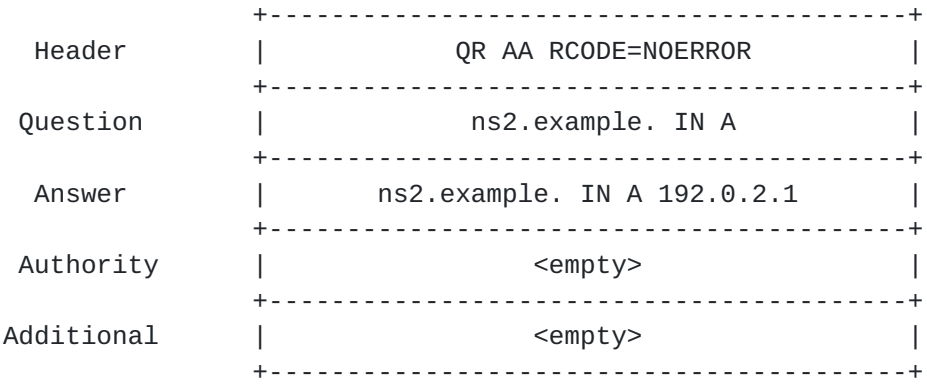


Figure 2

### 5.3. Response to QTYPE=A with missing A, but added AAAA

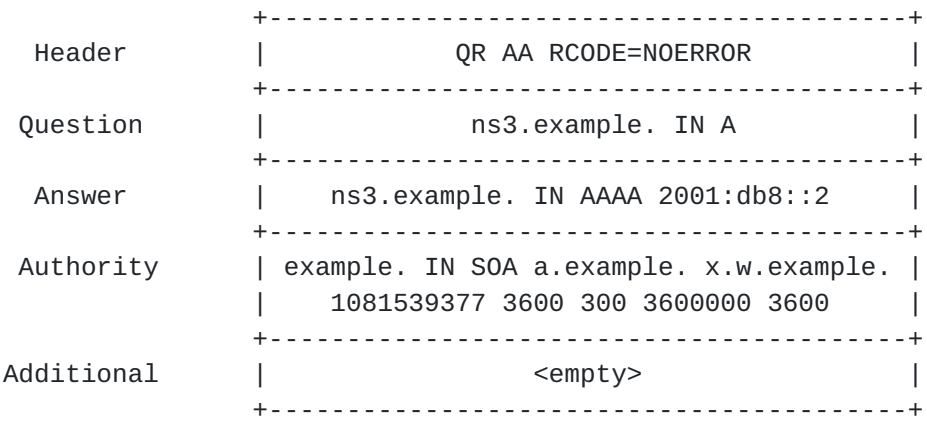


Figure 3

## 6. Security Considerations

In cases where a caching resolver either doesn't validate or the authoritative answer is insecure, a successful spoofing attack may poison both address types in one successful attempt. However, the chance of successful spoofing attack is not affected.

## 7. Performance Considerations

Some resolvers might reject the answer due to "extra" records in the answer section, but more likely the resolver will discard the AAAA records, thus we are no different than today.

## 8. Acknowledgements

Dani Grant, Vicky Shrestha and Filippo Valsorda provided valuable comments on the draft.

## 9. References

### 9.1. Normative References

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

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

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

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, DOI 10.17487/RFC4035, March 2005, <http://www.rfc-editor.org/info/rfc4035>.

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

[RFC7719] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", RFC 7719, DOI 10.17487/RFC7719, December 2015, <http://www.rfc-editor.org/info/rfc7719>.

### 9.2. Informative References

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

Authors' Addresses

Marek Vavrusa
CloudFlare Inc.
101 Townsend St.
San Francisco 94107
USA

Email: mvavrusa@cloudflare.com

Olafur Gudmundsson
CloudFlare Inc.
101 Townsend St.
San Francisco 94107
USA

Email: olafur@cloudflare.com