Abstract

This document defines an extensible method to return additional information about the cause of DNS errors. Though created primarily to extend SERVFAIL to provide additional information about the cause of DNS and DNSSEC failures, the Extended DNS Errors option defined in this document allows all response types to contain extended error information.

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 January 9, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.
This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction and background ................................... 3
   1.1. Requirements notation .................................. 4
2. Extended Error EDNS0 option format ................................. 4
3. Use of the Extended DNS Error option .............................. 5
   3.1. The R (Retry) flag ................................... 5
   3.2. The RESPONSE-CODE field ................................ 5
   3.3. The INFO-CODE field ................................... 6
   3.4. The EXTRA-TEXT field .................................. 6
4. Defined Extended DNS Errors ...................................... 6
   4.1. INFO-CODEs for use with RESPONSE-CODE: NOERROR(0) ...... 6
       4.1.1. NOERROR Extended DNS Error Code 1 - Unsupported DNSKEY Algorithm .................................. 6
       4.1.2. NOERROR Extended DNS Error Code 2 - Unsupported DS Algorithm .................................. 6
       4.1.3. INFO-CODEs for use with RESPONSE-CODE: NOERROR(3) ................................ 7
       4.1.4. NOERROR Extended DNS Error Code 4 - Forged answer ................................ 7
       4.1.5. SERVFAIL Extended DNS Error Code 5 - DNSSEC Indeterminate ................................. 7
   4.2. INFO-CODEs for use with RESPONSE-CODE: SERVFAIL(2) ............................... 7
       4.2.1. SERVFAIL Extended DNS Error Code 1 - DNSSEC Bogus ................................ 7
       4.2.2. SERVFAIL Extended DNS Error Code 2 - Signature Expired ................................ 7
       4.2.3. SERVFAIL Extended DNS Error Code 3 - Signature Not Yet Valid ................................ 7
       4.2.4. SERVFAIL Extended DNS Error Code 4 - DNSKEY missing ................................ 7
       4.2.5. SERVFAIL Extended DNS Error Code 5 - RRSIGs missing ................................ 8
       4.2.6. SERVFAIL Extended DNS Error Code 6 - No Zone Key Bit Set ................................ 8
       4.2.7. SERVFAIL Extended DNS Error Code 7 - No Reachable Authority ................................ 8
       4.2.8. SERVFAIL Extended DNS Error Code 8 - NSEC Missing ................................ 8
       4.2.9. SERVFAIL Extended DNS Error Code 9 - Cached Error ................................ 8
       4.2.10. SERVFAIL Extended DNS Error Code 10 - Not Ready ................................ 8
   4.3. INFO-CODEs for use with RESPONSE-CODE: NOTIMP(4) ........... 8
       4.3.1. NOTIMP Extended DNS Error Code 1 - Deprecated ................................ 8
   4.4. INFO-CODEs for use with RESPONSE-CODE: REFUSED(5) ........... 8
1. Introduction and background

There are many reasons that a DNS query may fail, some of them transient, some permanent; some can be resolved by querying another server, some are likely best handled by stopping resolution. Unfortunately, the error signals that a DNS server can return are very limited, and are not very expressive. This means that applications and resolvers often have to "guess" at what the issue is — e.g. was the answer marked REFUSED because of a lame delegation, or because the nameserver is still starting up and loading zones? Is a SERVFAIL a DNSSEC validation issue, or is the nameserver experiencing a bad hair day?

A good example of issues that would benefit by additional error information are errors caused by DNSSEC validation issues. When a stub resolver queries a DNSSEC bogus name (using a validating resolver), the stub resolver receives only a SERVFAIL in response. Unfortunately, SERVFAIL is used to signal many sorts of DNS errors, and so the stub resolver simply asks the next configured DNS resolver. The result of trying the next resolver is one of two outcomes: either the next resolver also validates, a SERVFAIL is returned again, and the user gets an (largely) incomprehensible error message; or the next resolver is not a validating resolver, and the user is returned a potentially harmful result.

This document specifies a mechanism to extend (or annotate) DNS errors to provide additional information about the cause of the error. When properly authenticated, this information can be used by
the resolver to make a decision regarding whether or not to retry or it can be used or by technical users attempting to debug issues.

These extended error codes are specially useful when received by resolvers, to return to stub resolvers or to downstream resolvers. Authoritative servers MAY parse and use them, but most error codes would make no sense for them. Authoritative servers may need to generate extended error codes though.

1.1. Requirements notation

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. Extended Error EDNS0 option format

This draft uses an EDNS0 ([RFC2671]) option to include Extended DNS Error (EDE) information in DNS messages. The option is structured as follows:

```
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                            OPTION-CODE                        |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                           OPTION-LENGTH                       |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   RCODE                                         | R | Res       |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| INFO-CODE                                                     |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| EXTRA-TEXT ...                                                |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
```

Field definition details:

- OPTION-CODE, 2 octets (defined in [RFC6891]), for EDE is TBD.
- OPTION-LENGTH, 2 octets (defined in [RFC6891]) contains the length of the payload (everything after OPTION-LENGTH) in octets and should be 4 plus the length of the EXTRA-TEXT section (which may be a zero-length string).
- The RETRY flag, 1 bit; the RETRY bit (R) indicates a flag defined for use in this specification.
- The RESERVED bits, 4 bits: these bits are reserved for future use, potentially as additional flags. The RESERVED bits MUST be set to 0 by the sender and MUST be ignored by the receiver.
3. Use of the Extended DNS Error option

The Extended DNS Error (EDE) is an EDNS option. It can be included in any response (SERVFAIL, NXDOMAIN, REFUSED, etc) to a query that includes OPT Pseudo-RR [RFC6891]. This document includes a set of initial codepoints (and requests to the IANA to add them to the registry), but is extensible via the IANA registry to allow additional error and information codes to be defined in the future.

The fields of the Extended DNS Error option are defined further in the following sub-sections.

3.1. The R (Retry) flag

The R (Retry) flag provides a hint as to what the receiver may want to do with this annotated error. Specifically, the R (or Retry) flag provides a hint to the receiver that it should retry the query to another server. If the R bit is set (1), the sender believes that retrying the query may provide a successful answer next time; if the R bit is clear (0), the sender believes that the resolver should not ask another server.

The mechanism is specifically designed to be extensible, and so implementations may receive EDE codes that it does not understand. The R flag allows implementations to make a decision as to what to do if it receives a response with an unknown code - retry or drop the query. Note that this flag is only a suggestion. Unless a protective transport mechanism (like TSIG [RFC2845] or (D)TLS xref target="RFC7858"/> [RFC8094]) is used, the bit’s value could have been altered by a person-in-the-middle. Receivers can choose to ignore this hint. See the security considerations for additional considerations.

3.2. The RESPONSE-CODE field

This 12-bit value SHOULD be a copy of the combined RCODE from the extended RCODE field defined in the EDNS0 optional resource record (stored in the TTL field of the EDNS0 resource record [RFC2671]) and the 4 bits of the RCODE field of the DNS message. RESPONSE-CODEs MAY
use a different RCODE to provide additional or better information. For example, multiple EDNS0/EDE records may be included in the response and the supplemental EDNS0/EDE records may wish to include other RESPONSE-CODE values based on communication results with other DNS servers.

3.3. The INFO-CODE field

This 16-bit value provides the additional context for the RESPONSE-CODE value. This combination of the RESPONSE-CODE and the INFO-CODE serve as a joint-index into the IANA "Extended DNS Errors" registry.

Note to implementers: the combination of the RESPONSE-CODE and INFO-CODE fits within a 24-bit field, allowing implementers the choice of treating the combination as either two separate values, as defined in this document, or as a single 24-bit integer as long as the results are deterministic.

3.4. The EXTRA-TEXT field

The UTF-8-encoded, EXTRA-TEXT field may be zero-length, or may hold additional information useful to network operators.

4. Defined Extended DNS Errors

This document defines some initial EDE codes. The mechanism is intended to be extensible, and additional code-points can be registered in the "Extended DNS Errors" registry. This document provides suggestions for the R flag, but the originating server may ignore these recommendations if it knows better.

The RESPONSE-CODE and the INFO-CODE from the EDE EDNS option is used to serve as a double index into the "Extended DNS Error codes" IANA registry, the initial values for which are defined in the following sub-sections.

4.1. INFO-CODEs for use with RESPONSE-CODE: NOERROR(0)

4.1.1. NOERROR Extended DNS Error Code 1 - Unsupported DNSKEY Algorithm

The resolver attempted to perform DNSSEC validation, but a DNSKEY RRSET contained only unknown algorithms. The R flag should be set.

4.1.2. NOERROR Extended DNS Error Code 2 - Unsupported DS Algorithm

The resolver attempted to perform DNSSEC validation, but a DS RRSET contained only unknown algorithms. The R flag should be set.
4.1.3. INFO-CODEs for use with RESPONSE-CODE: NOERROR(3)

4.1.3.1. NOERROR Extended DNS Error Code 3 - Stale Answer

The resolver was unable to resolve answer within its time limits and
decided to answer with a previously cached data instead of answering
with an error. This is typically caused by problems on authoritative
side, possibly as result of a DoS attack. The R flag should not be
set, since retrying is likely to create additional load without
yielding a more fresh answer.

4.1.4. NOERROR Extended DNS Error Code 4 - Forged answer

For policy reasons (legal obligation, or malware filtering, for
instance), an answer was forged. The R flag should not be set.

4.1.5. SERVFAIL Extended DNS Error Code 5 - DNSSEC Indeterminate

The resolver attempted to perform DNSSEC validation, but validation
ended in the Indeterminate state. The R flag should not be set.

4.2. INFO-CODEs for use with RESPONSE-CODE: SERVFAIL(2)

4.2.1. SERVFAIL Extended DNS Error Code 1 - DNSSEC Bogus

The resolver attempted to perform DNSSEC validation, but validation
ended in the Bogus state. The R flag should not be set.

4.2.2. SERVFAIL Extended DNS Error Code 2 - Signature Expired

The resolver attempted to perform DNSSEC validation, a signature in
the validation chain was expired. The R flag should not be set.

4.2.3. SERVFAIL Extended DNS Error Code 3 - Signature Not Yet Valid

The resolver attempted to perform DNSSEC validation, but the
signatures received were not yet valid. The R flag should not be
set.

4.2.4. SERVFAIL Extended DNS Error Code 4 - DNSKEY missing

A DS record existed at a parent, but no supported matching DNSKEY
record could be found for the child. The R flag should not be set.
4.2.5. SERVFAIL Extended DNS Error Code 5 - RRSIGs missing
The resolver attempted to perform DNSSEC validation, but no RRSIGs could be found for at least one RRset where RRSIGs were expected.

4.2.6. SERVFAIL Extended DNS Error Code 6 - No Zone Key Bit Set
The resolver attempted to perform DNSSEC validation, but no Zone Key Bit was set in a DNSKEY.

4.2.7. SERVFAIL Extended DNS Error Code 7 - No Reachable Authority
The resolver could not reach any of the authoritative name servers (or they refused to reply). The R flag should be set.

4.2.8. SERVFAIL Extended DNS Error Code 8 - NSEC Missing
The resolver attempted to perform DNSSEC validation, but the requested data was missing and a covering NSEC or NSEC3 was not provided. The R flag should be set.

4.2.9. SERVFAIL Extended DNS Error Code 9 - Cached Error
The resolver has cached SERVFAIL for this query without additional information. The R flag should be set.

4.2.10. SERVFAIL Extended DNS Error Code 10 - Not Ready
The server is unable to answer the query as it is not fully up and functional yet.

4.3. INFO-CODEs for use with RESPONSE-CODE: NOTIMP(4)

4.3.1. NOTIMP Extended DNS Error Code 1 - Deprecated
The requested operation or query is not supported as its use has been deprecated. Implementations should not set the R flag. (Retrying request elsewhere is unlikely to yield any other results.)

4.4. INFO-CODEs for use with RESPONSE-CODE: REFUSED(5)

4.4.1. REFUSED Extended DNS Error Code 1 - Lame
An authoritative server that receives a query (with the RD bit clear) for a domain for which it is not authoritative SHOULD include this EDE code in the SERVFAIL response. A resolver that receives a query (with the RD bit clear) SHOULD include this EDE code in the REFUSED
response. Implementations should set the R flag in this case (another nameserver or resolver might not be lame).

4.4.2. REFUSED Extended DNS Error Code 2 - Prohibited

An authoritative or recursive resolver that receives a query from an "unauthorized" client can annotate its REFUSED message with this code. Examples of "unauthorized" clients are recursive queries from IP addresses outside the network, blacklisted IP addresses, local policy, etc.

Implementations SHOULD allow operators to define what to set the R flag to in this case.

4.5. INFO-CODEs for use with RESPONSE-CODE: NXDOMAIN(3)

4.5.1. NXDOMAIN Extended DNS Error Code 1 - Blocked

The resolver attempted to perform a DNS query but the domain is blacklisted due to a security policy implemented on the server being directly talked to. The R flag should be set.

4.6. INFO-CODEs for use with RESPONSE-CODE: NXDOMAIN(3)

4.6.1. NXDOMAIN Extended DNS Error Code 2 - Censored

The resolver attempted to perform a DNS query but the domain was blacklisted by a security policy imposed upon the server being talked to. Note that how the imposed policy is applied is irrelevant (in-band DNS somehow, court order, etc). The R flag should be set.

4.7. INFO-CODEs for use with RESPONSE-CODE: NXDOMAIN(3)

4.7.1. NXDOMAIN Extended DNS Error Code 3 - Stale Answer

The resolver was unable to resolve answer within its time limits and decided to answer with a previously cached NXDOMAIN answer instead of answering with an error. This is typically caused by problems on authoritative side, possibly as result of a DoS attack. The R flag should not be set, since retrying is likely to create additional load without yielding a more fresh answer.

5. IANA Considerations
5.1. A New Extended Error Code EDNS Option

This document defines a new EDNS(0) option, entitled "Extended DNS Error", assigned a value of TBD1 from the "DNS EDNS0 Option Codes (OPT)" registry [to be removed upon publication: [http://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml#dns-parameters-11]

<table>
<thead>
<tr>
<th>Value</th>
<th>Name</th>
<th>Status</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>TBD</td>
<td>Extended DNS Error</td>
<td>TBD</td>
<td>[This document]</td>
</tr>
</tbody>
</table>

5.2. New Double-Index Registry Table for Extended Error Codes

This document defines a new double-index IANA registry table, where the first index value is the combined RCODE value (see the Section 3.2 section) and the second index value is the INFO-CODE from the Extended DNS Error EDNS option defined in this document. The IANA is requested to create and maintain this "Extended DNS Error codes" registry. The codepoint space for each INFO-CODE index is to be broken into 3 ranges:

- 0 - 65023: Specification required.
- 65023 - 65279: First come, first served.
- 65280 - 65536: Experimental / Private use

A starting set of entries, based on the contents of this document, is as follows:

- RESPONSE-CODE: 0 (NOERROR)
  INFO-CODE: 1
  Purpose: Unsupported DNSKEY
  Reference: Section 4.1.1

- RESPONSE-CODE: 0 (NOERROR)
  INFO-CODE: 2
  Purpose: Unsupported DS Algorithm
  Reference: Section 4.1.2

- RESPONSE-CODE: 3 (NOERROR)
  INFO-CODE: 3
  Purpose: Answering with stale/cached data
  Reference: Section 4.1.3.1

- RESPONSE-CODE: 0 (NOERROR)
  INFO-CODE: 4
  Purpose: Forged answer
  Reference: Section 4.1.4
RESPONSE-CODE: 0 (NOERROR)
INFO-CODE: 5
Purpose: DNSSEC Indeterminate
Reference: Section 4.1.5

RESPONSE-CODE: 2 (SERVFAIL)
INFO-CODE: 1
Purpose: DNSSEC Bogus
Reference: Section 4.2.1

RESPONSE-CODE: 2 (SERVFAIL)
INFO-CODE: 2
Purpose: Signature Expired
Reference: Section 4.2.2

RESPONSE-CODE: 2 (SERVFAIL)
INFO-CODE: 3
Purpose: Signature Not Yet Valid
Reference: Section 4.2.3

RESPONSE-CODE: 2 (SERVFAIL)
INFO-CODE: 4
Purpose: DNSKEY missing
Reference: Section 4.2.4

RESPONSE-CODE: 2 (SERVFAIL)
INFO-CODE: 5
Purpose: RRSIGs missing
Reference: Section 4.2.5

RESPONSE-CODE: 2 (SERVFAIL)
INFO-CODE: 6
Purpose: No Zone Key Bit Set
Reference: Section 4.2.6

RESPONSE-CODE: 2 (SERVFAIL)
INFO-CODE: 7
Purpose: No NSEC records could be obtained
Reference: Section 4.2.8

RESPONSE-CODE: 2 (SERVFAIL)
INFO-CODE: 9
Purpose: The SERVFAIL error comes from the cache
Reference: Section 4.2.9

RESPONSE-CODE: 2 (SERVFAIL)
INFO-CODE: 10
Purpose: Not Ready.
Reference: Section 4.2.10

RESPONSE-CODE: 3 (NXDOMAIN)
INFO-CODE: 1
Purpose: Blocked
Reference: Section 4.5.1

RESPONSE-CODE: 3 (NXDOMAIN)
INFO-CODE: 2
Purpose: Censored
Reference: Section 4.6.1

RESPONSE-CODE: 3 (NXDOMAIN)
INFO-CODE: 3
Purpose: Answering with stale/cached NXDOMAIN data
Reference: Section 4.7.1

RESPONSE-CODE: 4 (NOTIMP)
INFO-CODE: 1
Purpose:
Reference: Section 4.4.2

RESPONSE-CODE: 5 (REFUSED)
INFO-CODE: 1
Purpose: Lame
Reference: Section 4.4.1

RESPONSE-CODE: 5 (REFUSED)
INFO-CODE: 2
Purpose: Prohibited
Reference: Section 4.4.2

6. Security Considerations

Though DNSSEC continues to be deployed, unfortunately a significant number of clients (~11% according to [GeoffValidation]) that receive a SERVFAIL from a validating resolver because of a DNSSEC validation issue will simply ask the next (potentially non-validating) resolver in their list, and thus don’t get any of the protections which DNSSEC should provide. This is very similar to a kid asking his mother if he can have another cookie. When the mother says "No, it will ruin your dinner!", going off and asking his (more permissive) father and getting a "Yes, sure, have a cookie!".

This information is unauthenticated information, and an attacker (e.g MITM or malicious recursive server) could insert an extended error response into already untrusted data -- ideally clients and resolvers would not trust any unauthenticated information, but until we live in
an era where all DNS answers are authenticated via DNSSEC or other mechanisms, there are some tradeoffs. As an example, an attacker who is able to insert the DNSSEC Bogus Extended Error into a packet could instead simply reply with a fictitious address (A or AAAA) record. The R bit hint and extended error information are informational — implementations can choose how much to trust this information and validating resolvers/stubs may choose to put a different weight on it.

7. Acknowledgements

The authors wish to thank Joe Abley, Mark Andrews, Stephane Bortzmeyer, Vladimir Cunat, Peter DeVries, Peter van Dijk, Donald Eastlake, Bob Harold, Evan Hunt, Geoff Huston, Shane Kerr, Edward Lewis, Carlos M. Martinez, George Michelson, Michael Sheldon, Petr Spacek, Ondrej Sury, Loganaden Velvindron, and Paul Vixie. They also vaguely remember discussing this with a number of people over the years, but have forgotten who all they were -- if you were one of them, and are not listed, please let us know and we'll acknowledge you.

I also want to thank the band "Infected Mushroom" for providing a good background soundtrack (and to see if I can get away with this!) Another author would like to thank the band "Mushroom Infectors". This was funny at the time we wrote it, but I cannot remember why...

8. References

8.1. Normative References


8.2. Informative References


Appendix A. Changes / Author Notes.

[RFC Editor: Please remove this section before publication ]

From -00 to -01:

- Address comments from IETF meeting.
- Document copying the response code
- Mention zero length fields are ok
- Clarify lookup procedure
- Mention that table isn’t done

From -03 to -IETF 00:

- Renamed to draft-ietf-dnsop-extended-error

From -02 to -03:

- Added David Lawrence -- I somehow missed that in last version.

From -00 to -01:

- Fixed up some of the text, minor clarifications.

Authors’ Addresses