                    xNAME RCODE and Status Bits Clarification

Abstract

   The Domain Name System (DNS) has long provided means, such as the
   CNAME (Canonical Name), whereby a DNS query can be redirected to a
   different name. A DNS response header has an RCODE (Response Code)
   field, used for indicating errors, and response status bits. This
   document clarifies, in the case of such redirected queries, how the
   RCODE and status bits correspond to the initial query cycle (where
   the CNAME or the like was detected) and subsequent or final query
   cycles.

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 5741.

   Information about the current status of this document, any errata,
   and how to provide feedback on it may be obtained at
   http://www.rfc-editor.org/info/rfc6604.

Table of Contents

1. Introduction

   The Domain Name System (DNS) has long provided means, such as the
   CNAME (Canonical Name [RFC1035]) and DNAME [RFC2672] RRs (Resource
   Records), whereby a DNS query can be redirected to a different name.
   In particular, CNAME normally causes a query to its owner name to be
   redirected, while DNAME normally causes a query to any lower-level
   name to be redirected. There has been a proposal for another
   redirection RR. In addition, as specified in [RFC2672], redirection
   through a DNAME also results in the synthesis of a CNAME RR in the
   response. In this document, we will refer to all RRs causing such
   redirection as xNAME RRs.

   xNAME RRs can be explicitly retrieved by querying for the xNAME type.
   When a different type is queried and an xNAME RR is encountered, the
   xNAME RR (and possibly a synthesized CNAME) is added to the answer in
   the response, DNS Security Extensions (DNSSEC) [RFC4035] RRs
   applicable to the xNAME RR may be added to the response, and the
   query is restarted with the name to which it was redirected.

   An xNAME may redirect a query to a name at which there is another
   xNAME and so on. In this document, we use "xNAME chain" to refer to
   a series of one or more xNAMEs each of which refers to another xNAME
   except the last, which refers to a non-xNAME or results in an error.

   A DNS response header has an RCODE (Response Code) field, used for
   indicating errors, and status bits that indicate whether an answer is
   authoritative and/or authentic. This document clarifies, in the case
   of such redirected queries, how the RCODE and status bits correspond
   to the initial query cycle (where the (first) xNAME was detected) and
   subsequent or final query cycles.

1.1. Conventions Used in This Document

   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. Restatement of Status Bits and What They Mean

   There are two status bits returned in query responses for which a
   question could arise as to how, in the case of an xNAME chain, they
   relate to the first, possible intermediate, and/or last queries, as
   below. Note that the following is unchanged from [RFC1035] and
   [RFC4035]. The meaning of these bits is simply restated here for
   clarity, because of observations of released implementations that did
   not follow these meanings.

2.1. The Authoritative Answer Bit

   The AA, or Authoritative Answer bit, in the DNS response header
   indicates that the answer returned is from a DNS server authoritative
   for the zone containing that answer. For an xNAME chain, this
   "authoritative" status could be different for each answer in that
   chain.

   [RFC1035] states that the AA bit is to be set based on whether the
   server providing the answer with the first owner name in the answer
   section is authoritative. This specification of the AA bit has not
   been changed.

2.2. The Authentic Data Bit

   The AD, or Authentic Data bit, indicates that the response returned
   is authentic according to the dictates of DNSSEC [RFC4035].
   [RFC4035] unambiguously states that the AD bit is to be set in a DNS
   response header only if the DNSSEC-enabled server believes all RRs in
   the answer and authority sections of that response to be authentic.
   This specification of the AD bit has not been changed.

3. RCODE Clarification

   The RCODE field in a DNS query response header is non-zero to
   indicate an error. Section 4.3.2 of [RFC1034] has a resolution
   algorithm that includes CNAME processing but has been found to be
   unclear concerning the ultimate setting of RCODE in the case of such
   redirection. Section 2.1 of [RFC2308] implies that the RCODE should
   be set based on the last query cycle in the case of an xNAME chain,
   but Section 2.2.1 of [RFC2308] says that some servers don't do that!

When there is an xNAME chain, the RCODE field is set as follows:

   When an xNAME chain is followed, all but the last query cycle
   necessarily had no error. The RCODE in the ultimate DNS response
   MUST BE set based on the final query cycle leading to that
   response. If the xNAME chain was terminated by an error, it will
   be that error code. If the xNAME chain terminated without error,
   it will be zero.

4. Security Considerations

The AA header flag bit is not protected by DNSSEC [RFC4033]. To
secure it, secure communications are needed between the querying
resolver and the DNS server. Such security can be provided by DNS
transaction security, either TSIG [RFC2845] or SIG(0) [RFC2931].

An AD header flag bit and the RCODE in a response are not, in
general, protected by DNSSEC, so the same conditions as stated in the
previous paragraph generally apply to them; however, this is not
always true. In particular, if the following apply, then the AD bit
and an NXDOMAIN RCODE are protected by DNSSEC in the sense that the
querier can calculate whether they are correct:

1. The zone where an NXDOMAIN RCODE occurs or all the zones where the
   data whose authenticity would be indicated by the AD flag bit are
   signed zones.

2. The query or queries involved indicate that DNSSEC RRs are OK in
   responses.

3. The responses providing these indications are from servers that
   include the additional DNSSEC RRs required by DNSSEC.

4. The querier has appropriate trust anchor(s) and appropriately
   validates and processes the DNSSEC RRs in the response.

5. References

5.1. Normative References

   [RFC1034]   Mockapetris, P., "Domain names - concepts and
                facilities", STD 13, RFC 1034, November 1987.

   [RFC1035]   Mockapetris, P., "Domain names - implementation and
                specification", STD 13, RFC 1035, November 1987.

   [RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate
                Requirement Levels", BCP 14, RFC 2119, March 1997.

   [RFC2672]   Crawford, M., "Non-Terminal DNS Name Redirection",
                RFC 2672, August 1999.

   [RFC4035]   Arends, R., Austein, R., Larson, M., Massey, D., and S.
                Rose, "Protocol Modifications for the DNS Security
                Extensions", RFC 4035, March 2005.

5.2. Informative References

   [RFC2308]   Andrews, M., "Negative Caching of DNS Queries (DNS
                NCACHE)", RFC 2308, March 1998.

   [RFC2845]   Vixie, P., Gudmundsson, O., Eastlake 3rd, D., and B.
                Wellington, "Secret Key Transaction Authentication for
                DNS (TSIG)", RFC 2845, May 2000.

   [RFC2931]   Eastlake 3rd, D., "DNS Request and Transaction Signatures
                (SIG(0)s)", RFC 2931, September 2000.

   [RFC4033]   Arends, R., Austein, R., Larson, M., Massey, D., and S.
                Rose, "DNS Security Introduction and Requirements",
                RFC 4033, March 2005.

Author's Address

   Donald E. Eastlake 3rd
   Huawei R&D USA
   155 Beaver Street
   Milford, MA 01757

   Phone: +1-508-333-2270
   EMail: d3e3e3@gmail.com