Authors: S. Cheshire   T. Lemon
         Apple Inc.   Apple Inc

An EDNS(0) option to negotiate Leases on DNS Updates

Abstract

This document describes an EDNS(0) option that can be used by DNS
Update requestors 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

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 EDNS(0) Update Lease option is included in a standard DNS Update message [RFC2136] within an EDNS(0) OPT pseudo-RR [RFC6891].

4. Update Message Format

Dynamic DNS Update Leases Requests and Responses are formatted as standard DNS Dynamic Update messages [RFC2136]. This update MUST include the EDNS(0) OPT RR, as described in [RFC6891]. This OPT RR MUST include an EDNS(0) Option as shown below. Note that if a TSIG resource record ([RFC2845]) is included to authenticate the update, the TSIG RR MUST appear *after* the OPT RR, allowing the message digest in the TSIG to cover the OPT RR.

The Update Lease EDNS(0) option is formatted as follows:

```
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 requestor, 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 requestor.

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 Update Lease option 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 Update Lease option applies to all resource records in the Update section *except* for KEY records. The KEY-LEASE indicated in the Update Lease option applies to KEY records in the Update section.

The reason the KEY record can be given a special lease time is that this record is used in the DNS-SD Service Registration Protocol [I-D.ietf-dnssd-srp] to reserve a name (or names) when the service is not present.

4.1. Requestor Behavior

DNS Update requestors SHOULD send an Update Lease option with any DNS Update that is not intended to be present indefinitely. The Update Lease option SHOULD specify a time interval that is no shorter than 30 minutes (1800 seconds). Requestors that expect the updated records to be relatively static MAY request appropriately longer leases.

If the DNS response received by the requestor does not include an Update Lease option, this is an indication that the DNS server does not support the Update Lease option. The requestor SHOULD in this case continue sending refresh messages (see below) as if the server had returned an identical update lease option in its response.

If the DNS response does include an Update Lease option, the requestor MUST use the interval(s) returned in this option when determining when to send Refresh messages. This is true both if the interval(s) returned by the server are shorter and if they are longer.

4.2. Server Behavior

DNS Servers implementing the Update Lease option MUST include an Update Lease option in response to any successful DNS Update (RCODE=0) that includes an Update Lease option. Servers MAY return different lease interval(s) than specified by the requestor, granting relatively longer or shorter leases to reduce network traffic due to Refreshes, or reduce stale data, respectively.

Note that both the 4-byte and 8-byte variant are valid on both clients and servers. If a server receives a 4-byte variant, it MUST respond with a 4-byte variant. If a client sends an 8-byte variant, it MUST accept either an 8-byte variant or a 4-byte variant in the response. If it receives a 4-byte variant, it MUST assume that both the key lease and update lease values are the same on the server.

5. Refresh Messages

A Refresh message is a DNS Update message that is sent to the server
after an initial DNS Update has been sent, in order to prevent the
updates records from being garbage collected.

5.1. Refresh Message Format

Refresh messages are formatted like Dynamic Update Leases Requests
and Responses (see Section 4 "Update Message Format"). The Refresh
message is constructed with the assumption that the result of the
previous update or Refresh is still in effect. The Refresh message
will, in the case that the records added in a previous update were
for some reason garbage collected, result in those records being
added again.

The Refresh message SHOULD NOT include any update prerequisites that
would, if the state produced by the previous update or Refresh is
still in effect, fail. The update SHOULD NOT be constructed to fail
in the case that the state produced by the previous update or
Refresh has for some reason been garbage collected.

An update message that changes the server state resulting from a
previous Refresh or update is an update, not a Refresh.

The Update Lease option in a Refresh contains the desired new lease
on Requests, and the actual granted lease on Responses. The LEASE
interval indicated in the Update Lease option applies to all
resource records in the Update section of the Refresh request,
except that if a KEY-LEASE interval is included as well, that
interval applies to any KEY records included in the Update section.

5.2. Requestor Behavior

A requestor that intends that its records from a previous update,
whether an initial update or a Refresh, remain active, MUST send a
Refresh message before the lease elapses, or else the records will
be removed by the server.

Requestors SHOULD Refresh resource records after 75% of the original
lease has elapsed. If the requestor uses UDP and does not receive a
response from the server, the requestor SHOULD retry after 2
seconds. The requestor SHOULD continue to retry, doubling the length
of time between each retry, or retry using TCP.

For Refresh messages, the server is expected to return an Update
Lease option, if supported, just as with the initial update. As with
the initial update, the requestor MUST use the interval(s) specified
by the server when determining when to send the next Refresh
message.

When sending Refresh messages, the requestor MUST include an Update
Lease option, as it did for the initial Update. The Update Lease
option MAY either specify the same intervals as in the initial
Update, or MAY use the values returned by the server in the previous
Update, whether it was an initial Update or a Refresh. As with
Update responses, the requestor MUST use the intervals returned by
the server in the response when determining when to send the next
refresh message.

5.2.1. Coalescing Refresh Messages

If the requestor has performed multiple successful updates with a
single server, the requestor MAY include Refreshes for all such
updates to that server in a single message. This effectively places
all records for a requestor on the same expiration schedule,
reducing network traffic due to Refreshes.

In doing so, the requestor 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 requestor
uses UDP, the requestor MUST NOT coalesce Refresh messages if doing
so would cause truncation of the message; in this case, either
multiple messages or TCP SHOULD be used.

Requestors SHOULD NOT send a Refresh messages when all of the
records in the Refresh have more than 50% of their lease interval
remaining before expiry. However, there may be cases where the
requestor needs to send an early refresh, and it MAY do so. For
example, a power-constrained device may need to send an update when
the radio is powered so as to avoid having to power it up later.

Another case where this may be needed is if the lease interval
registered with the server is no longer appropriate and the
Requestor wishes to negotiate a different lease interval. However,
in this case, if the server does not honor the requested interval in
its response, the requestor MUST NOT retry this negotiation.

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. The
server MUST NOT increment the SOA serial number of a zone as the
result of a Refresh.

However, the server's state may not match what the client expects.
In this case, a Refresh may actually appear to be an Update from the

server's perspective. In this case, if the Update changes the
contents of the zone, the server MUST update the zone serial number.

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. The
lease interval(s) returned by the server to the requestor are used
in determining when the lease on a resource record has expired.

For all resource records other than a KEY record included in an
update, the Update Lease is the LEASE value in the Update Lease
option. For KEY records, if the optional KEY-LEASE value was
included, this interval is used rather than the interval specified
in LEASE. If KEY-LEASE was not specified, the interval specified in
LEASE is used.

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. This document appears in the registry with the name 'UL'
and the status 'On-hold,' and a document reference to an older
version of this document. When this document has been approved, the
IANA is asked to update the registry, retaining the value '2',
changing the name 'UL' to 'Update Lease', changing the status to
'Standard' and changing the reference to refer to the final version
of this document published by the RFC Editor.

9. Acknowledgments

Thanks to Marc Krochmal and Kiren Sekar for their work in 2006 on
the precursor to this document. Thanks also to Roger Pantos and
Chris Sharp for their contributions. Thanks to Chris Box, Esko Dijk,
Jonathan Hui, Peter van Dijk, Abtin Keshvarzian, Nathan Dyck, Steve
Hanna, Gabriel Montenegro, and Kangping Dong for their reviews of
this document.

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-15, 14 September 2022, <https://www.ietf.org/archive/id/draft-ietf-dnssd-srp-15.txt>.

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