Workgroup: dnsop
Internet-Draft: draft-ietf-dnsop-alt-tld-22
Published: 3 March 2023
Intended Status: Standards Track
Expires: 4 September 2023
Authors: W. Kumari P. Hoffman
Google ICANN

The ALT Special Use Top Level Domain

Abstract

This document reserves a TLD label, "alt" to be used in non-DNS contexts. It also provides advice and guidance to developers developing alternative namespaces.

[This document is being collaborated on in Github at <https://github.com/wkumari/draft-wkumari-dnsop-alt-tld>. The most recent version of the document, open issues, etc should all be available here. The authors (gratefully) accept pull requests.]

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 4 September 2023.

Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

Many Internet protocols need to name entities. Names that look like DNS names (a series of labels separated with dots) have become common, even in systems that are not part of the global DNS administered by IANA. This document reserves the top-level label "alt" (short for "alternative") as a special-use domain name ([RFC6761]). This top-level label can be used as the final (rightmost) label to signify that the name is not rooted in the global DNS, and that it should not be resolved using the DNS protocol.

In Section 3.1, the IANA is requested to add the .alt name to the "Special-Use Domain Name" registry. IANA sets aside names in that registry, as described in <https://www.iana.org/domains/reserved>.

Throughout the rest of this document, the top-level "alt" label is shown as ".alt" to match the common presentation form of DNS names.

The techniques in this document are primarily intended to address some of the issues discussed in [RFC8244], which contains additional background on the issues with special use domain names.

In this document, ".alt" was chosen for the special-use domain name instead of something like "alt.arpa" so that systems that use the name do not have to worry that a parent of their name would be resolved if the name leaked to the Internet. Historically, some systems that want to use non-DNS names wanted the entire name to be not in the DNS, and reserving ".alt" fulfills that use case.

1.1. Terminology

This document assumes familiarity with DNS terms; please see [RFC8499]. Terminology that is specific to this document is:

- DNS name: Domain names that are intended to be used with DNS resolution, either in the global DNS or in some other context.

- DNS context: The namespace anchored at the globally-unique DNS root, administered by IANA. This is the namespace or context that "normal" DNS uses.

- non-DNS context: Any other (alternative) namespace.

- pseudo-TLD: A label that appears in a fully-qualified domain name in the position of a TLD, but which is not part of the global DNS. This term is not intended to be pejorative.

- TLD: See the definition in Section 2 of [RFC8499].

1.2. Requirements 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.

2. The alt Namespace

This document reserves the .alt label for use as an unmanaged pseudo-TLD namespace. The .alt label can be used in any domain name as a pseudo-TLD to signify that this is an alternative (non-DNS) namespace, and should not be looked up in a DNS context.

This document uses ".alt" for the pseudo-TLD in the presentation format for the DNS, corresponding to a 0x03616c7400 suffix in DNS wire format. The on-the-wire formats for non-DNS protocols might be different.

Because names beneath .alt are in an alternative namespace, they have no significance in the regular DNS context. DNS stub and recursive resolvers do not need to look them up in the DNS context.

DNS resolvers that serve the DNS protocol and non-DNS protocols at the same time might consider .alt like a DNS entry in the "Transport-Independent Locally-Served DNS Zone Registry" that is part of IANA's "Locally-Served DNS Zones" registry, except that .alt is always used to denote names that are to be resolved by non-DNS

protocols. Note that this document does not request adding .alt to these registries because .alt, by definition, is not a DNS name.

Note that using .alt as a pseudo-TLD does not mandate how the non-DNS protocol will handle the name. To maximize compatibility with existing applications, it is suggested, but not required, that non-DNS protocols using names that end in .alt follow DNS name syntax. If the non-DNS protocol has a wire format like the DNS wire format, it might append the null label at the end of the name, but it also might not. This document does not make any suggestion for how non-DNS protocols deal with the wire format of their names.

Groups wishing to create new alternative namespaces may create their alternative namespace under a label that names their namespace under the .alt pseudo-TLD. This document defines neither a registry nor governance model for the .alt namespace, as it is not managed by the IETF or IANA. There is no guarantee of unambiguous mappings from names to name resolution mechanisms. Mitigation or resolution of collisions that occur under .alt are outside the scope of this document and outside the IETF's remit. Users are advised to consider the associated risks when using names under .alt.

Regardless of the expectations above, names in the .alt pseudo-TLD will leak outside the context in which they are valid. Decades of experience show that such names will appear at recursive resolvers, and will thus also appear at the root servers for the global DNS.

Sending traffic to the root servers that is known to always elicit an NXDOMAIN response, such as queries for names ending in .alt, wastes resources on both the resolver and the root server. Caching resolvers performing aggressive use of DNSSEC- validated caches (described in [RFC8198]) may mitigate this by synthesizing negative answers from cached NSEC records for names under .alt. Similarly, caching resolvers using QNAME minimization (described in [RFC9156]) will cause less of this traffic to the root servers because the negative responses will cover all names under .alt.

Currently deployed projects and protocols that are using pseudo-TLDs are recommended to move under the .alt pseudo-TLD, but this is not a requirement. Rather, the .alt pseudo-TLD is being reserved so that current and future projects of a similar nature have a designated place to create alternative resolution namespaces that will not conflict with the regular DNS context.

3. IANA Considerations

3.1. Special-Use Domain Name Registry

The IANA is requested to add the .alt name to the "Special-Use Domain Name" registry ([RFC6761]), and reference this document.

3.2. Domain Name Reservation Considerations

This section exists to meet the requirements of [RFC6761]. The questions posed in RFC 6761 were largely written assuming a DNS resolution system, and so some of the questions are not especially relevant or well suited.

1. Users might or might not recognize that names in the .alt pseudo-TLD as special.

2. Application software that uses alternative namespaces in the .alt pseudo-TLD are expected to have their own processing rules for their own names, probably in specialized resolver APIs, libraries, and/or application software. Application software that is not specifically designed to use names in the .alt pseudo-TLD are not expected to make their software recognize these names as special.

3. Writers of name resolution APIs and libraries that are specifically designed to implement resolution of an alternative name resolution system are expected to recognize names in the .alt pseudo-TLD as special and thus perform resolution of those names. The exact mechanism used by the name resolution APIs and libraries will obviously depend on the particular alternative resolution system. Regular DNS resolution APIs and libraries are not expected to recognize or treat names in the .alt pseudo-TLD differently.

4. Caching DNS servers SHOULD NOT recognize names in the .alt pseudo-TLD as special and SHOULD NOT perform any special handling with them.

5. Authoritative DNS servers SHOULD NOT recognize names in the .alt pseudo-TLD as special and should not perform any special handling with them.

6. DNS server operators will treat names in the .alt pseudo-TLD as they would names in any other TLD not in the global DNS. DNS server operators MAY be aware that queries for name ending in .alt are not DNS names, and queries for those names were leaked into the DNS context. This information can be useful for support or debugging purposes.

7. DNS registries/registrars for the global DNS will never register names in the .alt pseudo-TLD because .alt will not exist in the global DNS root.

4. Privacy Considerations

This document reserves .alt to be used to indicate that a name is not a DNS name. Unfortunately, these queries will undoubtedly leak

into the global DNS. This is a general problem with alternative name spaces and not confined to names ending in .alt.

For example, a value such as "somename.alt" could easily cause a privacy issue for any names in that namespace that are leaked to the Internet. In addition, if a name ending in .alt is sufficiently unique, long-lasting, and frequently leaks into the global DNS, then regardless of how the value is constructed, that value can act similar to a web cookie with all the associated downsides of (re-)identification.

5. Security Considerations

Because names in the .alt pseudo-TLD are explicitly outside of the DNS context, it is impossible to rely on any DNS-related security considerations. Care must be taken when mapping the pseudo-TLD into its corresponding non-DNS name resolution system in order to get whatever security is offered by that system.

6. Acknowledgements

We would like to thank Joe Abley, Mark Andrews, Erik Auerswald, Roy Arends, Ray Bellis, Vittorio Bertola, Marc Blanchet, John Bond, Stephane Bortzmeyer, David Cake, Vint Cerf, David Conrad, Steve Crocker, Vladimir Cunat, Brian Dickson, Ralph Droms, Robert Edmonds, Patrik Faltstrom, Bernd Fix, Christian Grothoff, Olafur Gudmundsson, Ted Hardie, Bob Harold, Wes Hardaker, Geoff Huston, Joel Jaeggli, John C Klensin, Eliot Lear, Ted Lemon, Edward Lewis, John Levine, George Michaelson, Ed Pascoe, Libor Peltan, Jim Reid, Martin Schanzenbach, Ben Schwartz, Arturo Servin, Peter Thomassen, Paul Vixie, Duane Wessels, Paul Wouters, and Suzanne Woolf for feedback.

This document was many years in the making, and we would like to sincerely apolgized for anyone who we forgot to credit.

We would also like to thank Rob Wilton for serving as Responsible AD for this document.

In addition, Andrew Sullivan was an author from adoption (2015) through version 14 (2021).

7. References

7.1. 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>.

[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>.

[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>.

7.2. Informative References

[RFC8198] Fujiwara, K., Kato, A., and W. Kumari, "Aggressive Use of DNSSEC-Validated Cache", RFC 8198, DOI 10.17487/RFC8198, July 2017, <https://www.rfc-editor.org/info/rfc8198>.

[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>.

[RFC8499] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", BCP 219, RFC 8499, DOI 10.17487/RFC8499, January 2019, <https://www.rfc-editor.org/info/rfc8499>.

[RFC9156] Bortzmeyer, S., Dolmans, R., and P. Hoffman, "DNS Query Name Minimisation to Improve Privacy", RFC 9156, DOI 10.17487/RFC9156, November 2021, <https://www.rfc-editor.org/info/rfc9156>.

Appendix A. Changes / Author Notes.

[RFC Editor: Please remove this section before publication]

From -21 to -22:

* Addressed issues from AD review - https://mailarchive.ietf.org/arch/msg/dnsop/aIkeZUqKDZzzseCPfiIJ9J6zYXc/

* Combined some of the acknowledgements into one paragraph.

From -20 to -21:

* During WGLC review, replaced the descriptive text with the requirements from RFC 6761 with a list. This in turn required adding in the BCP 14 boilerplate.

* During WGLC review, made a few more requested changes

From -19 to -20:

* Expanded the privacy considerations

* Clarified benefit of using aggressive NSEC

* Clarified that the .alt namespace is unmanaged and thus comes with risks.

* Added description of why .alt was chosen instead of alt.arpa

* Removed 2119 language because there are no MUSTs or SHOULDs

From -18 to -19:

* Document was discussed at IETF115

* Changed the intended status to Standards Track at the request of the responsible AD (Rob Wilton)

* Clarified that this only deals with some of the problems from RFC 8244

* Removed text telling protocol designers that they should differentiate their names from other designers

* Added a note that .alt names will leak out of the local context

* Reminded resolver operators that there are already ways to reduce .alt traffic to the root servers

* Moved the paragraph related to 6761 to the IANA Considerations section

* Strengthened the security considerations

* Added references for QNAME minimization and agressive NSEC caching

From -16 to -18:

* Lots of editorial fix-ups

* Fixed reference to RFC 8499

* Clarified presentation format for .alt

* Clarified that IANA will set aside the name when it goes into the 6761 registry

* Removed the loose registry for names under .alt

* Added back the required discussion for RFC 6761

From -15 to -16:

* Many simplifications to focus the document on the technical bits as much as possible, based on mailing list feedback.

* Removed unused references.

* Removed the RFC 2119 language because it is no longer used in the document.

* Added a non-normative IANA registry.

* Added Paul Hoffman as second author to help get the draft moving in the DNSOP WG again.

From -14 to -15:

* [Pinky]: Gee, Brain. What are we going to do tonight?

* [The Brain]: The same thing we do every 6 months, Pinky. Post a new version of this document, with only the version number changed.

From -13 to -14:

* Andrew asked to be removed as co-author, due to potential perception of CoI.

* Erik Auerswald provided Github issues and comments re: references and grammar.

From -12 to -13:

* Just bumping versions to prevent expiration.

From -08 to -12:

* Just bumping versions to prevent expiration.

* Updated references (aggressive-nsec is now RFC 8198, draft-ietf-dnsop-sutld-ps is now 8244).

From -07 to -08:

* Made it clear that this is only for non-DNS.

* As per Interim consensus, removed the "add this to local zones" text.

* Added a Privacy Considerations section

*Grammar fix -- "alternative" is more correct than "alternate", replaced.

From -06 to -07:

*Rolled up the GItHub releases in to a full release.

From -07.2 to -07.3 (GitHub point release):

Removed 'sandbox' at Stephane's suggestion - https://www.ietf.org/mail-archive/web/dnsop/current/msg18495.html

Suggested (in 4.1 bullet 3) that DNS libraries ignore these -- Bob Harold - https://mailarchive.ietf.org/arch/msg/dnsop/a_ruPf8osSzi_hCzCqOxYLXhYoA

Added some pointers to the SUTLD document.

From -07.1 to -07.2 (Github point release):

*Reverted the <TBD> string (at request of chairs).

*Added an editors note explaining the above.

*Removed some more background, editorializing, etc.

From -06 to -07.1 (https://github.com/wkumari/draft-wkumari-dnsop-alt-tld/tree/7988fcf06100f7a17f21e6993b781690b5774472):

*Replaced ALT with <TBD> at the suggestions of George.

From -05 to -06:

*Removed a large amount of background - we now have the (adopted) tldr document for that.

*Made it clear that pseudo-TLD is not intended to be pejorative.

*Tried to make it cleat that this is something people can choose to use - or not.

From -04 to -05:

*Version bump - we are waiting in the queue for progress on SUN, bumping this to keep it alive.

From -03 to -04:

*3 changes - the day, the month and the year (a bump to keep alive).

From -02 to -03:

* Incorporate suggestions from Stephane and Paul Hoffman.

From -01 to -02:

* Merged a bunch of changes from Paul Hoffman. Thanks for sending a git pull.

From -00 to 01:

* Removed the "delegated to new style AS112 servers" text -this was legacy from the omnicient AS112 days. (Joe Abley)

* Removed the "Advice to implemntors" section. This used to recommend that people used a subdomain of a domain in the DNS. It was pointed out that this breaks things badly if the domain expires.

* Added text about why we don't want to adminster a registry for ALT.

From Individual-06 to DNSOP-00

* Nothing changed, simply renamed draft-wkumari-dnsop-alt-tld to draft-ietf-dnsop-alt-tld

From -05 to -06

* Incorporated comments from a number of people, including a number of suggestion heard at the IETF meeting in Dallas, and the DNSOP Interim meeting in May, 2015.

* Removed the "Let's have an (optional) IANA registry for people to (opportinistically) register their string, if they want that option" stuff. It was, um, optional....

From -04 to -05

* Went through and made sure that I'd captured the feedback received.

* Comments from Ed Lewis.

* Filled in the "Domain Name Reservation Considerations" section of RFC6761.

* Removed examples from .Onion.

From -03 to -04

*Incorporated some comments from Paul Hoffman

From -02 to -03

*After discussions with chairs, made this much more generic (not purely non-DNS), and some cleanup.

From -01 to -02

*Removed some fluffy wording, tightened up the language some.

From -00 to -01.

*Fixed the abstract.

*Recommended that folk root their non-DNS namespace under a DNS namespace that they control (Joe Abley)

Authors' Addresses

Warren Kumari
Google
1600 Amphitheatre Parkway
Mountain View, CA, 94043
United States of America

Email: warren@kumari.net

Paul Hoffman
ICANN

Email: paul.hoffman@icann.org