Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: March 13, 2020

W. Kumari
Google
E. Hunt
ISC
R. Arends
ICANN
W. Hardaker
USC/ISI
D. Lawrence
Oracle + Dyn

September 10, 2019

Extended DNS Errors
draft-ietf-dnsop-extended-error-09

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 March 13, 2020.

Table of Contents

1. Introduction and background 3
1.1. Requirements notation 4
2. Extended Error EDNS0 option format 4
3. Defined Extended DNS Errors 5
3.1. Extended DNS Error Code 0 - Other 5
3.2. Extended DNS Error Code 1 - Unsupported DNSKEY Algorithm 5
3.3. Extended DNS Error Code 2 - Unsupported DS Algorithm 5
3.4. Extended DNS Error Code 3 - Stale Answer 5
3.5. Extended DNS Error Code 4 - Forged Answer 5
3.6. Extended DNS Error Code 5 - DNSSEC Indeterminate 5
3.7. Extended DNS Error Code 6 - DNSSEC Bogus 6
3.8. Extended DNS Error Code 7 - Signature Expired 6
3.9. Extended DNS Error Code 8 - Signature Not Yet Valid . . . 6
3.10. Extended DNS Error Code 9 - DNSKEY Missing 6
3.11. Extended DNS Error Code 10 - RRSIGs Missing 6
3.12. Extended DNS Error Code 11 - No Zone Key Bit Set 6
3.13. Extended DNS Error Code 12 - NSEC Missing 6
3.14. Extended DNS Error Code 13 - Cached Error 6
3.15. Extended DNS Error Code 14 - Not Ready 6
3.16. Extended DNS Error Code 15 - Blocked 7
3.17. Extended DNS Error Code 16 - Censored 7
3.18. Extended DNS Error Code 17 - Prohibited 7
3.19. Extended DNS Error Code 18 - Filtered 7
3.20. Extended DNS Error Code 19 - Stale NXDOMAIN Answer . . . 7
3.21. Extended DNS Error Code 20 - Lame 7
3.22. Extended DNS Error Code 21 - Deprecated 8
3.23. Extended DNS Error Code 22 - No Reachable Authority . . . 8
3.24. Extended DNS Error Code 23 - Network Error 8
4. IANA Considerations 8
4.1. A New Extended DNS Error Code EDNS Option 8
4.2. New Registry Table for Extended DNS Error Codes 8
5. Security Considerations 11
6. Acknowledgements 11
7. References 11

7.1. Normative References 11
7.2. Informative References 12
Authors' Addresses 12

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 some other failure?

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 name which is DNSSEC bogus (using a validating resolver), the stub resolver receives only a SERVFAIL in response. Unfortunately, the SERVFAIL Response Code (RCODE) is used to signal many sorts of DNS errors, and so the stub resolvers only option is to ask the next configured DNS resolver. The result of trying the next resolver is one of two outcomes: either the next resolver also validates, and a SERVFAIL is returned again or the next resolver is not a validating resolver, and the user is returned a potentially harmful result. With an Extended DNS Error (EDE) option enclosed in the response message, the resolver is able to return a more descriptive reason as to why any failures happened, or add additional context to a message containing a NOERROR RCODE.

This document specifies a mechanism to extend DNS errors to provide additional information about the cause of an error. These extended DNS error codes described in this document and can be used by any system that sends DNS queries and receives a response containing an EDE option.. Different codes are useful in different circumstances, and thus different systems (stub resolvers, recursive resolvers, and authoritative resolvers) might receive and use them.

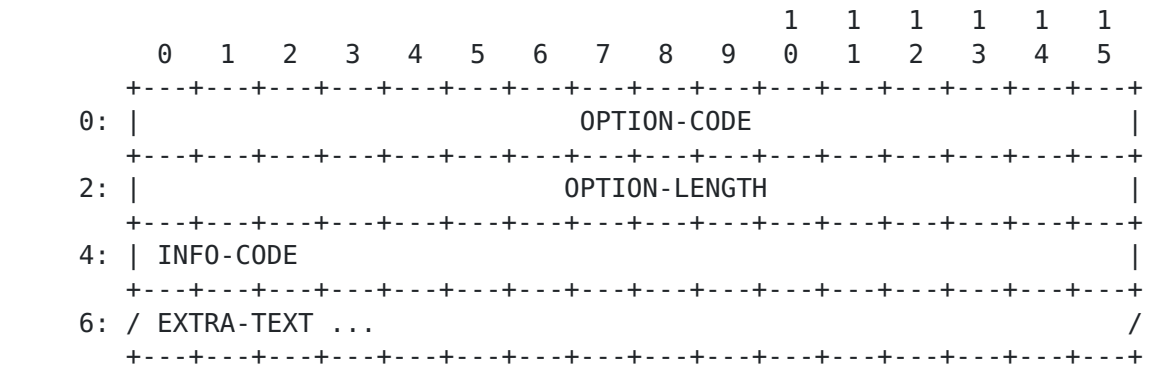
This document does not allow or prohibit any particular extended error codes and information be matched with any particular RCODEs. Some combinations of extended error codes and RCODEs may seem nonsensical (such as resolver-specific extended error codes in responses from authoritative servers), so systems interpreting the extended error codes MUST NOT assume that a combination will make sense. Receivers MUST be able to accept EDE codes and EXTRA-TEXT in all messages, including even those with a NOERROR RCODE.

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:



Field definition details:

- OPTION-CODE, 2 octets (defined in [RFC6891]]), for EDE is TBD. [RFC Editor: change TBD to the proper code once assigned by IANA.]
- 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).
- INFO-CODE, 16-bits, which is the principal contribution of this document. This 16-bit value, encoded in network (MSB) byte order, provides the additional context for the RESPONSE-CODE of the DNS message. The INFO-CODE serves as an index to the "Extended DNS Errors" registry Section 4.1.
- EXTRA-TEXT, a variable length, UTF-8 encoded, text field that may hold additional textual information. Note: EXTRA-TEXT may be zero octets in length, indicating there is no EXTRA-TEXT included. Care should be take not to leak private information that an observer would not otherwise have access to, such as account numbers.

The Extended DNS Error (EDE) option can be included in any response (SERVFAIL, NXDOMAIN, REFUSED, and even NOERROR, 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.

3. 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 Section 4.1. The INFO-CODE from the EDE EDNS option is used to serve as an index into the "Extended DNS Error" IANA registry, the initial values for which are defined in the following sub-sections.

3.1. Extended DNS Error Code 0 - Other

The error in question falls into a category that does not match known extended error codes. Implementations SHOULD include a EXTRA-TEXT value to augment this error code with additional information.

3.2. Extended DNS Error Code 1 - Unsupported DNSKEY Algorithm

The resolver attempted to perform DNSSEC validation, but a DNSKEY RRSET contained only unknown algorithms.

3.3. Extended DNS Error Code 2 - Unsupported DS Algorithm

The resolver attempted to perform DNSSEC validation, but a DS RRSET contained only unknown algorithms.

3.4. Extended DNS Error Code 3 - Stale Answer

The resolver was unable to resolve answer within its time limits and decided to answer with previously cached data instead of answering with an error. This is typically caused by problems communicating with an authoritative serever, possibly as result of a DoS attack against another network.

3.5. Extended DNS Error Code 4 - Forged Answer

For policy reasons (legal obligation, or malware filtering, for instance), an answer was forged.

3.6. Extended DNS Error Code 5 - DNSSEC Indeterminate

The resolver attempted to perform DNSSEC validation, but validation ended in the Indeterminate state.

3.7. Extended DNS Error Code 6 - DNSSEC Bogus

The resolver attempted to perform DNSSEC validation, but validation ended in the Bogus state.

3.8. Extended DNS Error Code 7 - Signature Expired

The resolver attempted to perform DNSSEC validation, but a signature in the validation chain was expired.

3.9. Extended DNS Error Code 8 - Signature Not Yet Valid

The resolver attempted to perform DNSSEC validation, but the signatures received were not yet valid.

3.10. Extended DNS Error Code 9 - DNSKEY Missing

A DS record existed at a parent, but no supported matching DNSKEY record could be found for the child.

3.11. Extended DNS Error Code 10 - RRSIGs Missing

The resolver attempted to perform DNSSEC validation, but no RRSIGs could be found for at least one RRset where RRSIGs were expected.

3.12. Extended DNS Error Code 11 - No Zone Key Bit Set

The resolver attempted to perform DNSSEC validation, but no Zone Key Bit was set in a DNSKEY.

3.13. Extended DNS Error Code 12 - NSEC Missing

The resolver attempted to perform DNSSEC validation, but the requested data was missing and a covering NSEC or NSEC3 was not provided.

3.14. Extended DNS Error Code 13 - Cached Error

The resolver has cached SERVFAIL for this query.

3.15. Extended DNS Error Code 14 - Not Ready

The server is unable to answer the query as it is not fully functional (yet).

3.16. Extended DNS Error Code 15 - Blocked

The resolver attempted to perfom a DNS query but the domain is blacklisted due to a security policy implemented on the server being directly talked to.

3.17. Extended DNS Error Code 16 - Censored

The resolver attempted to perfom 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 filtering, court order, etc).

3.18. Extended DNS Error Code 17 - 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.

3.19. Extended DNS Error Code 18 - Filtered

An authoritative or recursive resolver that receives a query from a client that had requested certain domains be filtered can annotate its REFUSED message with this code. Functionally, this amounts to "you requested that we filter domains like this one."

3.20. Extended DNS Error Code 19 - Stale NXDOMAIN Answer

The resolver was unable to resolve an answer within its configured time limits and decided to answer with a previously cached NXDOMAIN answer instead of answering with an error. This is typically caused by problems communicating with an authoritative serever, possibly as result of a DoS attack against another network.

3.21. Extended DNS Error Code 20 - 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.

3.22. Extended DNS Error Code 21 - Deprecated

The requested operation or query is not supported as its use has been deprecated.

3.23. Extended DNS Error Code 22 - No Reachable Authority

The resolver could not reach any of the authoritative name servers (or they refused to reply).

3.24. Extended DNS Error Code 23 - Network Error

An unrecoverable error occurred while communicating with another server.

4. IANA Considerations

4.1. A New Extended DNS 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]

Value	Name	Status	Reference
TBD	Extended DNS Error	TBD	[This document]

4.2. New Registry Table for Extended DNS Error Codes

This document defines a new IANA registry table, where the 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 code-point space for the INFO-CODE index is to be broken into 3 ranges:

- 0 - 32767: Expert Review [RFC2434].
- 32768 - 49151: First come, first served.
- 49152 - 65535: Experimental / Private use.

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

INFO-CODE: 0
Purpose: Other Error
Reference: Section 3.1

INFO-CODE: 1
Purpose: Unsupported DNSKEY Algorithm
Reference: Section 3.2

INFO-CODE: 2
Purpose: Unsupported DS Algorithm
Reference: Section 3.3

INFO-CODE: 3
Purpose: Stale Answer
Reference: Section 3.4

INFO-CODE: 4
Purpose: Forged Answer
Reference: Section 3.5

INFO-CODE: 5
Purpose: DNSSEC Indeterminate
Reference: Section 3.6

INFO-CODE: 6
Purpose: DNSSEC Bogus
Reference: Section 3.7

INFO-CODE: 7
Purpose: Signature Expired
Reference: Section 3.8

INFO-CODE: 8
Purpose: Signature Not Yet Valid
Reference: Section 3.9

INFO-CODE: 9
Purpose: DNSKEY Missing
Reference: Section 3.10

INFO-CODE: 10
Purpose: RRSIGs Missing
Reference: Section 3.11

INFO-CODE: 11
Purpose: No Zone Key Bit Set
Reference: Section 3.12

INFO-CODE: 12
Purpose: NSEC Missing
Reference: Section 3.13

INFO-CODE: 13
Purpose: Cached Error
Reference: Section 3.14

INFO-CODE: 14
Purpose: Not Ready.
Reference: Section 3.15

INFO-CODE: 15
Purpose: Blocked
Reference: Section 3.16

INFO-CODE: 16
Purpose: Censored
Reference: Section 3.17

INFO-CODE: 17
Purpose: Prohibited
Reference: Section 3.18

INFO-CODE: 18
Purpose: Filtered
Reference: Section 3.19

INFO-CODE: 19
Purpose: Stale NXDomain Answer
Reference: Section 3.20

INFO-CODE: 20
Purpose: Lame
Reference: Section 3.21

INFO-CODE: 21
Purpose: Deprecated
Reference: Section 3.22

INFO-CODE: 22
Purpose: No Reachable Authority
Reference: Section 3.23

INFO-CODE: 23
Purpose: Network Error
Reference: Section 3.24

5. 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 validaion 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 information is unauthenticated information, and an attacker (e.g a 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 [RFC2845] [RFC8094], 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.

6. Acknowledgements

The authors wish to thank Joe Abley, Mark Andrews, Vittorio Bertola, Stephane Bortzmeyer, Vladimir Cunat, Ralph Dolmans, Peter DeVries, Peter van Dijk, Donald Eastlake, Bob Harold, Paul Hoffman, Geoff Huston, Shane Kerr, Edward Lewis, Carlos M. Martinez, George Michelson, Michael Sheldon, Puneet Sood, 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.

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

7. References

7.1. Normative References

[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>.

[RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", RFC 2434, DOI 10.17487/RFC2434, October 1998, <https://www.rfc-editor.org/info/rfc2434>.

[RFC2671] Vixie, P., "Extension Mechanisms for DNS (EDNS0)", RFC 2671, DOI 10.17487/RFC2671, August 1999, <https://www.rfc-editor.org/info/rfc2671>.

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

7.2. Informative References

[GeoffValidation] IANA, "A quick review of DNSSEC Validation in today's Internet", June 2016, <http://www.potaroo.net/presentations/2016-06-27-dnssec.pdf>.

[RFC2845] Vixie, P., Gudmundsson, O., Eastlake 3rd, D., and B. Wellington, "Secret Key Transaction Authentication for DNS (TSIG)", RFC 2845, DOI 10.17487/RFC2845, May 2000, <https://www.rfc-editor.org/info/rfc2845>.

[RFC8094] Reddy, T., Wing, D., and P. Patil, "DNS over Datagram Transport Layer Security (DTLS)", RFC 8094, DOI 10.17487/RFC8094, February 2017, <https://www.rfc-editor.org/info/rfc8094>.

Authors' Addresses

Warren Kumari
Google
1600 Amphitheatre Parkway
Mountain View, CA 94043
US

Email: warren@kumari.net

Evan Hunt
ISC
950 Charter St
Redwood City, CA 94063
US

Email: each@isc.org

Roy Arends
ICANN

Email: roy.arends@icann.org

Wes Hardaker
USC/ISI
P.O. Box 382
Davis, CA 95617
US

Email: ietf@hardakers.net

David C Lawrence
Oracle + Dyn
150 Dow St
Manchester, NH 03101
US

Email: tale@dd.org