Network Working Group
Internet-Draft
Updates: 1035 (if approved)
Intended status: Standards Track
Expires: October 8, 2016

J. Abley
Dyn, Inc.
O. Gudmundsson
M. Majkowski
CloudFlare Inc.

April 06, 2016

Providing Minimal-Sized Responses to DNS Queries with QTYPE=ANY
draft-ietf-dnsop-refuse-any-01

Abstract

The Domain Name System (DNS) specifies a query type (QTYPE) "ANY". The operator of an authoritative DNS server might choose not to respond to such queries for reasons of local policy, motivated by security, performance or other reasons.

The DNS specification does not include specific guidance for the behaviour of DNS servers or clients in this situation. This document aims to provide such guidance.

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 October 8, 2016.

Copyright Notice

Table of Contents

1. Terminology

This document uses terminology specific to the Domain Name System (DNS), descriptions of which can be found in [RFC7719].

In this document, "ANY Query" refers to a DNS meta-query with QTYPE=ANY. An "ANY Response" is a response to such a query.

In an exchange of DNS messages between two hosts, this document refers to the host sending a DNS request as the initiator, and the host sending a DNS response as the responder.

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].

2. Introduction

The Domain Name System (DNS) specifies a query type (QTYPE) "ANY". The operator of an authoritative DNS server might choose not to respond to such queries for reasons of local policy, motivated by security, performance or other reasons.

The DNS specification [RFC1034] [RFC1035] does not include specific guidance for the behaviour of DNS servers or clients in this situation. This document aims to provide such guidance.

3. Motivations

ANY queries are legitimately used for debugging and checking the state of a DNS server for a particular name. ANY queries are sometimes used as a attempt to reduce the number of queries needed to get information, e.g. to obtain MX, A and AAAA RRSets for a mail domain in a single query. Although there is no documented guidance available for this use case and some implementations have been observed that appear not to function as perhaps their developers expected. For any developer that assumes that ANY query will be sent to authoritative server to fetch all RRSets, they need to include a fallback when that does not happen.

ANY queries are also frequently used to exploit the amplification potential of DNS servers/resolvers using spoofed source addresses and UDP transport (see [RFC5358]). Having the ability to return small responses to such queries makes DNS servers less attractive amplifiers.

ANY queries are sometimes used to help mine authoritative-only DNS servers for zone data, since they are expected to return all RRSets for a particular query name. A DNS operator MAY prefer not to send large ANY responses to reduce the potential for information leaks.

Some authoritative-only DNS server implementations require additional processing in order to send a conventional ANY response, and avoiding that processing expense might be desirable.

4. General Approach

This proposal provides a mechanism for an authority server to signal that conventional ANY queries are not supported for a particular QNAME, and to do so in such a way that is both compatible with and

triggers desirable behaviour by unmodified clients (e.g. DNS resolvers).

Alternative proposals for dealing with ANY queries have been discussed. One approach proposed using a new RCODE to signal that an authoritative server did not answer ANY queries in the standard way. This approach was found to have an undesirable effect on both resolvers and authoritative-only servers; resolvers receiving an unknown RCODE caused them to re-send the same query to all available authoritative servers, rather than suppress future such ANY queries for the same QNAME.

This proposal avoids that outcome by returning a non-empty RRSet in the ANY response, providing resolvers with something to cache and effectively suppressing repeat queries to the same or different authority servers.

This proposal specifies two different modes of behaviour by DNS responders, for names that exists. Operators/Implementers are free to choose whichever mechanism best suits their environment.

1. A DNS responder can choose to select one or subset of RRSets at the QNAME.

2. A DNS responder can return instead synthesised HINFO resource record. See Section 7 for discussion of the use of HINFO.

5. Behaviour of DNS Responders

A DNS responder which receives an ANY query MAY decline to provide a conventional response, and MAY instead send a response with a single RRSet in the answer section.

The RRSet returned in the answer section of the response MAY be a single RRSet owned by the name specified in the QNAME. Where multiple RRSets exist, the responder SHOULD choose a small one(s) to reduce its amplification potential.

If there is no CNAME present at the owner name matching the QNAME, the resource record returned in the response MAY instead be synthesised, in which case a single HINFO resource record SHOULD be returned. The CPU field of the HINFO RDATA SHOULD be set to RFCXXXX [note to RFC Editor, replace with RFC number assigned to this document]. The OS field of the HINFO RDATA SHOULD be set to the null string to minimize the size of the response.

The TTL encoded for a synthesised RR SHOULD be chosen by the operator of the DNS responder to be large enough to suppress frequent

subsequent ANY queries from the same initiator with the same QNAME, understanding that a TTL that is too long might make policy changes relating to ANY queries difficult to change in the future. The specific value used is hence a familiar balance when choosing TTL for any RR in any zone, and be specified according to local policy.

If the DNS query includes DO=1 and the QNAME corresponds to a zone that is known by the responder to be signed, a valid RRSIG for the RRSets in the answer (or authority if answer is empty) section MUST be returned. In case DO=0 RRSIG SHOULD be omitted.

Except as described in this section, the DNS responder MUST follow the standard algorithms when constructing a response.

6. Behaviour of DNS Initiators

A DNS initiator which sends a query with QTYPE=ANY and receives a response containing an HINFO, as described in Section 5, MAY cache the HINFO response in the normal way. Such cached HINFO resource records SHOULD be retained in the cache following normal caching semantics, as it would with any other response received from a DNS responder.

A DNS initiator MAY suppress queries with QTYPE=ANY in the event that the local cache contains a matching HINFO resource record with RDATA.CPU field, as described in Section 5.

7. HINFO Considerations

In the case where a zone that contains HINFO RRSets is served from an authority server that does not provide conventional ANY responses, it is possible that the HINFO RRSet in an ANY response, once cached by the initiator, might suppress subsequent queries from the same initiator with QTYPE=HINFO. The use of HINFO in this proposal would hence have effectively mask the HINFO RRSet present in the zone.

Authority-server operators who serve zones that rely upon conventional use of the HINFO RRTYPE MAY sensibly choose not to deploy the mechanism described in this document or select other type.

The HINFO RRTYPE is believed to be rarely used in the DNS at the time of writing, based on observations made both at recursive servers and authority servers.

8. Changes to RFC 1035

It is important to note that returning a subset of available RRSets when processing an ANY query is legitimate and consistent with [RFC1035]; ANY does not mean ALL.

This document describes optional behaviour for both DNS initiators and responders, and implementation of the guidance provided by this document is OPTIONAL.

9. Implementation experience

In October 2015 CloudFlare Authoritative Nameserver implementation implemented the HINFO response. Few minor problems have been reported and worked out. NSD has for a while implemented a sub-set response. A Bind user implemented this draft suggestion of returning only single RRset during an attack.

10. Security Considerations

Queries with QTYPE=ANY are frequently observed as part of reflection attacks, since a relatively small query can be used to elicit a large response; this is a desirable characteristic if the goal is to maximize the amplification potential of a DNS server as part of a volumetric attack. The ability of a DNS operator to suppress such responses on a particular server makes that server a less useful amplifier.

The optional behaviour described in this document to reduce the size of responses to queries with QTYPE=ANY is compatible with the use of DNSSEC by both initiator and responder.

11. IANA Considerations

The IANA is requested to update the Resource Record (RR) TYPEs Registry [1] entry as follows:

Type	Value	Meaning	Reference
*	255	A request for some or all records the server has available	[RFC1035][RFC6895] [This Document]

12. Acknowledgements

Evan Hunt and David Lawrence provided valuable observations and concrete suggestions. Jeremy Laidman helped make the document better. Tony Finch realized that this document was valuable and implemented it while under attack. A large number of people have provided comments and suggestions we thank them all for the feedback.

13. References

13.1. 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>.

[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>.

13.2. Informative References

[RFC5358] Damas, J. and F. Neves, "Preventing Use of Recursive Nameservers in Reflector Attacks", BCP 140, RFC 5358, DOI 10.17487/RFC5358, October 2008, <http://www.rfc-editor.org/info/rfc5358>.

[RFC6895] Eastlake 3rd, D., "Domain Name System (DNS) IANA Considerations", BCP 42, RFC 6895, DOI 10.17487/RFC6895, April 2013, <http://www.rfc-editor.org/info/rfc6895>.

[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>.

13.3. URIs

[1] http://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml#dns-parameters-4

Appendix A. Editorial Notes

This section (and sub-sections) to be removed prior to publication.

A.1. Change History

A.1.1. draft-ietf-dnsop-refuse-any-03

Text clarifications, reflecting experience, added implementation experience.

A.1.2. draft-ietf-dnsop-refuse-any-02

Added suggestion to call out RRSIG is optional when DO=0.

Number of text suggestions from Jeremy Laidman

A.1.3. draft-ietf-dnsop-refuse-any-01

Add IANA Considerations

A.1.4. draft-ietf-dnsop-refuse-any-00

Re-submitted with a different name following adoption at the dnsop wg meeting convened at IETF 94.

A.1.5. draft-jabley-dnsop-refuse-any-01

Make signing of RRSets in answers from signed zones mandatory.

Document the option of returning an existing RRSet in place of a synthesised one.

A.1.6. draft-jabley-dnsop-refuse-any-00

Initial draft circulated for comment.

Authors' Addresses

Joe Abley
Dyn, Inc.
103-186 Albert Street
London, ON N6A 1M1
Canada

Phone: +1 519 670 9327
Email: jabley@dyn.com

Olafur Gudmundsson
CloudFlare Inc.

Email: olafur@cloudflare.com

Marek Majkowski
CloudFlare Inc.

Email: marek@cloudflare.com