Network Working Group M. Andrews
Internet-Draft ISC
Intended status: Experimental March 28, 2014
Expires: September 29, 2014

EDNS EXPIRE OPTION
draft-andrews-dnsext-expire-04

Abstract

This document specifies a method for secondary DNS servers to honour the SOA EXPIRE field as if they were always transferring from the primary, even when using other secondaries to perform indirect transfers and refresh queries.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

The expire field of a DNS zone's SOA record [RFC 1035] is supposed to indicate when a secondary server shall discard the contents of the zone when it has been unable to contact the primary [RFC 1034]. Current practice only works when all the secondaries contact the primary directly to perform refresh queries and zone transfers.

While secondaries are expected to be able to, and often are configured to, transfer from other secondaries for robustness reasons as well as reachability constraints, there was no mechanism provided to preserve the expiry behaviour when using a secondary. Secondaries instead have to know whether they were talking directly to the primary or another secondary, and use that to decide whether to update the expire timer or not. This however fails to take into account delays in transferring from one secondary to another.

There are also zone transfer graphs in which the secondary never talks to the primary, so the effective expiry period becomes multiplied by the length of the zone transfer graph--which when it contains loops is infinite.

This document provides a mechanism to preserve the expiry behaviour regardless of what zone transfer graph is constructed and whether the secondary is talking to the primary or another secondary.

1.1. Reserved Words

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 [RFC 2119].

2. Expire EDNS option (Query)

The EDNS [RFC 6891] EXPIRE option has the value <TBA>. The EDNS EXPIRE option MAY included set on any QUERY, though usually this is only done on SOA, AXFR and IXFR queries involved in zone maintenance. This is done by adding a zero length EDNS EXPIRE option to the options field of the OPT record when the query is made.

3. Expire EDNS option (Response)

3.1. Primary Server

When the query is directed to the primary server for the zone, the response will be a EDNS EXPIRE option of length 4 containing the

value of the SOA EXPIRE field, in seconds and network byte order.

3.2. Secondary Server

When the query is directed to a secondary server for the zone, then the response will be an EDNS EXPIRE option of length 4 containing the value of the expire timer on that server, in seconds and network byte order.

3.3. Non-Authoritative Server

If an EDNS EXPIRE option is sent to a server that is not authoritative for the zone it MUST NOT add an EDNS EXPIRE option to the response.

4. Secondary Behaviour

When a secondary server performs a zone transfer request or performs a zone refresh query it SHALL add an EDNS EXPIRE option to the query message.

If a secondary receives an EDNS EXPIRE option in a response to a SOA query, it SHALL update its expire timer to be the maximum of the value returned in the EDNS EXPIRE option and the current timer value. Similarly, if a secondary receives an EDNS EXPIRE option in its response to an IXFR query which indicated the secondary is up to date (serial matches current serial) the secondary SHALL update the expire timer to be the maximum of the value returned in the EXPIRE EDNS option and the current timer value.

If the zone is transferred or updated as the result of an AXFR or IXFR query and there is an EDNS EXPIRE option with the response then the value of the EDNS EXPIRE option SHOULD be used instead of that of the SOA EXPIRE field to initialise the expire timer.

In all cases, if the value of SOA EXPIRE field is less than the value of the EDNS EXPIRE option, then the value of SOA EXPIRE field MUST be used and MUST be treated as a maximum when updating or initialising the expire timer.

5. IANA Considerations

IANA is requested to assign a EDNS option code point (Registry Name: DNS EDNS0 Options) for the EDNS EXPIRE option specified in Section 2 with "Optional" status.

6. Security Considerations

This ensures that servers that no longer have a connection to the primary server, direct or indirectly, cease serving the zone content when SOA EXPIRE timer is reached. This prevent stale data being served indefinitely.

The EDNS EXPIRE option exposes how long the secondaries have been out of communication with the primary server. This is not believed to be a problem and may provide some benefit to monitoring systems.

7. Normative References

[RFC 1034]
Mockapetris, P., "DOMAIN NAMES - CONCEPTS AND FACILITIES", STD 13, RFC 1034, November 1987.

[RFC 1035]
Mockapetris, P., "DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION", STD 13, RFC 1035, November 1987.

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

[RFC 6891]
Damas, J., Graff, M., and P. Vixie, "Extension Mechanisms for DNS (EDNS(0))", STD 75, RFC 6891, April 2013.

Author's Address

Mark P. Andrews
Internet Systems Consortium
950 Charter Street
Redwood City, CA 94063
US

Email: marka@isc.org