

**Using DNAME in the DNS root zone for sinking of special-use TLDs**  
**draft-bortzmeyer-dname-root-04**

Abstract

This documents asks IANA to add DNAME records in the DNS root zone for TLDs which are in the Special-Use Domain Names registry, in order to ensure they receive an appropriate reply (NXDOMAIN) and that the root nameservers are not too bothered by them.

REMOVE BEFORE PUBLICATION: there is no obvious place to discuss this document. May be the IETF DNSOP (DNS Operations) group, through its mailing list (the author reads it). Or may AS112 operators mailing lists? The source of the document, as well as a list of open issues, is currently kept at Github [[1](#)].

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 July 20, 2018.

Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents

carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

<a href="#">1.</a>	Introduction and background . . . . .	<a href="#">2</a>
<a href="#">1.1.</a>	Requirements Terminology . . . . .	<a href="#">2</a>
<a href="#">2.</a>	Rules . . . . .	<a href="#">3</a>
<a href="#">3.</a>	Benefits . . . . .	<a href="#">3</a>
<a href="#">4.</a>	Possible issues . . . . .	<a href="#">3</a>
<a href="#">5.</a>	IANA Considerations . . . . .	<a href="#">4</a>
<a href="#">6.</a>	Security Considerations . . . . .	<a href="#">5</a>
<a href="#">7.</a>	Acknowledgments . . . . .	<a href="#">5</a>
<a href="#">8.</a>	References . . . . .	<a href="#">5</a>
<a href="#">8.1.</a>	Normative References . . . . .	<a href="#">5</a>
<a href="#">8.2.</a>	Informative References . . . . .	<a href="#">6</a>
<a href="#">8.3.</a>	URIs . . . . .	<a href="#">7</a>
	Author's Address . . . . .	<a href="#">8</a>

## [1.](#) Introduction and background

The DNS root nameservers receive a lot of requests for TLDs which do not exist. See for instance [[fujiwara-root-traffic](#)] or [[icann-1-root-stats](#)] or [[ssac-045](#)]. In the spirit of [[RFC7534](#)], it would be good if they could be redirected to a sink such as AS112, to save root nameservers's resources.

Some of these names, and specially one of the biggest offenders, .local ([[RFC6762](#)]), are registered in the Special-Use Domain Names registry [[2](#)] of [[RFC6761](#)]. They are obvious candidates for a "delegation" to the sink.

It is proposed to use the new AS112, the one described by [[RFC7535](#)] to implement this sink.

### [1.1.](#) Requirements Terminology

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 [[RFC2119](#)].



## 2. Rules

Every TLD ([\[RFC7719\]](#), [section 2](#)) which is in the Special-Use Domain Names registry [[3](#)] ([\[RFC6761\]](#)) SHOULD be "delegated" by IANA through a DNAME ([\[RFC6672\]](#)) to empty.as112.arpa as described in [\[RFC7535\]](#) if and only if the registration of this TLD say that resolvers SHOULD NOT or MUST NOT look them up in the DNS.

It is important to notice that this document does not define a policy to decide if a TLD should be "delegated" or not. Instead, it relies on the existing Special-Use Domain Names registry and its rules.

RFC-EDITOR: remove before publication. As of today, with these rules, .local ([\[RFC6762\]](#)) or .onion ([\[RFC7686\]](#)) would be "delegated" but not .example (its registration in [\[RFC6761\]](#) does not define special handling for resolvers) or .home ([\[RFC7788\]](#)) or .belkin (this last one generates a huge traffic at the root nameservers but is not in the Special-Use Domain Names registry).

## 3. Benefits

The main benefit is less load on the root nameservers and a better efficiency of the caches, therefore helping the entire DNS ecosystem.

## 4. Possible issues

Of course, the solution described in this document requires a good support of DNAME by the resolvers. [Appendix A of \[RFC7535\]](#) describes an experiment which was run in 2013 and which shows that, indeed, we can rely on DNAME (quoting the authors: "We conclude that there is no evidence of a consistent failure on the part of deployed DNS resolvers to correctly resolve a DNAME construct."). The technical tests documented in [\[damas-dname\]](#) have the same conclusion: DNAMEs work fine.

Currently, the root is managed both by ICANN and by Verisign, with an EPP link between them (see [\[iana-update\]](#)). There is no EPP mapping for DNAME "delegations", [\[RFC5731\]](#) does not envision this case. A project is under way, to create a new EPP extension for DNAME "delegation", see [\[I-D.bortzmeyer-regext-epp-dname\]](#). Of course, it is expected that this small technical problem is of little importance compared with the "Internet governance" problem of having ICANN allowing such DNAMEs (see [Section 5](#)).

Because DNAME require additional processing by the authoritative servers ([\[RFC6672\]](#), [section 3.2](#)), root name servers operators may estimate that it will add an unknown risk for them (at least, it will be more work for the server).



What could be the expected "saving" of resources by this "delegation"? Well-behaved resolvers should cache the NXDOMAIN (negative caching duration in the root zone is currently one day) but this covers only the requested name, not the whole TLD (until [\[RFC8020\]](#) is widely deployed and it would only partially solved the issue). There is also a concern that the requests for these non-existing TLDs are not issued by "proper" systems (because they are supposed to never leave the local network). If these requests are sent by badly programmed or badly configured systems, can we be sure they will honor the "delegation" and the caching? To summarise, it would be interesting to design and conduct an experiment to measure the expected effect. Ideas are welcome (the most obvious one, running a "delegation" during a moment then deleting it and comparing the results, is difficult to foresee, for political reasons).

To be sure AS112 could handle the load, AS 112 operators were consulted and expressed no objection.

Regarding DNSSEC, do note the future DNAMEs in the root zone will be signed, but the target, empty.as112.arpa, is not. See George Michaelson's message [\[4\]](#). So, it will not be possible to validate the answers. Not a problem since these requests should never have been sent to the root nameservers, anyway.

RFC-EDITOR: remove before publication. As of today, it exists apparently five nodes in the new AS112. There is no "official" "delegation" to it. Do note that, as a consequence of the new AS122 structure, it is not possible to see how many unofficial "delegations" exist (to see an example, see [sink.bortzmeyer.fr](#)).

## **5. IANA Considerations**

IANA is directed to add a DNAME in the root zone for every TLD which fits the rules of [Section 2](#).

RFC-EDITOR: remove before publication. There is currently no DNAME in the root zone. It is expected that the creation of the first one will require a top-down, multi-stakeholder, long and complicated process with a lot of meetings, reports by consultants and design teams. We already have one short mention of this possibility in [\[ssac-009\]](#), then one decision by ICANN [\[icann-idn-dname\]](#) to study the matter and one technical report made after that decision [\[damas-dname\]](#) ("This report found no failure in resolution nor in the ability to perform DNSSEC validation when DNAME was used in the root zone.")

TODO: if DNAMEs in the "real" root zone are delayed, is it possible/realistic for IANA to create an experimental root zone containing the



new AS112 "delegations", so that roots like Yeti could publish it and test it?

REMOVE BEFORE PUBLICATION: there are today TLDs with a DNAME at their apex (not the same thing): xn--kprw13d and xn--mgb3a4f16a.

## 6. Security Considerations

The requests for the TLD in the Special-Use Domain Names registry are typically NOT supposed to leak to the authoritative public name servers such as the ones of the root zone. If they do, it means a misconfiguration somewhere. The leak is independant on whether the name is "delegated" to AS112 or not. See [section 8 of \[RFC7534\]](#) for an analysis.

Nevertheless, privacy considerations have to be taken into account. Some people believe there are added risks, because the queries will be seen by AS112 servers which, unlike the root nameservers, are managed by many "random people". This means that population of people who can see the query streams is increased from the set of root nameserver operators and people that they share data with, to potentially anybody. There's no defence against a malefactor hijacking AS112 traffic, because in a real sense that traffic is intended to be hijacked.

## 7. Acknowledgments

Thanks to Paul Hoffman to say that it may be a good idea, for Patrik Faltstrom for documentation and research, for Joe Abley for tough proofreading and many suggestions, and for Ted Lemon to give the final impulse, with his [\[RFC8244\]](#).

## 8. References

### 8.1. Normative References

- [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>>.
- [RFC6672] Rose, S. and W. Wijngaards, "DNAME Redirection in the DNS", [RFC 6672](#), DOI 10.17487/RFC6672, June 2012, <<https://www.rfc-editor.org/info/rfc6672>>.
- [RFC6761] Cheshire, S. and M. Krochmal, "Special-Use Domain Names", [RFC 6761](#), DOI 10.17487/RFC6761, February 2013, <<https://www.rfc-editor.org/info/rfc6761>>.



- [RFC7534] Abley, J. and W. Sotomayor, "AS112 Nameserver Operations", [RFC 7534](#), DOI 10.17487/RFC7534, May 2015, <<https://www.rfc-editor.org/info/rfc7534>>.
- [RFC7535] Abley, J., Dickson, B., Kumari, W., and G. Michaelson, "AS112 Redirection Using DNAME", [RFC 7535](#), DOI 10.17487/RFC7535, May 2015, <<https://www.rfc-editor.org/info/rfc7535>>.
- [RFC7719] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", [RFC 7719](#), DOI 10.17487/RFC7719, December 2015, <<https://www.rfc-editor.org/info/rfc7719>>.

## 8.2. Informative References

- [damas-dname]  
Damas, J., "Report on the Assessment of Security and Stability Implications of the Use of DNAME Resource Records in the Root Zone of the DNS", May 2011, <<https://www.icann.org/news/announcement-2011-05-24-en>>.
- [fujiwara-root-traffic]  
Fujiwara, K., "2014 Root DITL Data analysis and TLD popularity analysis (OARC workshop)", October 2014, <<https://indico.dns-oarc.net/event/20/session/2/contribution/2/material/slides/4.pdf>>.
- [I-D.bortzmeyer-regext-epp-dname]  
Bortzmeyer, S., "EPP Mapping for DNAME delegation of domain names", [draft-bortzmeyer-regext-epp-dname-01](#) (work in progress), January 2018.
- [iana-update]  
Davies, K., "Update on IANA", October 2009, <<https://archive.icann.org/en/meetings/seoul2009/bitcache/IANA%20Update%20-%20Kim%20Davies,%20IANA-vid=7506&disposition=attachment&op=download.pdf>>.
- [icann-idn-dname]  
ICANN, "Adopted Board Resolutions - IDN Variants", March 2010, <<https://www.icann.org/resources/board-material/resolutions-2010-03-12-en#10>>.
- [icann-l-root-stats]  
"QTYPE values for most popular TLDs (ICANN's L-root server public statistics)", April 2016, <<http://stats.dns.icann.org/hedgehog/hedgehog.html>>.



- [RFC5731] Hollenbeck, S., "Extensible Provisioning Protocol (EPP) Domain Name Mapping", STD 69, [RFC 5731](#), DOI 10.17487/RFC5731, August 2009, <<https://www.rfc-editor.org/info/rfc5731>>.
- [RFC6762] Cheshire, S. and M. Krochmal, "Multicast DNS", [RFC 6762](#), DOI 10.17487/RFC6762, February 2013, <<https://www.rfc-editor.org/info/rfc6762>>.
- [RFC7686] Appelbaum, J. and A. Muffett, "The ".onion" Special-Use Domain Name", [RFC 7686](#), DOI 10.17487/RFC7686, October 2015, <<https://www.rfc-editor.org/info/rfc7686>>.
- [RFC7788] Stenberg, M., Barth, S., and P. Pfister, "Home Networking Control Protocol", [RFC 7788](#), DOI 10.17487/RFC7788, April 2016, <<https://www.rfc-editor.org/info/rfc7788>>.
- [RFC8020] Bortzmeyer, S. and S. Huque, "NXDOMAIN: There Really Is Nothing Underneath", [RFC 8020](#), DOI 10.17487/RFC8020, November 2016, <<https://www.rfc-editor.org/info/rfc8020>>.
- [RFC8244] Lemon, T., Droms, R., and W. Kumari, "Special-Use Domain Names Problem Statement", [RFC 8244](#), DOI 10.17487/RFC8244, October 2017, <<https://www.rfc-editor.org/info/rfc8244>>.
- [ssac-009] ICANN, "SAC 009 - Alternative TLD Name Systems and Roots: Conflict, Control and Consequences", March 2006, <<http://www.icann.org/committees/security/alt-tlds-roots-report-31mar06.pdf>>.
- [ssac-045] ICANN, "SAC 045 - Invalid Top Level Domain Queries at the Root Level of the Domain Name System", November 2010, <<https://www.icann.org/en/groups/ssac/documents/sac-045-en.pdf>>.

### 8.3. URIs

- [1] <https://github.com/bortzmeyer/ietf-dname-root>
- [2] <http://www.iana.org/assignments/special-use-domain-names/special-use-domain-names.xml>
- [3] <http://www.iana.org/assignments/special-use-domain-names/special-use-domain-names.xml>



- [4] [https://mailarchive.ietf.org/arch/msg/dnsop/JsPNz66aQE3-r3toawCV\\_ajocNo](https://mailarchive.ietf.org/arch/msg/dnsop/JsPNz66aQE3-r3toawCV_ajocNo)

Author's Address

Stephane Bortzmeyer  
AFNIC  
1, rue Stephenson  
Montigny-le-Bretonneux 78180  
France

Phone: +33 1 39 30 83 46  
Email: [bortzmeyer+ietf@nic.fr](mailto:bortzmeyer+ietf@nic.fr)  
URI: <http://www.afnic.fr/>

