      Providing Minimal-Sized Responses to DNS Queries That Have QTYPE=ANY

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
   behavior of DNS servers or clients in this situation. This document
   aims to provide such guidance.

   This document updates RFCs 1034 and 1035.

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/rfc8482.

Copyright Notice

Table of Contents

1. 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 behavior of DNS servers or clients in this
   situation. This document aims to provide such guidance.

1.1. Terminology

   This document uses terminology specific to the Domain Name System
   (DNS), descriptions of which can be found in [RFC8499].

   [RFC1035] defined type 255 to be "*". However, DNS implementations
   commonly use the keyword "ANY" to refer to that type code; this
   document follows that common usage.

   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 this document, "conventional ANY response" means an ANY response
   that is constructed in accordance with the algorithm documented in
   Section 4.3.2 of [RFC1034] and specifically without implementing any
   of the mechanisms described in this document.

   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", "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.

2. Motivations for Use of ANY Queries

        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 an attempt to reduce the number of
        queries needed to get information, e.g., to obtain MX, A, and AAAA
        resource record sets (RRsets) for a mail domain in a single query.
        However, there is no documented guidance available for this use case,
        and some implementations have been observed not to function as their

Abley, et al.   Standards Track   [Page 3]

---

        developers expected. If implementers assume that an ANY query will
        ultimately be received by an authoritative server and will fetch all
        existing RRsets, they should include a fallback mechanism to use when
        that does not happen.

        ANY queries are frequently used to exploit the amplification
        potential of DNS servers and 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. If DNS operators prefer to reduce the
        potential for information leaks, they might choose not to send large
        ANY responses.

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

3. General Approach

        This proposal provides a mechanism for an authoritative DNS server to
        signal that conventional ANY queries are not supported for a
        particular QNAME. It does so in a way that is both compatible with
        and triggers desirable behavior by unmodified clients (e.g., DNS
        resolvers).

Alternative proposals for dealing with ANY queries have been
discussed. One approach proposes 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 would resend the same query to all available
authoritative servers rather than suppress future ANY queries for the
same QNAME.

The proposal described in this document avoids that outcome by
returning a non-empty RRset in the ANY response, which provides
resolvers with something to cache and effectively suppresses repeat
queries to the same or different authoritative DNS servers.

4. Behavior of DNS Responders

   Below are the three different modes of behavior by DNS responders
   when processing queries with QNAMEs that exist, QCLASS=IN, and
   QTYPE=ANY. Operators and implementers are free to choose whichever
   mechanism best suits their environment.

   1. A DNS responder can choose to select one or a larger subset of
       the available RRsets at the QNAME.

   2. A DNS responder can return a synthesized HINFO resource record.
       See Section 6 for discussion of the use of HINFO.

   3. A resolver can try to give out the most likely records the
       requester wants. This is not always possible, and the result
       might well be a large response.

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

4.1. Answer with a Subset of Available RRsets

A DNS responder that receives an ANY query MAY decline to provide a
conventional ANY response or MAY instead send a response with a
single RRset (or a larger subset of available RRsets) in the answer
section.

The RRsets returned in the answer section of the response MAY consist
of a single RRset owned by the name specified in the QNAME. Where
multiple RRsets exist, the responder SHOULD choose a small subset of
those available to reduce the amplification potential of the
response.

If the zone is signed, appropriate RRSIG records MUST be included in
the answer.

Note that this mechanism does not provide any signaling to indicate
to a client that an incomplete subset of the available RRsets has
been returned.

4.2. Answer with a Synthesized HINFO RRset

If there is no CNAME present at the owner name matching the QNAME,
the resource record returned in the response MAY instead be
synthesized. In this case, a single HINFO resource record SHOULD be
returned. The CPU field of the HINFO RDATA SHOULD be set to
"RFC8482". 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 the synthesized HINFO resource record 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 SHOULD be configurable by the
operator of the nameserver according to local policy, based on the
familiar considerations involved in choosing a TTL value for any
resource record in any zone.

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 the case of DO=0, the RRSIG SHOULD be omitted.

A system that receives an HINFO response SHOULD NOT infer that the
response was generated according to this specification and apply any
special processing of the response because, in general, it is not
possible to tell with certainty whether the HINFO RRset received was
synthesized. In particular, systems SHOULD NOT rely upon the HINFO
RDATA described in this section to distinguish between synthesized
and non-synthesized HINFO RRsets.

4.3. Answer with Best Guess as to Intention

In some cases, it is possible to guess what the initiator wants in
the answer (but not always). Some implementations have implemented
the spirit of this document by returning all RRsets of RRTYPE CNAME,
MX, A, and AAAA that are present at the owner name while suppressing
others. This heuristic seems to work well in practice; it satisfies
the needs of some applications whilst suppressing other RRsets such
as TXT and DNSKEY that can often contribute to large responses.
Whilst some applications may be satisfied by this behavior, the
resulting responses in the general case are larger than in the
approaches described in Sections 4.1 and 4.2.

As before, if the zone is signed and the DO bit is set on the
corresponding query, an RRSIG RRset MUST be included in the response.

4.4. Transport Considerations

A DNS responder MAY behave differently when processing ANY queries
received over different transports, e.g., by providing a conventional
ANY response over TCP whilst using one of the other mechanisms
specified in this document in the case where a query was received
using UDP.

Implementers MAY provide configuration options to allow operators to
specify different behavior over different transports.

5. Behavior of DNS Initiators

A DNS initiator that sends a query with QTYPE=ANY and receives a
response containing an HINFO resource record or a single RRset, as
described in Section 4, MAY cache the response in the normal way.

Such cached resource records SHOULD be retained in the cache
following normal caching semantics, as 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 the
CPU field of the HINFO RDATA, as described in Section 4. A DNS
initiator MAY instead respond to such queries with the contents of
the local cache in the usual way.

6. HINFO Considerations

It is possible that the synthesized HINFO RRset in an ANY response,
once cached by the initiator, might suppress subsequent queries from
the same initiator with QTYPE=HINFO. Thus, the use of HINFO in this
proposal would effectively mask the HINFO RRset present in the zone.

Operators of authoritative servers who serve zones that rely upon
conventional use of the HINFO RRTYPE SHOULD sensibly choose the
"single RRset" method described in this document or select another
type.

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

7. Updates to RFCs 1034 and 1035

This document extends the specification for processing ANY queries
described in Section 4.3.2 of [RFC1034].

It is important to note that returning a subset of available RRsets
when processing an ANY query is legitimate and consistent with
[RFC1035]; it can be argued that ANY does not always mean ALL, as
used in Section 3.2.3 of [RFC1035]. The main difference here is that
the TC bit SHOULD NOT be set in the response, thus indicating that
this is not a complete answer.

This document describes optional behavior for both DNS initiators and

responders; implementation of the guidance provided by this document
is OPTIONAL.

RRSIG queries (i.e., queries with QTYPE=RRSIG) are similar to ANY
queries in the sense that they have the potential to generate large
responses as well as extra work for the responders that process them,
e.g., in the case where signatures are generated on the fly. RRSIG
RRsets are not usually obtained using such explicit queries but are
rather included in the responses for other RRsets that the RRSIGs
cover. This document does not specify appropriate behavior for RRSIG
queries; however, future such advice might well benefit from
consistency with and experience with the approaches for ANY queries
described here.

8. Implementation Experience

In October 2015, the Cloudflare authoritative nameserver
implementation implemented the HINFO response. A few minor problems
were reported and have since been resolved.

An implementation of the subset-mode response to ANY queries was
implemented in NSD 4.1 in 2016.

An implementation of a single RRset response to an ANY query was made
for BIND9 by Tony Finch, and that functionality was subsequently made
available in production releases starting in BIND 9.11.

9. 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 behavior 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.

10. IANA Considerations

   IANA has updated the following entry in the "Resource Record (RR)
   TYPEs" registry [RR_TYPES]:

   +------+-------+----------------------------+-------------------+
   | TYPE | Value | Meaning | Reference |
   +------+-------+----------------------------+-------------------+
*	255	A request for some or all	[RFC1035][RFC6895]
		records the server has	[RFC8482]
		available	
   +------+-------+----------------------------+-------------------+

11. References

11.1. 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>.

   [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>.

11.2. 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,
              <https://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, <https://www.rfc-editor.org/info/rfc6895>.

   [RFC8499] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS

                Terminology", BCP 219, RFC 8499, DOI 10.17487/RFC8499,
                January 2019, <https://www.rfc-editor.org/info/rfc8499>.

   [RR_TYPES] IANA, "Domain Name System (DNS) Parameters",
             <https://www.iana.org/assignments/dns-parameters>.

Authors' Addresses

   Joe Abley
   Afilias
   300-184 York Street
   London, ON N6A 1B5
   Canada

   Phone: +1 519 670 9327
   Email: jabley@afilias.info

   Olafur Gudmundsson
   Cloudflare Inc.

   Email: olafur+ietf@cloudflare.com

   Marek Majkowski
   Cloudflare Inc.

   Email: marek@cloudflare.com

   Evan Hunt
   ISC

      950 Charter St
      Redwood City, CA 94063
      United States of America

      Email: each@isc.org