Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: 26 October 2022

S. Cheshire
Apple Inc.
T. Lemon
Apple Inc

24 April 2022

An EDNS0 option to negotiate Leases on DNS Updates
draft-ietf-dnssd-update-lease-01

Abstract

This document proposes a new EDNS0 option that can be used by DNS Update clients and DNS servers to include a lease lifetime in a DNS Update or response, allowing a server to garbage collect stale resource records that have been added by DNS Updates

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 https://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 26 October 2022.

Copyright Notice

Table of Contents

1. Introduction

Dynamic DNS Update [RFC2136] allows for a mapping from a persistent hostname to a dynamic IP address. This capability is particularly beneficial to mobile hosts, whose IP address may frequently change with location. However, the mobile nature of such hosts often means that dynamically updated resource records are not properly deleted. Consider, for instance, a mobile user who publishes address records via dynamic update. If this user moves their laptop out of range of the Wi-Fi access point, the address record containing stale information may remain on the server indefinitely. An extension to Dynamic Update is thus required to tell the server to automatically delete resource records if they are not refreshed after a period of time.

Note that overloading the resource record TTL [RFC1035] is not appropriate for purposes of garbage collection. Data that is susceptible to frequent change or invalidation, thus requiring a garbage collection mechanism, needs a relatively short resource record TTL to avoid polluting intermediate DNS caches with stale data. Using this TTL, short enough to minimize stale cached data, as a garbage collection lease lifetime would result in an unacceptable amount of network traffic due to refreshes (see Section 5 "Refresh Messages").

2. Conventions and Terminology Used in this Document

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 "Key words for use in RFCs to Indicate Requirement Levels", when, and only when, they appear in all capitals, as shown here [RFC2119] [RFC8174].

3. Mechanisms

The EDNS0 Update Lease option is included in a standard DNS Update message [RFC2136] within an EDNS(0) OPT pseudo-RR [RFC6891] with a new OPT and RDATA format proposed here. Encoding the Update Lease Lifetime in an OPT RR requires minimal modification to a name server's front-end, and will cause servers that do not implement this extension to automatically return a descriptive error (NOTIMPL).

4. Update Message Format

Dynamic DNS Update Leases Requests and Responses are formatted as standard DNS Dynamic Update messages [RFC2136], with the addition of a single OPT RR in the Additional section. Note that if a TSIG resource record is to be added to authenticate the update [RFC2845], the TSIG RR should appear *after* the OPT RR, allowing the message digest in the TSIG to cover the OPT RR.

The OPT RR is formatted as follows:

Field Name	Field Type	Description
NAME	domain name	empty (root domain)
TYPE	u_int16_t	OPT
CLASS	u_int16_t	0
TTL	u_int32_t	0
RDLEN	u_int16_t	describes RDATA

```
RDATA           byte stream   (see below)

RDATA Format:

Field Name       Field Type   Description
-------------------------------------------------------------
OPTION-CODE      u_int16_t    UPDATE-LEASE (2)
OPTION-LENGTH    u_int16_t    4 or 8
LEASE            u_int32_t    desired lease (request) or
                              granted lease (response), in seconds
KEY-LEASE        u_int32_t    optional desired (or granted)
                              lease for KEY records, in seconds
```


Figure 1

Update Requests contain, in the LEASE field of the OPT RDATA, an unsigned 32-bit integer indicating the lease lifetime, in seconds, desired by the client, represented in network (big-endian) byte order. In Update Responses, this field contains the actual lease granted by the server. The lease granted by the server may be less than, greater than, or equal to the value requested by the client. To reduce network and server load, a minimum lease of 30 minutes (1800 seconds) is RECOMMENDED. Leases are expected to be sufficiently long as to make timer discrepancies (due to transmission latency, etc.) between a client and server negligible. Clients that expect the updated records to be relatively static MAY request appropriately longer leases. Servers MAY grant relatively longer or shorter leases to reduce network traffic due to refreshes, or reduce stale data, respectively.

There are two variants of the EDNS(0) UPDATE-LEASE option, the basic (4-byte) variant and the extended (8-byte) variant.

In the basic (4-byte) variant, the LEASE indicated in the OPT RR applies to all resource records in the Update section.

In the extended (8-byte) variant, the Update Lease communicates two lease lifetimes. The LEASE indicated in the OPT RR applies to all resource records in the Update section *except* for KEY records. The KEY-LEASE indicated in the OPT RR applies to KEY records in the Update section. This variant is used specifically for supporting the DNS-SD Service Registration Protocol [I-D.ietf-dnssd-srp].

5. Refresh Messages

Resource records not to be deleted by the server MUST be refreshed by the client before the lease elapses. Clients SHOULD refresh resource records after 75% of the original lease has elapsed. If the client uses UDP and does not receive a response from the server, the client SHOULD re-try after 2 seconds. The client SHOULD continue to re-try, doubling the length of time between each re-try, or re-try using TCP.

5.1. Coalescing Refresh Messages

If the client has sent multiple updates to a single server, the client MAY include refreshes for all valid updates to that server in a single message. This effectively places all records for a client on the same expiration schedule, reducing network traffic due to refreshes. In doing so, the client includes in the refresh message all existing updates to the server, including those not yet close to expiration, so long as at least one resource record in the message

has elapsed at least 75% of its original lease. If the client uses UDP, the client MUST NOT coalesce refresh messages if doing so would cause truncation of the message; in this case, multiple messages or TCP should be used.

5.2. Refresh Message Format

Refresh messages are formatted like Dynamic Update Leases Requests and Responses (see Section 4 "Update Message Format"). The resource records to be refreshed are contained in the Update section. These same resource records are repeated in the Prerequisite section, as an "RRSet exists (value dependent)" prerequisite [RFC2136]. An OPT RR is the last resource record in the Additional section (except for a TSIG record, which, if required, follows the OPT RR). The OPT RR contains the desired new lease on Requests, and the actual granted lease on Responses. The Update Lease indicated in the OPT RR applies to all resource records in the Update section.

5.3. Server Behavior

Upon receiving a valid Refresh Request, the server MUST send an acknowledgment. This acknowledgment is identical to the Update

Response format described in Section 4 "Update Message Format", and contains the new lease of the resource records being refreshed. If no records in the Refresh Request have completed 50% of their leases, the server SHOULD NOT refresh the records; the response should contain the smallest remaining (unrefreshed) lease of all records in the refresh message. The server MUST NOT increment the SOA serial number of a zone as the result of a refresh.

6. Garbage Collection

If the Update Lease of a resource record elapses without being refreshed, the server MUST NOT return the expired record in answers to queries. The server MAY delete the record from its database.

7. Security Considerations

When DNS Update is enabled on an authoritative server, the Security Considerations of that specification [RFC2136] should be considered.

The addition of a record lifetime to facilitate automated garbage collection does not itself add any significant new security concerns.

8. IANA Considerations

The EDNS(0) OPTION CODE 2 has already been assigned for this DNS extension. No additional IANA services are required by this document.

9. Acknowledgments

Thanks to Marc Krochmal and Kiren Sekar to their work in 2006 on the precursor to this document. Thanks also to Roger Pantos and Chris Sharp for their contributions.

10. Normative References

[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>.

[RFC2136] Vixie, P., Ed., Thomson, S., Rekhter, Y., and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, DOI 10.17487/RFC2136, April 1997, <https://www.rfc-editor.org/info/rfc2136>.

[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>.

[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. Informative References

[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>.

[I-D.ietf-dnssd-srp]
Lemon, T. and S. Cheshire, "Service Registration Protocol for DNS-Based Service Discovery", Work in Progress, Internet-Draft, draft-ietf-dnssd-srp-12, 24 October 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-dnssd-srp-12>.

Authors' Addresses

Stuart Cheshire
Apple Inc.
One Apple Park Way
Cupertino, California 95014
United States of America
Phone: +1 408 974 3207
Email: cheshire@apple.com

Ted Lemon
Apple Inc
P.O. Box 958
Brattleboro, Vermont 05302
United States of America
Email: mellon@fugue.com