

DNSOP
Internet-Draft
Intended status: Informational
Expires: January 3, 2018

W. Kumari
Google
July 2, 2017

The .internal TLD.
draft-wkumari-dnsop-internal-00

Abstract

It has become clear that many users would like to use the DNS resolution system for names which do not have meaning in the global context but do have meaning in a context internal to their network. This document reserves the string ".internal" for this purpose.

[Ed note: Text inside square brackets ([]) is additional background information, answers to frequently asked questions, general musings, etc. They will be removed before publication. RFC Editor: Please remove these before publication.]

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

[Ed note: This document is intended to drive discussion. It is clear that there has been a desire for an "[RFC 1918](#)-style" TLD for a long time; in its absence, people have just started using whatever seemed convenient. This document requests that the allocation of .internal for this use. There is no existing process for this - some of the purpose of this document is to explore the process implications.]

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 <http://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."

Internet-Draft

.internal

July 2017

This Internet-Draft will expire on January 3, 2018.

Copyright Notice

Copyright (c) 2017 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 (<http://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

1.	Introduction	2
1.1.	Requirements notation	3
2.	Use cases	3
3.	Why not use <existing name>?	4
3.1.	Why not use .alt?	4
3.2.	Why not use something.arpa?	5
3.3.	Why not use .local?	5
3.4.	Why not use .example?	5
4.	DNSSEC Considerations	5
4.1.	Scenario 1 - No DNSSEC, .internal not delegated	6
4.2.	Scenario 2 - DNSSEC, .internal not delegated	6
4.3.	Scenario 3 - DNSSEC, .internal delegated	6
5.	IANA Considerations	7
5.1.	Domain Name Reservation Considerations	7
6.	Security Considerations	8
7.	Acknowledgements	8
8.	References	8
8.1.	Normative References	8
8.2.	Informative References	9
Appendix A.	Changes / Author Notes.	9
	Author's Address	10

[1.](#) Introduction

Over the years, a number of strings have been used as pseudo-TLDs for namespaces that are disjoint (or separate) from the "global DNS" namespace. Common examples of these include .home and .corp. See [\[I-D.chapin-additional-reserved-tlds\]](#), [\[I-D.ietf-dnsop-sutld-ps\]](#) for more background information on this issue. The

Internet-Draft

.internal

July 2017

[\[I-D.ietf-dnsop-sutld-ps\]](#) document discusses the issues in depth, and should be considered required reading for understanding this document.

The [\[I-D.ietf-dnsop-alt-tld\]](#) document reserves a string to be used as a pseudo-TLD for non-DNS resolution contexts. However, it is clear that there is a significant use case for a similar string to be used for namespaces which are resolved using the DNS protocol, but which do not have a meaning in the global DNS context.

There is no way to prevent users from simply picking a string (such as .home) and starting to use it for internal use. Unfortunately, although these strings are supposed to only be used internally, there is ample evidence that they often leak into the global DNS, sometimes causing technical issues for the user of the no-longer internal name.

This document requests allocation of a string to be used as a pseudo-TLD for namespaces that are not part of the global DNS, but are meant to be resolved with the DNS protocol. A reasonable analogy is that this is to names as [\[RFC1918\]](#) is to IP addresses. Such a reservation should alleviate pollution, such as junk queries at the root, and potential collisions with other users of the namespace.

Note that there was a discussion of the .homenet delegation in the HOMENET WG, and the resulting decision was to **not** request that the name be delegated as a TLD for the IETF's use. This document has significant similarities to the .homenet case, but also significant differences. These include (in no particular order) the fact that the use case is significant broader, and that there is no urgency to the request and does not delay or create uncertainty for any protocol work.

[1.1.](#) Requirements notation

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.](#) Use cases

The ".internal" TLD can be used for any purpose where a non-global DNS name is needed.

This includes creating a namespace "behind" a Customer Premises Equipment (CPE). For example, the Belkin company used ".belkin" for this. British Telecom used ".home", and shipped devices named "bthomehub.home" [[BT HOME HUB](#)]). Additionally, internal resolution systems like Microsoft Active Directory have documentation that

Kumari

Expires January 3, 2018

[Page 3]

Internet-Draft

.internal

July 2017

suggests (or previously suggested) that administrators use ".corp" for these cases.

The .internal TLD is intended to address some of the issues documented in the Special-Use Domain Names Problem Statement [[I-D.ietf-dnsop-sutld-ps](#)] specifically (from the list in [Section 3](#)):

- 5.3: Intended use is covered by gTLD process, but the third party doesn't want to pay a fee.
- 5.4: Intended use is covered by some IETF process, but the third party doesn't want to follow the process.
- 5.6: Unaware that a name intended to be used only locally may nevertheless leak
- 5.7: Unaware that a name used locally with informal allocation may subsequently be allocated formally, creating operational problems.
- 18 There exists no safe, non-process-violating mechanism for ad-hoc assignment of Special-Use Domain Names.

Other use cases for .internal include its use in testing, prototyping, and benchmarking. Researchers have often needed to set up a fake root and namespace in order to test something, and have needed an arbitrarily chosen a name for a piece of network equipment which it not connected to the Internet.

[3.](#) Why not use <existing name>?

The IANA "Special Use Names" registry [[IANA.SUN](#)] already contains some names which, it could be argued, already meet this need. Unfortunately, many of these names (such as ".example") are either reserved for a specific use case, or are semantically unsuitable (for example, a CPE manufacturer would likely not find "Open a browser and connect to 'router.invalid'" acceptable).

This section discusses why existing strings in the Special-Use Domain Names registry ([[IANA.SUN](#)]) are not appropriate.

[3.1.](#) Why not use .alt?

The proposed .alt pseudo-TLD is specifically only for use as a pseudo-TLD for non-DNS resolution contexts. At one point .alt was being considered both for DNS and non-DNS resolution contexts, but, after much discussion it was decided that the DNSSEC implications (and desired behavior) meant that .alt should be reserved specifically for non-DNS resolution.

Kumari

Expires January 3, 2018

[Page 4]

Internet-Draft

.internal

July 2017

[3.2.](#) Why not use something.arpa?

This is indeed an interesting idea. I suspect that it fails the semantically desirable / understandable case, but is definitely worth further discussion. It may also cause issues when server operators override part of the .arpa domain in order to instantiate something.arpa.

[3.3.](#) Why not use .local?

.local is already in wide use and has special handling implemented for handing .local names. See [[RFC6762](#)] [Section 22.1](#) [Subsection 3](#), 4, 5.

[3.4.](#) Why not use .example?

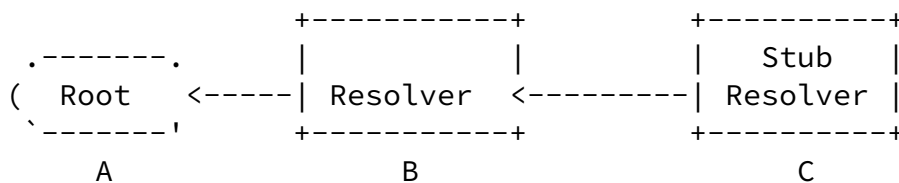
.example, .example.[com|net|org] may indeed be appropriate. Unfortunately, the hard part of all of this is not the selection and adding of a name to the "Special Use Names" registry, but rather deciding if this should be done and, if so, the process to interact with ICANN in order to achieve the delegation.

4. DNSSEC Considerations

The .internal TLD would be an unsigned TLD, as there is no (clean) way to sign it.

This particular topic received much discussion during the "Should .alt be used for DNS, or only non-DNS resolution" discussions, and was the cause of much confusion and misunderstandings. Much of this revolved around why it is important to have an insecure DNSSEC delegation for a name which is added to the Locally-Served DNS Zones ([\[IANA.LocallyServed\]](#)) registry, or any other case where a name is instantiated. It is briefly covered here, but interested readers should review the DNSOP mailing list archive for more details.

Take the following figure:



The user has just purchased a new CPE, which creates an internal namespace called .internal, and responds to lookups for router.internal with its (internal) management IP address (another example would be a corporate user at an organization which has

created a private internal namespace disconnected from the public, global DNS). The CPE hands out addresses using DHCP, and lists itself as the DNS server.

The user follows the instructions included in the box, and enters "http://router.internal" into a web browser. This causes a DNS lookup to be sent from the user's stub to the recursive resolver. The recursive resolver correctly identifies that this is query is for itself, and so responds with an answer saying "router.internal is 192.168.0.1".

4.1. Scenario 1 - No DNSSEC, .internal not delegated

In this scenario, the .internal name has not been added to the root zone, and the user's stub resolver *does not* perform DNSSEC

validation. The stub receives the response, performs no validation, and so trust the answer and connects. The user is happy. This is the current behavior for non-DNSSEC validating stubs.

[4.2.](#) Scenario 2 - DNSSEC, .internal not delegated

In this scenario, the .internal name has not been added to the root zone, and the user's stub resolver *does* perform DNSSEC validation. (Note that it is believed that validating stubs are currently rare.) The stub receives the response, and begins DNSSEC validation. As the .internal TLD has not been added to the root zone, DNSSEC Authenticated Denial of Existence proves that the .internal TLD does not exist (currently there is an NSEC record proving that nothing exists between .intel and .international). This resulting outcome is a DNSSEC "bogus" answer, the user is unable to connect, and becomes frustrated. This is the current behavior for DNSSEC validating stubs.

[4.3.](#) Scenario 3 - DNSSEC, .internal delegated

In this scenario, the .internal name has been added to the DNS root zone, with an insecure delegation to AS112 (by "insecure delegation" we mean that that there is no DS record for .internal in the root zone; the .internal domain is unsigned). The stub receives the response, and performs DNSSEC validation. As .internal has been delegated, there is an (insecure) entry in the root zone, proving that the .internal TLD exists. As it is an insecure delegation, the validating stub is perfectly happy to accept the "router.internal is 192.168.0.1" response, the user connects to their router, and everyone is happy.

[5.](#) IANA Considerations

This document requests that the .internal TLD be assigned to the IANA (similar to the way that .example is) and a DNSSEC insecure delegation (that is, a delegation with no DS records) be inserted into the root-zone, delegated to blackhole-[12].iana.org.

[Editor's note: This is not something which the IANA currently has

the authority to do. This fact was extensively discussed during the .homenet discussions. This text in the IANA considerations should be considered a placeholder for "what someone needs to do if this gets IETF consensus". If there is consensus that the reservation of .internal makes sense, there will need to be some process design before implementation. Such a process might be similar to "the IESG asks the IAB to request ICANN to consider the reservation / delegation of this string". ICANN does not currently have a process for handling requests like these, and so will also likely need to design a process for this. It is possible that either process might not be designed and this will fail. It is also possible that the IETF makes a request and ICANN does not make the delegation.]

5.1. Domain Name Reservation Considerations

[Ed: This section is to satisfy the requirement in [Section 5 of RFC6761](#). This document is intended to spark a discussion, there is currently no process for the IETF / IAB to request that ICANN delegate a TLD for special use, and simply adding .internal to the "Special-Use Domain Name" registry ([IANA.SUN](#)) does not accomplish this. I have decided to fill in the [RFC6761](#) "questions" simply to clarify the expected behavior. This entire section needs to be removed before publication.]

The string ".internal." is special in the following ways:

1. Users may know that strings that end in .internal behave differently to normal DNS names. They may expect that names of the form <something>.internal refer to resources internal to their network / enterprise / similar.
2. Writers of application software not required to perform any special handing for .internal names. They are resolved normally, using the DNS.
3. Writers of name resolution APIs and libraries are not expected to perform special handling.
4. Caching DNS servers MAY recognize these names as special. By default they should answer them locally (using "Locally Served

servers.

5. Authoritative DNS servers SHOULD NOT recognize these names as special and should not perform any special handling with them, unless they wish to instantiate an internal namespace, in which case they can choose to simply create any names within .internal that they want. Names are "local" to the network, and only have meaning within that network.
6. DNS server operators SHOULD be aware that queries for names ending in .internal are not part of the global, IANA DNS, and were leaked into the global DNS. This information may be useful for support or debugging purposes.
7. DNS Registries/Registrars MUST NOT grant requests to register ".internal" names in the normal way to any person or entity. These ".internal" names are defined by protocol specification to be nonexistent, and they fall outside the set of names available for allocation by registries/registrar.

6. Security Considerations

This section will certainly be filled in later as the discussion progresses.

7. Acknowledgements

The authors wish to thank Steve Crocker, Wes Hardaker, David Lawrence, Suzanne Woolf, and many others on the DNSOP mailing list.

The author would like to especially thank Paul Hoffman for creating a Pull Request.

8. References

8.1. Normative References

[I-D.ietf-dnsop-sutld-ps]

Lemon, T., Droms, R., and W. Kumari, "Special-Use Domain Names Problem Statement", [draft-ietf-dnsop-sutld-ps-06](#) (work in progress), June 2017.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.

8.2. Informative References

[BT_HOME_HUB]

IANA, "I have problems connecting 5GHz and dual band devices wirelessly to the BT Hub",
<http://bt.custhelp.com/app/answers/detail/a_id/44798/kw/bthomehub.home/c/346,7474,7477>.

[I-D.chapin-additional-reserved-tlds]

Chapin, L. and M. McFadden, "Additional Reserved Top Level Domains", [draft-chapin-additional-reserved-tlds-02](#) (work in progress), March 2015.

[I-D.ietf-dnsop-alt-tld]

Kumari, W. and A. Sullivan, "The ALT Special Use Top Level Domain", [draft-ietf-dnsop-alt-tld-08](#) (work in progress), March 2017.

[IANA.LocallyServed]

IANA, "Locally Served DNS Zones",
<<https://www.iana.org/assignments/locally-served-dns-zones/locally-served-dns-zones.xhtml>>.

[IANA.SUN]

IANA, "Special-Use Domain Names",
<<https://www.iana.org/assignments/locally-served-dns-zones/locally-served-dns-zones.xhtml>>.

[RFC1918] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G., and E. Lear, "Address Allocation for Private Internets", [BCP 5](#), [RFC 1918](#), DOI 10.17487/RFC1918, February 1996,
<<http://www.rfc-editor.org/info/rfc1918>>.

[RFC6762] Cheshire, S. and M. Krochmal, "Multicast DNS", [RFC 6762](#), DOI 10.17487/RFC6762, February 2013,
<<http://www.rfc-editor.org/info/rfc6762>>.

Appendix A. Changes / Author Notes.

[RFC Editor: Please remove this section before publication]

-00

- o This document was originally started in late 2014 / early 2015, but languished until being revived in June 2017.

Internet-Draft

.internal

July 2017

Author's Address

Warren Kumari
Google
1600 Amphitheatre Parkway
Mountain View, CA 94043
US

Email: warren@kumari.net

Kumari

Expires January 3, 2018

[Page 10]