Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 24 May 2026

D. Powers
cnTnc LLC

20 November 2025

Authenticated Cache-Expiration Opcode (EXPIRE)
draft-powers-dnsop-expire-00

Abstract

This document defines a new DNS message opcode, EXPIRE, which enables an authenticated authoritative operator to request immediate deletion of a specific RRset from a resolver's cache. EXPIRE messages may be authenticated either through DNSSEC signatures or through resolver control-channel authentication (for example TSIG, mutually authenticated TLS, IPsec, or local trust policy). EXPIRE applies only to resolver cache and MUST NOT modify authoritative data.

Resolvers validate authority, apply mandatory replay protection using SOA serials when available or equivalent replay-mitigation mechanisms, and flush the targeted RRset upon successful validation. EXPIRE provides a deterministic, authenticated mechanism for cache rollback and correction across both signed (DNSSEC) and unsigned (internal) DNS deployments.

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 24 May 2026.

Copyright Notice

Table of Contents

1. Introduction 3
1.1. Terminology 3
2. Requirements Language 4
3. Motivation 4
4. EXPIRE Opcode and Message Format 4
4.1. Opcode Definition 4
4.2. Message Overview 4
4.3. Question Section 5
4.4. Answer (Update) Section 5
4.5. Additional Section - SOA for Replay Protection 6
4.6. Wildcard Prohibition 6
4.7. No Capability Signaling 6
5. Resolver Behavior 6
5.1. Authentication Profiles 6
5.2. DNSSEC Authentication Profile 7
5.3. Control-Channel Authentication Profile 7
5.4. Replay Protection 8
5.4.1. SOA Availability Rules 8
5.4.2. Alternative Replay Mechanisms 8
5.5. Cache Deletion 9
5.6. No RRset Matching 9
5.7. Follow-Up Queries 9
5.8. Response Behavior 9
6. Authoritative Behavior 10
7. Transport 10
8. Security Considerations 10
8.1. Timing-Based Cache Probing 11
8.2. Control-Channel Trust Model 11
8.3. Rate Limiting of EXPIRE Processing 11
9. Operational Considerations 11
9.1. Authorized Sender Lists 11
9.2. Use in Unsigned Zones 11
9.3. Resolver Clusters 12
9.4. Public vs. Private Deployment 12
10. IANA Considerations 12
11. Relationship to Existing Mechanisms 12
11.1. EXPIRE vs. NOTIFY (RFC 1996) 12

11.2. EXPIRE vs. Dynamic UPDATE (RFC 2136) 12
11.3. EXPIRE vs. Low TTLs 13
12. Examples 13
12.1. DNSSEC-Authenticated EXPIRE 13
12.2. Control-Channel-Authenticated EXPIRE (TSIG) 13
13. References 13
13.1. Normative References 14
13.2. Informative References 14
Author's Address 15

1. Introduction

DNS caching improves performance but complicates rollback and repair when resolvers retain stale or erroneous RRsets. The DNS protocol includes no authenticated in-band mechanism for a resolver to flush a cached RRset before TTL expiration.

This document defines a new DNS opcode, EXPIRE, which allows an authoritative operator, authenticated via DNSSEC or a resolver control channel, to instruct a resolver to delete a specific RRset from its cache. EXPIRE uses RFC 2136-style RRset deletion semantics (QCLASS=NONE) but applies strictly to resolver cache.

EXPIRE is intended to be deployable in both DNSSEC-signed environments and non-DNSSEC internal environments that already rely on TSIG, mutually authenticated TLS, IPsec, or equivalent control-channel mechanisms. This dual-profile model is analogous to the operational deployment of RFC 2136 Dynamic Update.

1.1. Terminology

EXPIRE: The DNS opcode defined in this document.

RRset: A set of resource records sharing owner name, type, and class.

Resolver: A recursive DNS server that maintains a cache.

Validating Resolver: A resolver that performs DNSSEC validation.

Control Channel: An authenticated resolver interface such as TSIG, mutually authenticated TLS, IPsec, or an implementation-specific management channel.

Authoritative Operator: Entity controlling publication of zone data.

2. Requirements Language

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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Motivation

Operators often require immediate cache correction due to erroneous publication, emergency failover, rollback of TLSA or SRV records, stale negative cache entries, or long TTLs. Existing mechanisms such as low TTLs, aggressive resigning, or manual outreach to resolver operators are operationally insufficient.

DNSSEC already defines a cryptographic authority model for signed zones. For internal, unsigned zones, operators typically rely on authenticated control channels (TSIG, mutually authenticated TLS, IPsec, or local ACLs) to manage resolvers. EXPIRE therefore defines two authentication profiles: a DNSSEC profile and a control-channel profile, each providing a standards-aligned way to authenticate EXPIRE without introducing new trust assumptions.

A particularly critical operational scenario involves rapid NS record updates during DDoS or routing incidents. When authoritative operators update NS records to redirect traffic away from attacked infrastructure, cached NS RRsets at resolvers may persist for the duration of their TTL -- potentially hours or days. EXPIRE enables authenticated, immediate cache invalidation of NS records, allowing traffic redirection in near-real-time during operational emergencies when seconds matter.

4. EXPIRE Opcode and Message Format

4.1. Opcode Definition

IANA is requested to assign a new DNS Opcode, EXPIRE (TBD), from the DNS OpCode registry.

4.2. Message Overview

EXPIRE uses the DNS UPDATE message structure defined in RFC 2136 for RRset deletion semantics (QCLASS=NONE). EXPIRE messages operate exclusively on resolver cache and MUST NOT modify authoritative data.

4.3. Question Section

The Question Section of an EXPIRE message MUST contain:

* QNAME: owner of the RRset to be expired;

* QTYPE: RRType to be expired;

* QCLASS: NONE (RFC 2136 RRset deletion semantics).

Resolvers receiving an EXPIRE message with QCLASS not equal to NONE MUST discard the message.

4.4. Answer (Update) Section

The content of the Answer Section depends on the authentication profile in use.

DNSSEC Authentication Profile When DNSSEC is used, the Answer Section MUST contain:

* a synthetic RRset whose owner name, type, and class match the Question;

* a valid RRSIG covering that RRset.

Resolvers MUST validate the RRSIG but MUST ignore the RDATA and TTL of the synthetic RRset. No comparison against cached RDATA is performed.

Control-Channel Authentication Profile When control-channel authentication is used, the Answer Section MAY be omitted. If present, it MAY contain a synthetic RRset, but no RRSIG is required and no DNSSEC fields need to be included.

A resolver implementing the control-channel profile MUST accept an EXPIRE message whose Question Section is the only populated section, assuming the control-channel authentication has succeeded.

This distinction allows DNSSEC environments to obtain in-band cryptographic proof of authority, while non-DNSSEC deployments avoid unnecessary overhead and may treat EXPIRE as a remote cache-management operation.

4.5. Additional Section - SOA for Replay Protection

The use of the SOA RRset in the Additional Section depends on the authentication profile.

DNSSEC Authentication Profile The Additional Section MUST contain the zone's SOA RRset and a valid RRSIG covering it. The resolver MUST validate the SOA RRSIG and use the SOA serial number as the basis for replay protection as described in Section 5.4.

Control-Channel Authentication Profile The Additional Section MAY contain an unsigned SOA RRset. If present, the resolver SHOULD use the SOA serial for replay protection as described in Section 5.4.

If no SOA is present, the resolver MAY rely on implementation-defined replay-protection mechanisms (nonces, per-sender counters, authenticated-session state, or other mechanisms providing equivalent or stronger guarantees).

4.6. Wildcard Prohibition

EXPIRE messages MUST NOT contain wildcard owner names in the Question Section. Resolvers receiving EXPIRE messages with wildcard QNAMEs MUST discard them.

4.7. No Capability Signaling

EXPIRE requires no explicit capability negotiation. Resolvers that do not implement EXPIRE SHOULD silently discard EXPIRE messages. Legacy resolvers MAY return NOTIMP or REFUSED in accordance with RFC 1035. Authoritative operators and control tools MUST treat NOTIMP, REFUSED, and silent discard as equivalent indicators of non-support. Resolvers that implement EXPIRE but reject it for policy reasons (e.g., rate-limiting, sender not authorized) SHOULD return SERVFAIL or NOTAUTH rather than NOTIMP.

5. Resolver Behavior

5.1. Authentication Profiles

A resolver that implements EXPIRE MUST authenticate EXPIRE messages using at least one of the following profiles:

* the DNSSEC Authentication Profile (Section 5.2) for signed zones; and/or

* the Control-Channel Authentication Profile (Section 5.3) for environments that do not deploy DNSSEC or that prefer resolver management channels.

Deployments MAY enable both profiles concurrently. If any enabled profile successfully authenticates the EXPIRE message, the resolver MAY proceed with EXPIRE processing.

5.2. DNSSEC Authentication Profile

A resolver using the DNSSEC profile MUST perform DNSSEC validation of the EXPIRE message components as follows:

* validate the RRSIG over the synthetic RRset in the Answer Section;

* validate the RRSIG over the SOA RRset in the Additional Section;

* confirm that the signer DNSKEY is authoritative for the zone according to the resolver’s DNSSEC validation policy;

* confirm that each RRSIG is within its validity interval;

* verify the cryptographic correctness of all signatures.

Any DNSSEC validation failure under this profile MUST cause the resolver to reject the EXPIRE message.

5.3. Control-Channel Authentication Profile

For zones that are unsigned or environments that do not deploy DNSSEC, resolvers MAY authenticate EXPIRE messages using an authenticated control channel. This model is equivalent to the trust assumptions used for RFC 2136 Dynamic UPDATE, RNDC, and other resolver management operations.

Acceptable forms of control-channel authentication include, but are not limited to:

* TSIG (RFC 8945) shared-secret authentication;

* DNS-over-TLS (RFC 7858) with mutual TLS authentication;

* DNS-over-HTTPS (RFC 8484) with client certificate authentication;

* IPsec-authenticated channels;

* locally configured trust anchors or resolver policy designating specific senders as authorized EXPIRE sources.

When control-channel authentication is used, resolvers MAY bypass DNSSEC validation of the EXPIRE message, including the synthetic RRset and SOA, but MUST still apply replay protection whenever SOA data or an equivalent replay mechanism is available (Section 5.4).

Implementations SHOULD provide configuration allowing administrators to specify "authorized EXPIRE senders" per zone or per resolver instance, using source addresses, TSIG key identities, TLS client identities, or other locally meaningful attributes.

5.4. Replay Protection

Resolvers implementing EXPIRE MUST implement replay protection to prevent stale EXPIRE messages from deleting more recent data. SOA serial numbers SHOULD be used when available.

5.4.1. SOA Availability Rules

When SOA-based replay protection is used, the resolver applies the following rules:

* If the targeted RRset is cached but the SOA for the corresponding zone is not cached, the resolver MAY perform a one-time SOA query in order to obtain the current SOA serial and apply serial-based replay protection.

* If neither the targeted RRset nor the SOA is cached, the resolver SHOULD treat the EXPIRE message as a no-op and MUST NOT initiate an SOA query solely due to receiving EXPIRE.

* If both the targeted RRset and the SOA are present in cache, the resolver MUST apply serial-based replay protection by comparing the EXPIRE-associated SOA serial (when provided) or a newly fetched SOA serial with the cached SOA serial, according to its policy.

If the resolver determines, by local policy, that the EXPIRE-associated serial is older than the cached serial, it MUST reject the EXPIRE message as a replay.

5.4.2. Alternative Replay Mechanisms

Under the control-channel profile, resolvers MAY implement alternative replay-protection mechanisms, such as nonces, per-sender monotonic counters, or authenticated session state, provided these mechanisms offer replay resistance at least as strong as SOA-serial-based checks.

5.5. Cache Deletion

A resolver MAY check whether the targeted RRset is present in cache prior to performing DNSSEC validation of the synthetic RRset. If the RRset is not present, the resolver MAY skip DNSSEC validation of the synthetic RRset but MUST still apply any available replay protection when SOA data or other replay mechanisms are present.

Upon successful authentication and replay protection, the resolver MUST:

* delete the cached RRset (QNAME, QTYPE);

* delete any negative cache entries for (QNAME, QTYPE);

* delete synthesized answers where QNAME is the target of a CNAME or DNAME chain, and any answers derived from DNAME expansions that incorporate the expired RRset.

Resolvers MUST NOT delete unrelated RRsets, including other RRTypes at QNAME, CNAME/DNAME records pointing to QNAME, or RRsets under other owner names.

5.6. No RRset Matching

Resolvers MUST NOT compare EXPIRE RDATA to cached RDATA, MUST NOT require matching RRSIGs, and MUST NOT consider TTL or RRset cardinality when deciding whether to delete the cached RRset. EXPIRE is a cache control signal, not a replacement data payload.

5.7. Follow-Up Queries

After processing EXPIRE, the resolver MAY immediately requery authoritative servers for (QNAME, QTYPE) or MAY wait until the next client query for that name and type. This behavior is an implementation choice and does not affect protocol correctness.

5.8. Response Behavior

Responding to EXPIRE messages is OPTIONAL. If a resolver chooses to respond, it SHOULD use the following RCODEs for interoperability:

NOERROR The EXPIRE message was successfully processed. This includes cases where the targeted RRset was not present in cache.

NOTAUTH Authentication failed (DNSSEC validation failed, control channel authentication failed, or sender was not in the authorized-sender list for this resolver or zone).

NOTIMP / REFUSED / FORMERR The resolver does not support EXPIRE or rejected the message as unsupported. Authoritative operators and control tools MUST treat these codes as equivalent to non-support.

Silent discard is permitted for all failure conditions.

6. Authoritative Behavior

Authoritative servers or associated front ends (such as DNS load balancers or policy engines) MAY originate EXPIRE messages. EXPIRE MUST NOT modify authoritative zone data. A valid DNSSEC signature or authenticated control channel proves authority, depending on the chosen authentication profile.

In control-channel deployments, EXPIRE is conceptually similar to existing RNDC or management-API operations that flush cache entries, but uses a standardized on-the-wire format suitable for multi-vendor and cross-network use.

7. Transport

EXPIRE uses UDP by default. TCP MAY be used when message size, operational policy, or transport characteristics require it.

When EXPIRE is carried over DNS-over-TLS (RFC 7858) or DNS-over-HTTPS (RFC 8484) with mutual TLS authentication (client certificate authentication), the control-channel authentication profile MAY rely on the TLS client identity as proof of authorization. Server-only TLS authentication (typical for public resolvers) does NOT satisfy the control-channel authentication requirements and MUST NOT be accepted as authorization for EXPIRE unless combined with another authentication mechanism such as TSIG or the DNSSEC authentication profile.

EXPIRE does not require a persistent channel or an explicit acknowledgement beyond the optional DNS response described in Section 5.8. Standard DNS transport rules apply.

8. Security Considerations

EXPIRE introduces no new authority beyond DNSSEC and existing resolver control-channel mechanisms. Under the DNSSEC authentication profile, EXPIRE is limited by the same trust model and failure modes as DNSSEC validation. Under the control-channel profile, EXPIRE inherits the security properties of the resolver’s management channel (TSIG, mutually authenticated TLS, IPsec, or local trust policy).

8.1. Timing-Based Cache Probing

EXPIRE may enable inference of cache state through timing analysis if resolvers exhibit observable behavioral differences when an RRset is present versus absent in cache. However, similar probing is already possible using ordinary DNS queries and cache-priming techniques. Resolvers SHOULD avoid introducing additional timing side channels beyond those inherent in normal DNS operation.

8.2. Control-Channel Trust Model

The control-channel authentication profile relies on the same trust relationships already used for RNDC, Dynamic Update, and resolver management APIs. Operators MUST ensure that these channels are appropriately protected (for example, with strong TSIG keys, mutually authenticated TLS, IPsec, or physically or logically isolated management networks).

8.3. Rate Limiting of EXPIRE Processing

Resolvers SHOULD apply per-zone or per-source rate limiting to EXPIRE processing to avoid excessive work caused by repeated EXPIRE messages for the same owner name. EXPIRE does not introduce a fundamentally new class of denial-of-service attack beyond those associated with DNSSEC validation and existing management operations, but implementers SHOULD ensure that EXPIRE handling remains within typical validation and management cost profiles.

9. Operational Considerations

9.1. Authorized Sender Lists

For the control-channel profile, operators SHOULD explicitly configure which entities are authorized to send EXPIRE messages, using ACLs, TSIG key lists, TLS client identity mappings, or equivalent mechanisms. These lists SHOULD be maintained with the same discipline as other management access-control lists.

9.2. Use in Unsigned Zones

Control-channel authentication allows EXPIRE to be safely deployed in internal DNS environments that do not sign their zones with DNSSEC. In such environments, EXPIRE behaves as a standardized remote cache-expiration command, authenticated by the same mechanisms already used for update and management.

9.3. Resolver Clusters

In clustered resolver deployments, implementations MAY propagate the effects of EXPIRE across cluster members using any appropriate internal mechanism. This document does not specify intra-cluster propagation semantics and considers them implementation-specific.

9.4. Public vs. Private Deployment

EXPIRE is intended to be safe for both public and private deployments. Resolvers and operators that do not wish to support EXPIRE simply ignore the opcode or return NOTIMP or REFUSED as described in Section 4.4, and no protocol-level harm results.

10. IANA Considerations

IANA is requested to assign a new DNS OpCode value for EXPIRE in the "DNS OpCodes" registry. The mnemonic is:

EXPIRE (TBD)

11. Relationship to Existing Mechanisms

11.1. EXPIRE vs. NOTIFY (RFC 1996)

NOTIFY alerts secondary nameservers of zone changes but does not provide cache invalidation for resolvers. NOTIFY targets only configured secondary nameservers, whereas EXPIRE can be directed to arbitrary resolvers. NOTIFY and EXPIRE serve complementary roles and may coexist in DNS deployments.

11.2. EXPIRE vs. Dynamic UPDATE (RFC 2136)

Dynamic UPDATE modifies authoritative zone data and requires zone transfer privileges or TSIG-based authorization for zone updates. EXPIRE modifies only resolver cache and requires only DNSSEC zone-signing authority (under the DNSSEC profile) or resolver management-channel access (under the control-channel profile). EXPIRE cannot add data or modify zone contents; it can only request deletion of cached RRsets.

The dual-profile model used by EXPIRE follows the precedent established by RFC 2136, which supports both SIG(0) (DNSSEC) and TSIG authentication.

11.3. EXPIRE vs. Low TTLs

Reducing TTL values increases query load on authoritative infrastructure and cannot retroactively affect RRsets that are already cached with longer TTLs. EXPIRE provides immediate, targeted cache invalidation independent of TTL values and avoids the operational overhead of maintaining artificially low TTLs for rollback scenarios.

12. Examples

12.1. DNSSEC-Authenticated EXPIRE

The following example illustrates an EXPIRE message using the DNSSEC authentication profile. The resolver validates the RRSIGs over the synthetic RRset and the SOA.

```
;; HEADER
OPCODE: EXPIRE
;; QUESTION
example.com.     NONE    A
;; ANSWER
example.com.     0    IN    A      0.0.0.0
example.com.     0    IN    RRSIG  A  <dnssec-signature>
;; ADDITIONAL
example.com.     0    IN    SOA ns1.example.com. admin.example.com. (
                      2025111901 3600 600 604800 300 )
example.com.     0    IN    RRSIG SOA <dnssec-signature>
```

12.2. Control-Channel-Authenticated EXPIRE (TSIG)

The following example illustrates an EXPIRE message using the control-channel authentication profile with TSIG. The Answer Section is empty; the resolver relies on the TSIG-authenticated channel and its local policy to authorize the operation.

```
;; HEADER
OPCODE: EXPIRE
;; QUESTION
example.com.     NONE    A
;; ANSWER
;;   (empty - allowed under control-channel profile)
;; ADDITIONAL
example-key.     TSIG    hmac-sha256.  <tsig-data>
;;   (note: TSIG appears in Additional section per RFC 8945)
;;   (optional unsigned SOA MAY also be included for replay protection)
```

13. References

13.1. 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>.

[RFC8945] Dupont, F., Morris, S., Vixie, P., Eastlake 3rd, D., Gudmundsson, O., and B. Wellington, "Secret Key Transaction Authentication for DNS (TSIG)", STD 93, RFC 8945, DOI 10.17487/RFC8945, November 2020, <https://www.rfc-editor.org/info/rfc8945>.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <https://www.rfc-editor.org/info/rfc4033>.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, DOI 10.17487/RFC4034, March 2005, <https://www.rfc-editor.org/info/rfc4034>.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, DOI 10.17487/RFC4035, March 2005, <https://www.rfc-editor.org/info/rfc4035>.

[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>.

13.2. Informative References

[RFC1996] Vixie, P., "A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)", RFC 1996, DOI 10.17487/RFC1996, August 1996, <https://www.rfc-editor.org/info/rfc1996>.

[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>.

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <https://www.rfc-editor.org/info/rfc7858>.

[RFC8484] Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018, <https://www.rfc-editor.org/info/rfc8484>.

Author’s Address

Duane Powers
cnTnc LLC
Email: dpowers@cntnc.com