Domain Name System Operations
Internet-Draft
Updates: 2136 (if approved)
Intended status: Standards Track
Expires: 19 December 2025

J. Abley
Cloudflare
P. Thomassen
deSEC, Secure Systems Engineering

17 June 2025

Indicating Non-Availability of Dynamic Updates in the DNS
draft-jabley-dnsop-missing-mname-01

Abstract

The Start of Authority Resource Record in the Domain Name System includes various parameters related to the handling of data in DNS zones. These parameters are variously used by authority-only servers, caching resolvers and DNS clients to guide them in the way that data contained within particular zones should be used.

One particular field in the SOA RR is known as MNAME, which is used to specify the "Primary Master" server for a zone. This is the server to which clients use Dynamic Update to send DNS UPDATE messages. Many zones do not support the Dynamic Update, and any such DNS UPDATE messages which are received provide no usual purpose. For such zones it may be preferable not to receive updates from clients at all.

This document proposes a convention by which a zone operator can signal to clients that a particular zone does not support Dynamic Update.

About This Document

This note is to be removed before publishing as an RFC.

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-jabley-dnsop-missing-mname/.

Discussion of this document takes place on the Domain Name System Operations Working Group mailing list (mailto:dnsop@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/dnsop/. Subscribe at https://www.ietf.org/mailman/listinfo/dnsop/.

Source for this draft and an issue tracker can be found at https://github.com/ableyjoe/draft-jabley-dnsop-missing-mname.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

[RFC2136] specifies a mechanism for clients to update zones in the DNS dynamically. This Dynamic Update mechanism is widely-deployed and is used, for example, to update DNS records in response to a local change of IP address.

Many zones, however, do not support Dynamic Update as a matter of policy. For such zones, specifying a DNS server name in the MNAME field of an SOA record has no benefit, and in fact may well cause unwanted DNS UPDATE traffic to be received by the named server.

This document proposes a convention by which a zone operator can signal to clients that a particular zone does not support Dynamic Update.

2. Terminology

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.

This document assumes familiarity with the terminology of the Domain Name System as described in [RFC9499].

This document uses the abbreviation SOA.MNAME to mean the MNAME field of the RDATA of an SOA Resource Record.

This document uses the phrase "Dynamic Update" to describe the general facility used by clients to request changes to DNS data published by authority servers, and "DNS UPDATE" to refer to the particular DNS messages used to make that happen. See [RFC2136] for more information about Dynamic Update.

3. Use of SOA.MNAME

The Start of Authority (SOA) Resource Record (RR) is defined in [RFC1035]. The MNAME field of the SOA RDATA (SOA.MNAME) is defined in that document as "The <domain-name> of the name server that was the original or primary source of data for this zone."

[RFC1035] includes no specific guidance on the use of SOA.MNAME, although the general tone in which SOA RDATA are discussed suggests that its intended purpose was for the management of zone transfers between authority-only servers. There are no known implementations of authority-only servers known to the author which use SOA.MNAME to manage or perform zone transfers, however; for bootstrapping reasons, commonly-deployed implementations require master servers to be specified explicitly, usually by address rather than name.

SOA.MNAME was subsequently referred to in [RFC1996] as part of the definition of the term "Primary Master". The server specified in SOA.MNAME was, by default, to be excluded from the set of servers to which DNS NOTIFY messages would be sent.

In [RFC2136] SOA.MNAME was again used to provide a definition of the term "Primary Master", in this case for the purpose of identifying the server towards which DNS UPDATE messages relating to that zone should be sent.

There have been no other references to the use of SOA.MNAME in the RFC series.

This document specifies a convention by which a zone operator may include an empty SOA.MNAME in order to deliberately specify that there is no appropriate place for Dynamic Update messages to be sent, i.e. that the corresponding zone does not support Dynamic Update.

4. Operations

4.1. DNS Software

DNS software MUST accept an empty value of SOA.MNAME as valid. This includes software that consumes, generates, collects, manages and validates DNS messages and software that provides related provisioning and user interfaces for zone administrators.

4.2. Zone Administrators

Zone administrators who do not wish to receive Dynamic Update messages from clients for a particular zone MAY specify an empty SOA.MNAME. The textual representation of an empty field in the canonical representation of zone data is a single ".", as illustrated in Figure 1.

```
@       1800    IN      SOA     administrator.example.org. . (
                                  20080622  ; serial
                                  1800      ; refresh
                                  900       ; retry
                                  10800     ; expire
                                  1800 )    ; negative cache TTL
```

Figure 1: SOA Resource Record with empty SOA.MNAME

4.3. Dynamic Update Clients

Dynamic Update clients who identify the recipient of DNS UPDATE messages from the value of SOA.MNAME SHOULD interpret an empty SOA.MNAME as an indication that Dynamic Updates are unsupported by that zone.

Dynamic Update clients SHOULD NOT send DNS UPDATE messages for zones whose SOA.NAME is empty.

5. Impact on Deployed Systems and Protocols

5.1. Impact on DNS NOTIFY

[RFC1996] specifies that the Primary Server, which is derived from SOA.MNAME, be excluded from the set of servers to which NOTIFY messages should be sent.

For zones where the value of SOA.MNAME record corresponds to a namserver listed in the apex NS RRSet, making the MNAME field empty might cause additional DNS NOTIFY traffic, since DNS NOTIFY messages that would have been suppressed towards the nameserver published as SOA.MNAME will instead be sent.

Authoritative DNS infrastructure deployed on a scale where high NOTIFY traffic is a concern often uses dedicated zone transfer servers, separate from the authoritative nameservers intended to receive queries from the Internet, and in that situation no additional DNS NOTIFY traffic would be expected. However, in other situations, the operators of the authority-only servers for the zone might choose to avoid any unwanted NOTIFY traffic by using an explicit notify list.

5.2. Impact on Dynamic Update

The goal of the convention specified in this document is to prevent Dynamic Update clients from sending DNS UPDATE messages for particular zones. The use of an empty SOA.MNAME is intended to prevent a Dynamic Update client from finding a server to send DNS UPDATE messages to.

5.3. Unintended Consequences

Some concern has been raised in the past that an empty SOA.MNAME might result in unwanted traffic being sent to root servers, e.g. for clients that might interpret the MNAME as a host name and try to use the DNS to find addresses for it.

Use of an empty SOA.MNAME is not new; cursory analysis of passive DNS data demonstrates a robust volume of DNS responses that include an empty SOA.MNAME for zones across a variety of top-level domains. No negative consequences of this traffic have been identified. See Appendix A for discussion.

6. Updates to RFC 2136

[RFC2136] is updated to reflect the interpretation of an empty SOA.MNAME to mean that the enclosing zone does not support Dynamic Update.

7. Security Considerations

The convention described in this document provides no additional security risks to DNS zone or server administrators.

Name servers which do not support Dynamic Update for the zones they host might experience a security benefit from reduced DNS UPDATE traffic by including an empty SOA.MNAME in those zones, since the absence of that unwanted traffic might provide additional headroom in network bandwidth and server capacity for legitimate and intended DNS traffic.

Clients that normally send DNS UPDATE messages might see a security benefit from not leaking the information contained within those messages to nameservers that are not configured to receive them.

8. IANA Considerations

This document makes no requests of the IANA.

9. References

9.1. 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/rfc/rfc1035>.

[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/rfc/rfc1996>.

[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/rfc/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/rfc/rfc2136>.

[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/rfc/rfc8174>.

9.2. Informative References

[RFC9499] Hoffman, P. and K. Fujiwara, "DNS Terminology", BCP 219, RFC 9499, DOI 10.17487/RFC9499, March 2024, <https://www.rfc-editor.org/rfc/rfc9499>.

Appendix A. Empty SOA.MNAME Observed in SOA Responses

A quick check using a variety of passive DNS datasets relating to observed traffic on 2024-10-30 reveals examples of responses with empty SOA.MNAME in the real world, as illustrated in Table 1. This perhaps suggests that a study with normalisation and a longer time base might be useful to include in a future revision of this draft.

source	counter	notes
com	109328	
net	8854	
org	1792	
czds	964	
imp	634	old gTLDs e.g. aero
opencc	111	see openintel website

Table 1: DNS Responses Observed with empty SOA.MNAME

Acknowledgments

Various participants in the DNSOP working group provided feedback to this idea when it was originally circulated in 2008. The names of the people have concerned have long since faded from memory, but the authors thank them generally and anonymously, regardless.

Raffaele Sommese helped quantify existing observed use of SOA responses with empty MNAME fields in a variety of passive DNS datasets, as summarised briefly in Appendix A.

Authors' Addresses

Joe Abley
Cloudflare
Email: jabley@cloudflare.com

Peter Thomassen
deSEC, Secure Systems Engineering
Email: peter@desec.io