SAC113
SSAC Advisory on Private-Use TLDs

An Advisory from the ICANN Security and Stability Advisory Committee (SSAC)
18 September 2020

Preface

This is an advisory to the ICANN Board, the ICANN Organization staff, the ICANN community, and, more broadly, the Internet community from the ICANN Security and Stability Advisory Committee (SSAC) about private-use TLDs.

The SSAC focuses on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., pertaining to the correct and reliable operation of the root zone publication system), administrative matters (e.g., pertaining to address allocation and Internet number assignment), and registration matters (e.g., pertaining to registry and registrar services). SSAC engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly. The SSAC has no authority to regulate, enforce, or adjudicate. Those functions belong to other parties, and the advice offered here should be evaluated on its merits.

Table of Contents

Executive Summary

In this document, the SSAC recommends the reservation of a DNS label that does not (and cannot) correspond to any current or future delegation from the root zone of the global DNS. This label can then serve as the top-level domain name (TLD) of a privately resolvable namespace that will not collide with the resolution of names delegated from the root zone. In order for this to work properly, this reserved private-use TLD must never be delegated in the global DNS root.

Currently, many enterprises and device vendors make ad hoc use of TLDs that are not present in the root zone when they intend the name for private use only. This usage is uncoordinated and can cause harm to Internet users.

The DNS has no explicit provision for internally-scoped names, and current advice is for the vendors or service providers to use a sub-domain of a public domain name for internal, or private use. Using sub-domains of registered public domain names is still the best practice to name internal resources. The SSAC concurs with this best practice, and encourages enterprises, device vendors, and others who require internally-scoped names to use sub-domains of registered public domain names whenever possible. However, this is not always feasible and there are legitimate use cases for private-use TLDs.

The need for private-use identifiers is *not* unique for domain names, and a useful analogy can be drawn between the uses of private IP address space and those of a private-use TLD. Network operators use private IP address space to number resources not intended to be externally accessible, and private-use TLDs are used by network operators in a similar fashion. This document proposes reserving a string in a manner similar to the current use of private IP address space. A similar rationale can be used to reserve more strings in case the need arises.

This document does not recommend a specific string for reservation. Instead, criteria are provided in *Section 4.1* to guide the decision on which string to choose and assist the ICANN Board in making its determination. Four criteria are provided to help guide this decision and reasoning is provided for each.

This advisory takes a pragmatic approach to an issue that the DNS allows by its design. Because of the decentralized nature of the DNS, there is no way to prevent ad hoc use of a TLD, rather than use of an explicitly reserved private string as this advisory recommends. Nevertheless, the SSAC believes that the reservation of a private string will help to reduce the ad hoc usage, provide greater predictability for network administrators and equipment vendors, and, over time, reduce erroneous queries to root servers.

1 Introduction

Many enterprises and device vendors use locally-defined domain names to support their applications and infrastructure in the form of a name within a hierarchy rooted in a TLD that is not present in the root zone.[1] Such a TLD looks just like the familiar top-level domain names used in email addresses and web URLs in the public Internet, but is only useful within a local network environment such as a user's home or a company's enterprise environment, or as part of accessing a local Intranet in a hotel or in a coffee shop.

Currently, the use of TLDs in this manner is ad hoc. Due to the lack of a convention for private use, such ad hoc TLD usage is prone to many problems. Some of these are described in previous SSAC Advisories[2,3,4,5,6,7] and are being studied as part of the Name Collision Analysis Project.[8]

The need for private-use identifiers is *not* unique to domain names. The Internet Protocol (IP) addressing environment has encountered similar situations when enterprises needed to use IP addresses specifically not routable in the public Internet. The response was to designate a part of the IP address space as reserved for private use.[9,10] A similar designation has been made for private autonomous system (AS) numbers as well.[11] This advisory recommends a course of action that is comparable to the local-use reservations in IPv4, IPv6, and the AS number space: namely, the reservation of a special string for private use.

The SSAC believes that the reservation of a string provided for this purpose will help to alleviate many of the problems stemming from ad hoc TLD use, primarily by grouping this ad hoc usage under one, well-known string.

This document is organized as follows: The rest of *Section 1* introduces the terminology used in the document as well as the scope of this advisory. *Section 2* describes the ad hoc usage of TLDs and the need for the reservation of a namespace for private use. In *Section 3*, the SSAC compares private IP address space to the proposal outlined in this document. *Section 4* contains SSAC's proposal, and *Section 5* has a specific recommendation to the ICANN Board.

---

[1] An example of this is that a number of companies have internally used .corp to name devices within the organization.
[2] See SAC045: Invalid Top Level Domain Queries at the Root Level of the Domain Name System
[3] See SAC057: SSAC Advisory on Internal Name Certificates
[4] See SAC062: SSAC Advisory Concerning the Mitigation of Name Collision Risk
[5] See SAC064: SSAC Advisory on Search List Processing
[6] See SAC078: SSAC Advisory on Uses of the Shared Global Domain Name Space
[7] See SAC090: SSAC Advisory on the Stability of the Domain Namespace
[8] See Name Collision Analysis Project (NCAP) Study 1, https://www.icann.org/public-comments/ncap-study-1-2020-02-13-en
[9] See RFC 1918, Address Allocation for Private Internets, https://datatracker.ietf.org/doc/rfc1918/
[10] See RFC 4193, Unique Local IPv6 Unicast Addresses, https://datatracker.ietf.org/doc/rfc4193/
[11] See RFC 6996, Autonomous System (AS) Reservation for Private Use, https://datatracker.ietf.org/doc/rfc6996/

1.1 Terminology and Scope of Work

private-use TLD
A domain name label that is used (or is intended to be used) ad hoc as the top-level domain name (TLD) of a privately resolvable namespace that is separate from the global namespace resolved from the public DNS root. The separation depends on the fact that the private-use TLD is not a valid public root zone delegation.

reserved private-use TLD
A domain name label that is explicitly reserved for use as the top-level domain name (TLD) of a privately resolvable namespace that will not collide with the resolution of names delegated from the root zone.

.internal
An example string used throughout this document for discussion purposes. It is used in this document as the *hypothetical* example of a reserved private-use TLD. Neither this string nor any other is specifically recommended in this document.

In this document, the SSAC limits its discussion to private-use TLDs intended for use with the DNS protocol and for private use only. Many private-use TLDs, such as .onion and .gnu, do not use the DNS protocol or DNS infrastructure. The reservation and usage for such TLDs would require special handling and is not discussed in this document; there have been efforts in the IETF to address them.[12,13]

2 Private-Use TLDs and Their Uses

The DNS namespace has no explicit provision for internally-scoped names, and current advice is for vendors or service providers to use a sub-domain of a public domain name (i.e., a fully qualified domain name, or FQDN) for internal, or private, use.[14] For example, an organization using example.org may choose to name resources that they intend only for internal use webserver.intranet.example.org or file-server.example.org. They may also employ split DNS to prevent these private names from being resolved outside of their organization. The SSAC previously discussed split DNS in SAC009.[15]

The SSAC encourages organizations to continue with this behavior and believes that using sub-domains of registered public domain names is still the best way to name internal resources and avoid future problems. However, it is not always feasible for organizations to use sub-domains of public domain names for private resources. This section discusses why some

[12] See draft-ietf-dnsop-alt-tld, The ALT Special Use Top Level Domain, https://datatracker.ietf.org/doc/draft-ietf-dnsop-alt-tld/
[13] See RFC 7686, The ".onion" Special-Use Domain Name, https://datatracker.ietf.org/doc/rfc7686/
[14] See Guide to Name Collision Identification and Mitigation for IT Professionals, Section 4, https://www.icann.org/en/system/files/files/name-collision-mitigation-05dec13-en.pdf
[15] See SAC009: Alternative TLD Name Systems and Roots: Conflict, Control and Consequences

organizations choose ad hoc usage of TLDs instead, and why that choice is likely justified, given their needs.

2.1 Use-Cases for Private-Use TLDs

Many enterprises use locally-defined domain names to support their applications and infrastructure in the form of a name drawn from a hierarchy rooted in a TLD that is not present in the root zone. Such a private-use TLD looks just like the familiar domain names used in email addresses and web URLs in the public Internet. However, it is only useful within a local network environment such as a user's home or a company's enterprise environment, or as part of accessing the local Intranet in a hotel or in a coffee shop. Two examples of private-use TLDs that are well known within the ICANN community are .corp and .home.[16]

Some of the motivations why enterprises and other network operators have stated they use private-use TLDs, as opposed to sub-domains of a publicly registered domain are:

- to avoid any form of external participation in the resolution of the name, which may change the behavior of the name in unexpected ways, including exfiltration of metadata that they intended to remain local.

- to ensure the name resolves, should Internet access be unavailable.

- to develop and test products and services on disconnected networks, where any interaction with the public Internet may be intentionally prohibited or otherwise problematic.

- to avoid undesirable behavior due to search list processing. If a "." exists in a name, resolvers should treat it as a fully qualified domain name and attempt to look up the name in the public DNS first.[17,18,19] For example, a user entering www.corp and relying on search list processing to have it expanded to www.corp.example.com will first have the name looked up in the public DNS. The SSAC understands that some organizations may not want these names to first be sent to the public DNS for many operational reasons, including the undesirable disclosure of the existence of a private system.

In addition to network operators, vendors of home routers, IoT devices, captive portal networks, and other software also have a significant use case for private-use TLDs. These vendors often use a namespace that will resolve without working Internet access, or without *a priori* knowledge of the network environment in which those devices are deployed.

---

[16] See Name Collision in the DNS, https://www.icann.org/en/system/files/files/name-collision-02aug13-en.pdf and Mitigating the Risk of DNS Namespace Collisions, https://www.icann.org/en/system/files/files/name-collision-mitigation-study-06jun14-en.pdf

[17] See RFC 1535, A Security Problem and Proposed Correction With Widely Deployed DNS Software, https://datatracker.ietf.org/doc/rfc1535/

[18] See RFC 1536, Common DNS Implementation Errors and Suggested Fixes, https://datatracker.ietf.org/doc/rfc1536/

[19] See resolv.conf(5) - Linux man page, https://linux.die.net/man/5/resolv.conf

In this use case, vendors do not pre-configure a delegated public domain name into the equipment they sell. Many of these devices use statically configured domain names for access or configuration. Vendors of these devices may be short lived, or simply not want to embed a public domain name linked to a brand into their devices. If there is a public domain name and the company changes, is acquired, or goes out of business, there is a significant risk that the domain name will get a new registrant thereby causing private information to leak to this new registrant.

Given the strong consumer preference for “plug and play” equipment that does not require configuration by the user or is pre-configured to the user's specification “out of the box”, they often choose a private-use TLD instead.

More importantly, vendors cannot determine ahead of time whether their products will be deployed in a private environment or on the public Internet, yet they desire consistent behaviour of their products for proper operation and support purposes. A private-use TLD enables this functionality, providing for more consistent behaviour in a multitude of environments. See *Appendix B* for an example device using a private namespace.

2.2 Current Usage of Private-Use TLDs

Currently, the usage of private-use TLDs is ad hoc. Many vendors, service providers, and enterprises use a string not found in the root zone as a private-use TLD in the context of their application or service. A number of common uses for such TLDs have been observed as queries to the root servers, as can be seen in *Figure 1*; a historical analysis of the traffic volume to some of these TLDs is listed in *Appendix A*.

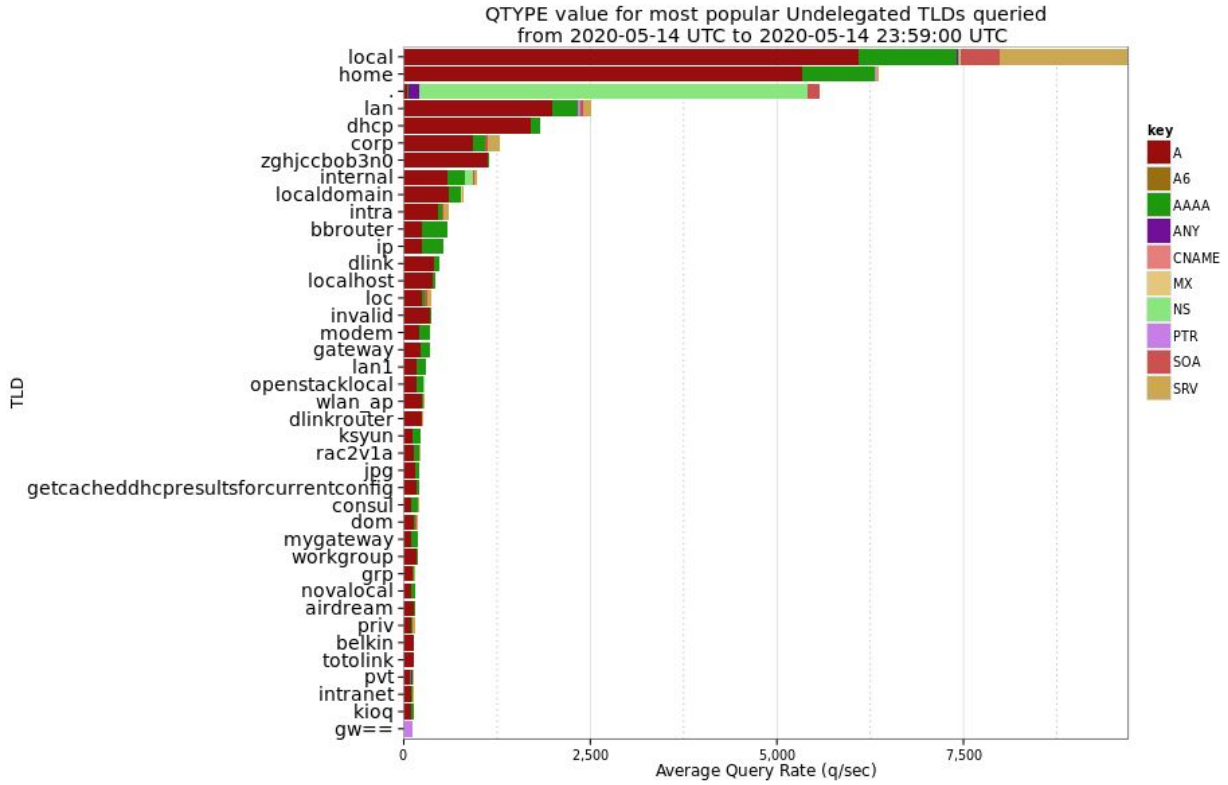


Figure 1: Private-use TLD usage observed as queries to l.root-servers.net on 14 May 2020.[20]

Table 2 below lists some of the most popular private-use TLDs and their query volume to two root server identifiers (a.root-servers.net and j.root-servers.net) on 14 May 2020. This is not a problem for the root server system, but illustrates, very indirectly, the prevalence of this type of configuration.

Private-use TLD	**Presumed Source**	**Queries to [a,j].root-servers.net on 14 May 2020**
.home	Used by some customer premise equipment (CPE)[21]	854 million (~9884/second)
.internal	Used by corporate networks	210 million (~2431/second)
.lan	Used by OpenWrt, a Linux operating system for embedded devices (see *Appendix C*)	165 million (~1909/second)

[20] See ICANN Hedgehog DNS-Stats, http://stats.dns.icann.org/plotcache/L-Root/qtype_vs_othertld/2020-05-14T00:00-2020-05-14T23:59-all.png?nocache=2020-05-15T13:20

[21] See Name Collision in the DNS, https://www.icann.org/en/system/files/files/name-collision-02aug13-en.pdf

.corp	Used by corporate networks[22]	151 million (~1748/second)
.localdomain	Default private-use TLD of several Linux distributions (see *Appendix C*)	82 million (~949/second)
.dlink	Used by dlink routers	52 million (~602/second)
.zyxel-usg	Matches the name of a network security appliance vendor	28 million (~324/second)

Table 2: Popular private-use TLDs seen at Verisign's Root Servers

2.3 Issues with Private-Use TLDs

There are significant problems with the current ad hoc usage of private-use TLDs. Although these strings are intended only to be used internally (or in scoped network domains that do not interfere with the public Internet), there is ample evidence that they leak into the global public DNS infrastructure, causing the following issues:

- Name collisions leading to unexpected and unpredictable behaviour if the TLD is delegated by ICANN (and during the trial delegation period) (see SAC045, SAC062, SAC066).

- Potential insecurity and compromise to confidentiality through on-path-attacks when externally resolving names, as well as after controlled interruption if they remain in use.

- Name ambiguity, where it is unclear to either a client or service in what context a published name is applicable.

- Security risks stemming from certificates issued by globally trusted Certification Authorities (CAs) for domain names within these TLDs (see also SAC057).

- Difficulty in debugging, as a clean, bounded resolution context is hard to achieve.

- Unnecessary DNS load, such as that experienced by root name servers receiving queries for non-delegated TLDs. (While the vast bulk of traffic to the root servers is unnecessary and the root servers are provisioned to support much larger loads than they receive unless attacked, there is, nonetheless, some desire to reduce unnecessary load.)

3 Private IP Address Space, a Useful Precedent

The IP addressing environment has encountered similar situations on past occasions when enterprises wanted to use IP addresses not routable in the public Internet. The response was to designate a part of the address space as shared private use address space (see RFC1918,

[22] *id.*

RFC4193).[23,24] Such addresses can be used within private networks with no requirement for coordination.

These addresses, such as the 192.168.x.x and 172.16.x.x spaces, support the needs of private (i.e., internal) networks with the explicit understanding that their use is not supported on the public Internet. For example, many home router devices ship with a default LAN IP address of 192.168.0.1 or 192.168.1.1, and users expect that to work out of the box. A similar designation has been made for private autonomous system (AS) numbers.[25]

What the IP address 192.168.0.23 refers to in one network will differ from what 192.168.0.23 refers to in another network. This is an intentional design feature of these IP address reservations. In the same way, one instance of www.internal would be different to another instance of www.internal.

Because the private use address space supports the needs of private networks with the explicit understanding that the use of those addresses is not supported on the public Internet, if two or more of these networks merge, address conflicts and resolution ambiguities may occur. The scope of this conflict is, however, limited to the intersecting private realms, and does not have broader impacts on other private realms, nor on the public Internet. Similarly, significant planning on how to use private names would be necessary if networks using the same internal names were to merge.

Even with this planning significant costs are typically incurred both in migration and in ongoing operations from trying to merge networks that use overlapping, non-unique IP addresses. Operators who choose to use private namespaces of the kind proposed in this document should understand the potential for that decision to have corresponding costs, and that those costs might well be avoided by choosing instead to use a sub-domain of their own publicly registered domain name.

While there are important similarities in how a private IP address and a private-use TLD can be used, there are also important differences to note. An IP address is not intended to be used as a human-oriented identifier, while domain names often are. Thus, when choosing a DNS label the interfacing between humans and computers must be taken into account. Second, the deciding factor in creating RFC 1918 and reserving IP address space for private use was the impending exhaustion of IPv4 addresses. No such pending exhaustion looms for TLDs. Third, for those who could not procure IPv4 addresses in the 1990s, there was no other option but squatting on a finite and rapidly depleting resource, with no analogous address collision mitigation strategy possible. Fourth, there was a clear consensus on the need for, and a plan for, architectural changes to solve the problem in the long term. There is no such consensus here.

These differences are noted here for completeness and because this limited analogy of IP addresses to DNS labels can still be useful for educational purposes.

[23] See RFC 1918, Address Allocation for Private Internets, https://datatracker.ietf.org/doc/rfc1918/
[24] See RFC 4193, Unique Local IPv6 Unicast Addresses, https://datatracker.ietf.org/doc/rfc4193/
[25] See RFC 6996, Autonomous System (AS) Reservation for Private Use, https://datatracker.ietf.org/doc/rfc6996/

4 SSAC Proposal

Because of the decentralized nature of the DNS, there is no way to prevent ad hoc usage of a TLD rather than use of an explicitly reserved private-use TLD as this advisory recommends. The best approach is to create a designated place in the namespace to accomplish this. Vendors and others who instantiate names for ad hoc purposes have no guidance other than using a sub-domain of a public domain name. Without a name reserved for this purpose, they do not have the choice of a safe name to use. They cannot know with any certainty that the name they choose today will not be delegated into the root zone later. Providing a permanent reservation for this purpose can help alleviate the uncoordinated ad hoc usage of TLDs for private use.

In addition, reserving a name for this purpose now may limit future incidents of name collisions at the top level and simplify policy for future new gTLD rounds.

This advisory recommends a course of action that is comparable to the local use reservations in IPv4, IPv6 and the AS number space: namely ICANN reserves a string specifically for use as a private-use TLD for namespaces that are not part of the global DNS, but are meant to be resolved using the DNS protocol.

Such a reservation should provide a clear path for developers, vendors, service providers, and users to define internally-scoped namespaces for themselves without the requirement for prior coordination, and to do so with the clear understanding that all names in this namespace will **never** be resolvable in the public Internet, and will not collide with existing or future delegated TLDs in the global DNS.

In this section, the SSAC explains the proposal in detail.

4.1 Criteria to Choose the String for Reservation

The SSAC proposes the following criteria for the selection of the string:

1. It is a valid DNS label.[26]
2. It is not already delegated in the root zone.
3. It is not confusingly similar to another TLD in existence.
4. It is relatively short, memorable, and meaningful.

Although ICANN can reserve a string, it cannot force people to use it. To increase its appeal, the label selected should be simple and intuitive for its anticipated users. A label that is too long, or easy to forget, is less likely to be used, and will therefore be less successful.

It is not possible to choose a name that will accommodate the preferences of all DNS users. Therefore, further strings could be considered to fit such criteria if and when such a need arises.

[26] See RFC 5890, Section 2.3, Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework, https://datatracker.ietf.org/doc/rfc5890/

For example, consideration could be given to internationalized versions of the string, reserving strings that are meaningful in different scripts.

Additional consideration may be given to names already in use for this purpose. If a given string is already in common use for this purpose, explicitly reserving it for this purpose would be less burdensome than asking users to switch to using a new string.

4.2 There is no Single Solution

The reservation of a string for private use does not preclude other potential solutions for the use cases outlined in *Section 2.1*. The SSAC continues to believe that in most cases the best option for network designers and vendors is to use a sub-domain of their own publicly registered domain name.

When this is not practical, the SSAC believes that people should make the best decision for their specific requirements. One possible option could be to use a sub-domain of a reserved string, as described in this document. Another option is to use an insecure delegation at the second-level of the hierarchy (e.g., home.arpa).[27] It is likely that other options exist as well, and more will be conceived in the future.

The choice should be made consciously, taking into account all available options, and considering the specific requirements. It is not the role of the SSAC to prescribe specific solutions for specific network use cases. Instead, the SSAC believes that, ideally, designers should have options, and sufficient information to weigh the pros and cons of each, prior to making a decision on which to implement.

5 Recommendation

Recommendation 1: The SSAC recommends that the ICANN Board ensure a string is identified using the criteria specified in Section 4.1 and reserved at the top level for private use. This particular string must never be delegated.

6 Acknowledgments, Statements of Interests, Dissents, Alternative Views and Withdrawals

In the interest of transparency, these sections provide the reader with information about aspects of the SSAC process. The Acknowledgments section lists the SSAC members, outside experts, and ICANN staff who contributed directly to this particular document. The Statements of Interest section points to the biographies of all SSAC members, which disclose any interests that might represent a conflict—real, apparent, or potential—with a member's participation in the preparation of this Report. The Dissents and Alternative Views section provides a place for individual members to describe any disagreement with, or alternative view of, the content of this

[27] See RFC 8375, Special-Use Domain 'home.arpa.', https://datatracker.ietf.org/doc/rfc8375/

document or the process for preparing it. The Withdrawals section identifies individual members who have recused themselves from discussion of the topic with which this report is concerned. Except for members listed in either the Dissents and Alternative Views or Withdrawals sections, this document has the consensus approval of all of the members of SSAC.

6.1 Acknowledgments

The committee wishes to thank the following SSAC members for their time, contributions, and review in producing this report.

SSAC members
Greg Aaron
Joe Abley
Jaap Akkerhuis
Tim April
Lyman Chapin
kc claffy
Patrik Fältström
James Galvin
Cristian Hesselman
Geoff Huston
Merike Kaeo
Warren Kumari
Barry Leiba
John Levine
Danny McPherson
Russ Mundy
Rod Rasmussen
Mark Seiden
Suzanne Woolf

ICANN staff
Danielle Rutherford
Andrew McConachie (editor)
Kathy Schnitt
Steve Sheng

6.2 Statements of Interest

SSAC member biographical information and Statements of Interest are available at:
https://www.icann.org/resources/pages/ssac-biographies-2020-07-02-en

6.3 Dissents and Alternative Views

kc claffy provided the following alternative view.

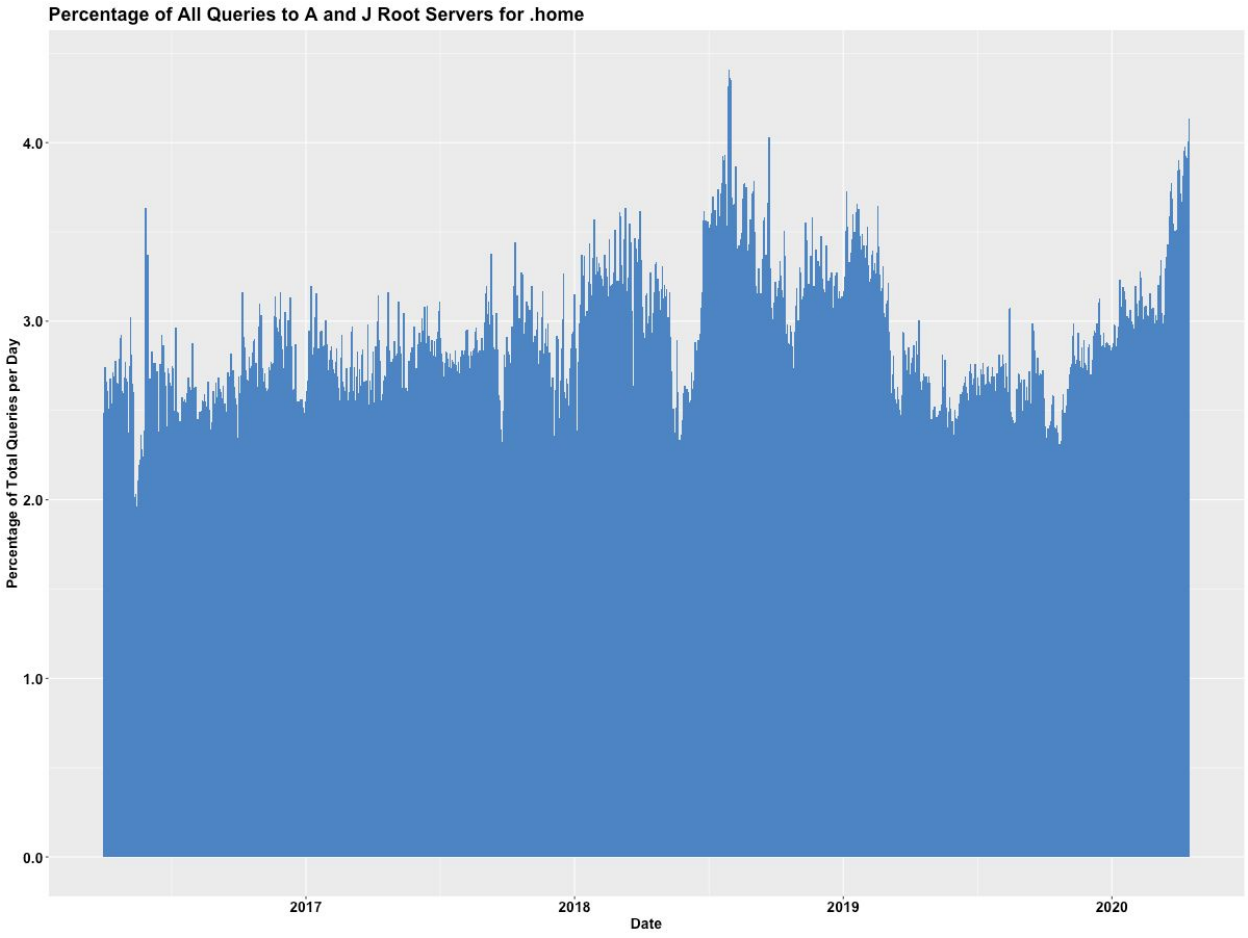
This advisory notes a lack of consensus on the long-term solution to the problem of proliferating use of ad hoc TLDs. Instead, SSAC proposes a short-term measure: reserve one string, to "alleviate many of the problems stemming from ad hoc TLD use, primarily by grouping this ad hoc usage under one, well-known string."

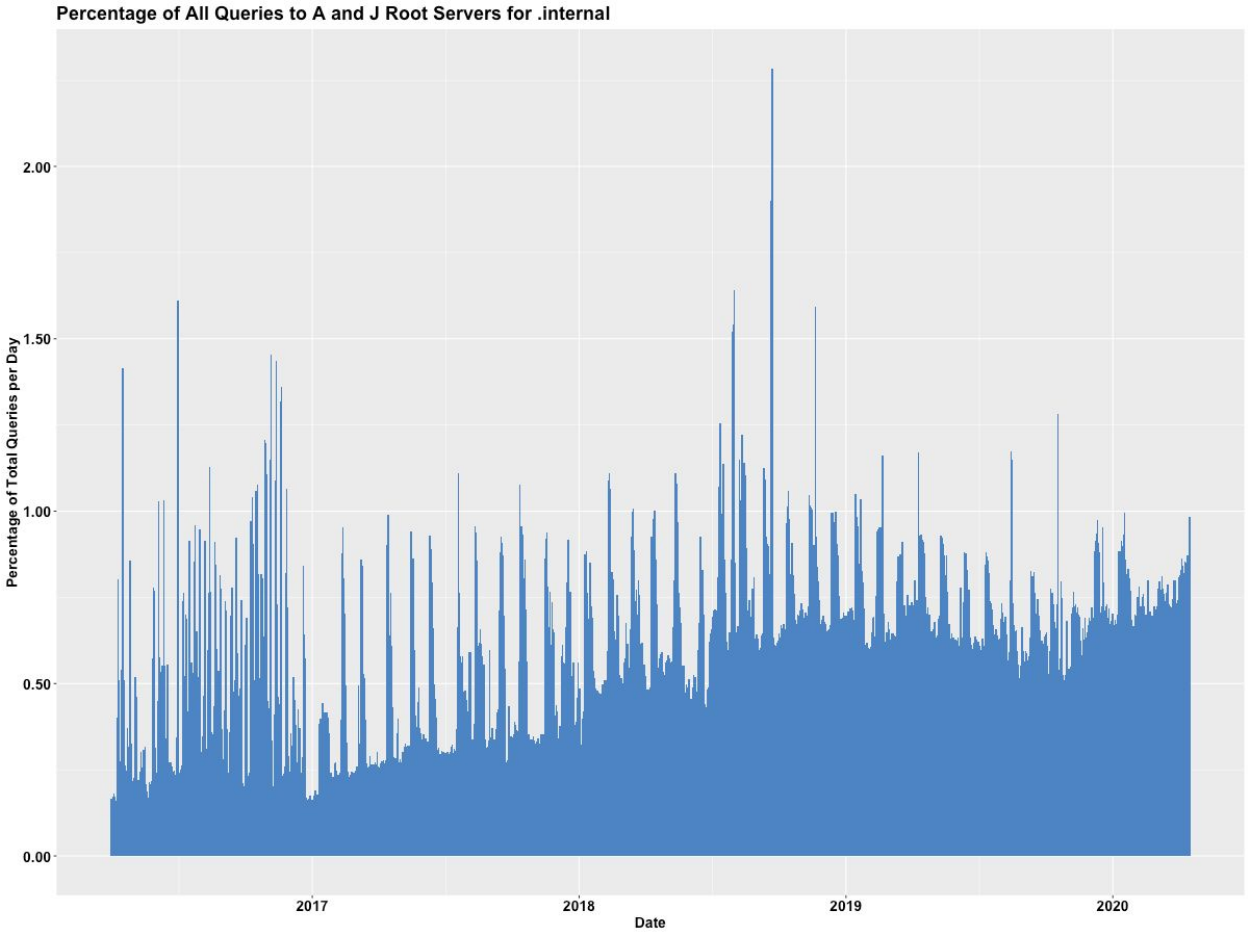
I agree that ICANN and the IETF should accommodate private-use TLDs. But I believe they need a more coherent, coordinated, and long-term strategy, as SAC090 and SAC062 advised 4 and 7 years ago. Most importanty, if ICANN is going to create new "unlicensed" namespace, there should be a commitment to related standards work aimed at avoiding harmful consequences of pervasive use of such namespace. But this standards work is generally IETF territory. There seems to be an impasse there. Hopefully this advisory is a step toward overcoming it.

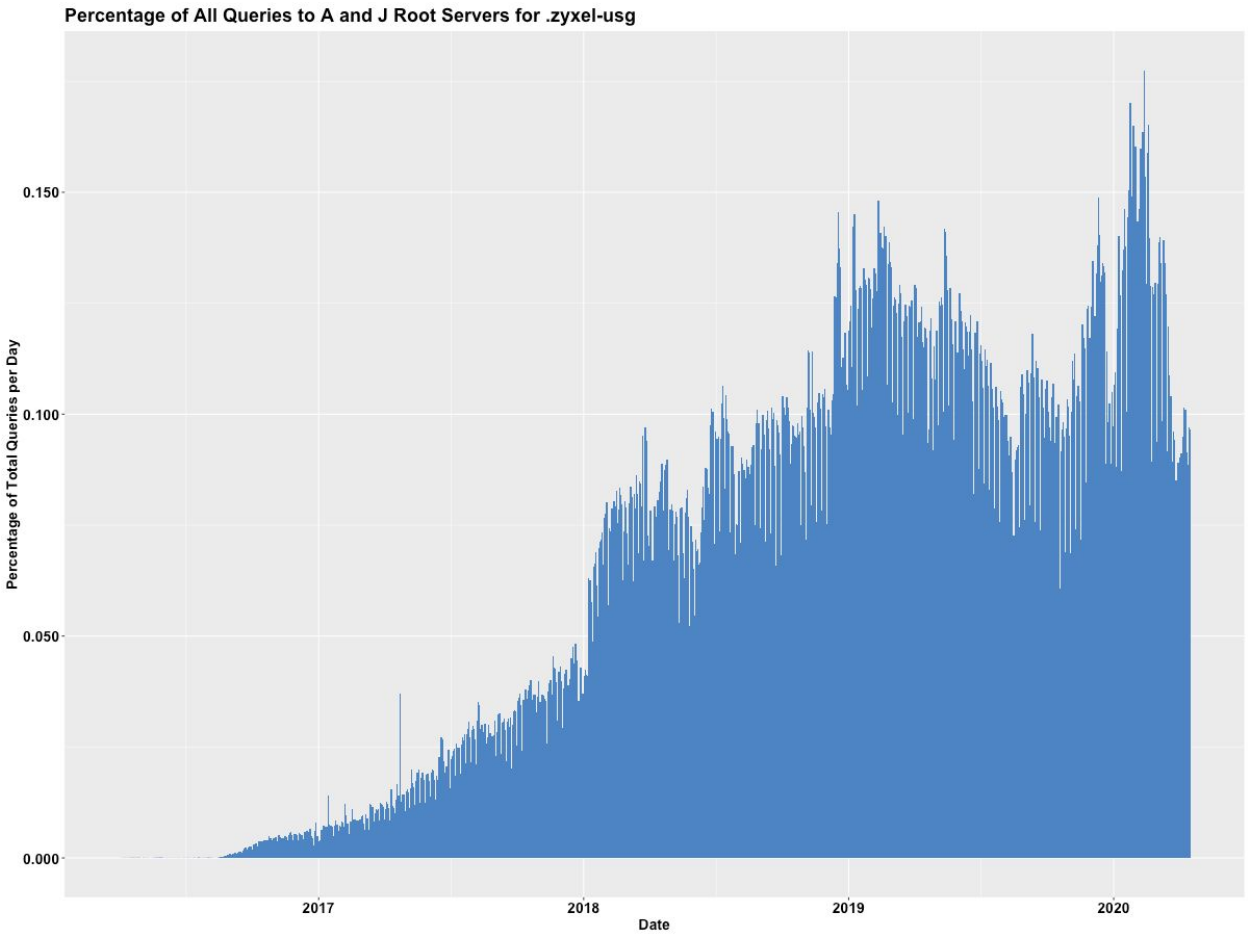
6.4 Withdrawals

There were no withdrawals.

Appendix A: Additional Statistics on Private-Use TLDs




Percentage of All Queries to A and J Root Servers for .internal
Percentage of Total Queries per Day
2.00
1.50
1.00
0.50
0.00
2017
2018
2019
2020
Date


Percentage of All Queries to A and J Root Servers for .zyxel-usg
Percentage of Total Queries per Day
0.150
0.100
0.050
0.000
2017
2018
2019
2020
Date

Appendix B: Example Device Using a Private Namespace

What follows is the partially redacted terminal output from a real home Internet user's laptop captured in 2020. The user installed a device in their home provided by their residential cable Internet service provider (ISP). This device is designed to act as a combination Data Over Cable Service Interface Specification (DOCSIS) modem, Network Address Translator (NAT), and forwarding/caching DNS stub resolver. The user's laptop is connected directly to this device and enabled for auto-configuration via Dynamic Host Configuration Protocol (DHCP).

```
user@laptop# cat /etc/resolv.conf
..
domain home
nameserver 192.168.178.1
nameserver 2001:****:3e42::53
nameserver 2001:****:3e42:1000::53

user@laptop# dig 1.178.168.192.in-addr.arpa PTR
..
1.178.168.192.in-addr.arpa. 0 IN PTR compalhub.home.

user@laptop# dig compalhub.home A
..
compalhub.home. 0 IN A 192.168.178.1

user@laptop# dig compalhub.home AAAA
..
compalhub.home. 0 IN AAAA 2a02:****:9284:4680:ae22:5ff:fe8e:12ec
compalhub.home. 0 IN AAAA fe80::ae22:5ff:fe8e:12ec
compalhub.home. 0 IN AAAA fe80::ae22:5ff:fe8e:12ec

user@laptop# dig anything.home A
..
;; >>HEADER<< opcode: QUERY, status: NXDOMAIN, id: 8245
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1,
ADDITIONAL: 0
..
```

This example shows a device that is statically configured, either by the vendor or the ISP, with a hardcoded domain name of “compalhub.home”. End-user installation documentation shipped with the device directed the user to open their web browser and visit “compalhub.home” to begin setting up their Internet service. Because the device is also acting as a forwarding DNS stub resolver[28] it can intercept queries to “compalhub.home” and respond to them directly without

[28] DNS forwarding stub resolvers are common in residential home networking devices that also perform network address translation (NAT). A DNS forwarding stub resolver receives DNS queries from internal stub resolvers and

contacting the ISP's recursive resolver. Queries for other names, including other names under the private-use TLD ".home", will be forwarded to the ISP's recursive resolver.

If IANA were to delegate ".home" into the DNS root zone and a registrant registered "compalhub.home" this user would not be able to resolve that name from within their residence. Once the same name "compalhub.home" exists on both the user's private residential network and the public Internet any attempt by the user to reach the public resource would be prevented by this device.

passes them on to external recursive resolvers. It will typically cache the responses received from the recursive resolver and may also perform DNSSEC validation on those responses.

Appendix C: Default Private-Use TLDs in Linux Distributions

Popular Linux distributions were surveyed to determine what, if any, default private-use TLDs each used during installation. They are listed below grouped by their default installation behavior.

No default private-use TLD

Distributions in this grouping did not use or suggest any default private-use TLD. All either required a hostname (i.e., single label without dot), or provided a default. However, if the user did not specify a domain for this hostname the distribution would install without it. For every entry in this section hostname -f returned the empty string, /etc/hosts contained no configured domain name, and/or systemd-resolved was not configured with a domain name.

Gentoo 2020-04-19
Ubuntu Desktop 20.04 LTS
Ubuntu Server 20.04 LTS

- Install does not have default hostname, but requires the user to provide one

Debian 10.4.0

- Default hostname is 'debian'

OpenSuse-Tumbleweed-2020-05-09

- Default hostname is 'localhost'

Default private-use TLD

Distributions in this grouping provided a default private-use TLD as part of their installation. Some also provided a default hostname part, while others required the user to provide one.

Arch Linux 2020-05-01

- No default hostname
- Default private-use TLD of '.localdomain'[29]

Fedora 32 Server
Fedora 32 Workstation
CentOS 8

- Default hostname 'localhost'
- Default private-use TLD of '.localdomain'

[29] See Arch Linux Installation Guide, https://wiki.archlinux.org/index.php/Installation_guide#Network_configuration

OpenWRT 19.07

- No default hostname
- Default private-use TLD of '.lan'[30]
- Default blocking of names in the IANA Special-Use Domain Names Registry[31]

[30] See OpenWRT DNS and DHCP configuration /etc/config/dhcp, https://openwrt.org/docs/guide-user/base-system/dhcp

[31] See OpenWRT git repo, dnsmasq, rfc6761.conf, https://git.openwrt.org/?p=openwrt/openwrt.git;a=blob;f=package/network/services/dnsmasq/files/rfc6761.conf;h=ebc1a12118682d62748735c5e177e1efaaeaae33;hb=9356a6bfc7b4f930e0c07e95aceb987967e095d5

Appendix D: Related Work

Our current work is informed by four streams of work on this topic: architectural guidance, existing process at ICANN and IETF to handle special use names or to reserve TLDs, past and current proposals to reserve names, and analysis of risks stemming from the current ad hoc usage of TLDs for private use.

Architectural Guidance

RFC2826[32] is the Internet Architecture Board's Technical Comment on the Unique DNS Root. This architectural guidance, written twenty years ago, lays out the distinct reasons why the DNS requires a single root for hierarchical names in order to operate properly, and speaks directly to several key issues related to special use domain names.

RFC8244[33] applied the architectural guidance in RFC2826 to the special use context. The most relevant finding for this publication is, "Domain names with unambiguous global meaning are preferable to domain names with local meaning that will be ambiguous. Nevertheless, both globally meaningful and locally special names are in use and must be supported."

The scope of consideration for special use domain names in the IETF includes the fact that domain names are not used only by the DNS. They were used in other protocols before the DNS,[34] and various protocol development efforts such as IETF working groups and open source projects have also used domain names and naming conventions. The IETF has thus not assumed that domain names are to appear in the public DNS or be resolved by the DNS protocol. Discussion of domain names in the IETF has also not focused entirely on root-level names or TLDs. For example, the IETF HOMENET Working Group asked for ".home" as a special use name for a protocol they developed, but the name that was ultimately reserved was "home.arpa".[35]

The potential for collision, and the need to avoid or resolve it, occurs only if the same name is reserved or used for both a delegation in the public root zone for resolution in the DNS, and some other scope or protocol purpose, such as private use, or a novel protocol such as the Tor protocol or the GNU Name System.[36] The Memorandum of Understanding (MoU) between ICANN and the IETF allows the IETF to reserve names for "technical use," without specifying further guidelines or process of any kind to determine what that actually means, which further suggests coordination of processes or procedures would be a good idea.[37]

---

[32] See RFC 2826, IAB Technical Comment on the Unique DNS Root, https://datatracker.ietf.org/doc/rfc2826/
[33] See RFC 8244, Special-Use Domain Names Problem Statement, https://datatracker.ietf.org/doc/rfc8244/
[34] See draft-lewis-domain-names-13, RFC Origins of Domain Names, https://datatracker.ietf.org/doc/draft-lewis-domain-names
[35] See RFC 8375, Special-Use Domain 'home.arpa.', https://datatracker.ietf.org/doc/rfc8375/
[36] See draft-schanzen-gns-01, The GNU Name System, https://datatracker.ietf.org/doc/draft-schanzen-gns/
[37] See IETF-ICANN Memorandum of Understanding Concerning the Technical Work of the Internet Assigned Numbers Authority, Section 4.3, https://www.icann.org/resources/unthemed-pages/ietf-icann-mou-2000-03-01-en

Similar guidance for private use has also been discussed in SAC062, where the SSAC recommended ICANN to identify (1) what strings are appropriate to reserve for private namespace use and (2) what type of private namespace use is appropriate.[38]

This document is guided by RFC2826 and SSAC062, and built on the premise that locally special names are in use and must be supported.

In SAC090: SSAC Advisory on the Stability of the Domain Namespace, the SSAC articulates the risks to security and stability that arise from ambiguity in the use of the domain namespace. It made a set of recommendations to mitigate these risks and called for ICANN to establish effective means of collaboration on these issues with relevant groups outside of ICANN, including the IETF. On 23 June 2018, the ICANN Board accepted all SAC090 recommendations and asked the GNSO new gTLD Subsequent Procedures Policy Development Work Party to include the recommendations in its work.[39]

SAC090 provides a framework to consider special use names:

> Because no one owns (or can own) the domain namespace, and programmers and network managers cannot be prevented from creating their own names and naming scopes, these risks arise regardless of how policy debates about authority or oversight are resolved. Therefore, the observations and recommendations in this advisory [SAC090] are directed at mitigating clearly identified risks and developing policies that provide practical guidance to software and system developers, rather than debating whether or not private network operators should use the domain namespace, or who (if anyone) should have the authority to declare and enforce exclusive uses for specific individual domain name labels or categories of labels.[40]

Our current work adopts this pragmatic approach: given the widespread usage, it is not productive to debate whether or not private network operators should use the domain namespace, or who should have the authority to declare and enforce exclusive uses for specific individual domain name labels or categories of labels. Instead, the focus is to mitigate clearly identified risks.

Existing Processes at IETF and ICANN

Within the IETF, there is a procedure to note a name as being reserved for special use. RFC 6761: Special-Use Domain Names, describes what it means to say that a DNS name is reserved for special use, when reserving such a name is appropriate, and the procedure for doing so.[41] It establishes an IANA registry for such domain names and seeds it with entries for some of the already established special use domain names. The following TLDs were listed in RFC 6761 as the initial entries for the IANA registry: .test, .example, .localhost, .invalid.

[38] See SAC062: SSAC Advisory Concerning the Mitigation of Name Collision Risk
[39] See Approved Board Resolutions 23 June 2018, https://www.icann.org/resources/board-material/resolutions-2018-06-23-en#1.g
[40] See SAC090: SSAC Advisory on the Stability of the Domain Namespace
[41] See RFC 6761, Special-Use Domain Names, https://datatracker.ietf.org/doc/rfc6761

The IETF, through the standards process, also reserved .onion for the Tor protocol, specified as part of the Tor Project.[42] The rationales are documented in RFC 7686.[43] During the consideration of .onion as a special use TLD, and discussion of other proposed special use domain names in several other internet-drafts around the same time, it became clear that the issues surfaced presented challenges that were not anticipated when RFC 6761 was written.

The IETF suspended consideration of additional special use domain names after RFC 7686 was approved, and initiated an effort to better define the problem space and produce updated guidelines for special use names. The first publication of such an effort is RFC 8244: Special-Use Domain Names Problem Statement. A draft to define guidelines for the IESG and the IETF community on the interpretation of RFC 6761 and the use of the special use names registry has also been developed.[44]

A proposal similar to the one in this document was submitted as an Internet Draft[45] in July 2017 for the IETF's consideration. The IETF DNSOP WG considered it at IETF100 and declined to adopt it as a working group document. The majority of the participants at the time thought that a proposal to set aside names from being delegated in the root zone should be submitted for ICANN's consideration.

Within ICANN, the policy recommendations regarding reserved names are being developed in the Generic Name Supporting Organization (GNSO)'s Policy Development Processes. Such policy recommendations in 2012 as well as subsequent implementation efforts resulted in the creation of the Applicant Guidebook.[46] In the guidebook ICANN cited or created several lists of strings that could not be applied for as new gTLD names, such as the "reserved names" listed in Section 2.2.1.2.1, the "ineligible strings" listed in Section 2.2.1.2.3, the two-character ISO 3166 codes forbidden in Section 2.2.1.3.2 Part III, and the geographic names described in Section 2.2.1.4.

[42] See The Tor Project, https://www.torproject.org/
[43] See RFC 7686, The ".onion" Special-Use Domain Name, https://datatracker.ietf.org/doc/rfc7686/
[44] See draft-stw-6761ext-01, Guidelines for Use of the Special Use Names Registry, https://datatracker.ietf.org/doc/draft-stw-6761ext/
[45] See draft-wkumari-dnsop-internal, The .internal TLD., https://datatracker.ietf.org/doc/draft-wkumari-dnsop-internal/
[46] See gTLD Applicant Guidebook, https://newgtlds.icann.org/en/applicants/agb/guidebook-full-04jun12-en.pdf

Past and Current Proposals For Private-Use TLDs

Several documents have proposed reservations of TLDs. These are organized in the table below by dates. This is not an exhaustive list and there may be others that the SSAC is unaware of.

Date	Authors	Description of Proposal	Status
Feb 2013	S. Cheshire and M. Krochmal	Reserve .local for multicast DNS use	Published as RFC6762[47]
Jan 2014	L. Chapin and M. McFadden	Reserve eight domain name labels for special use in accordance with the criteria and procedures of RFC6761: localdomain, domain, lan, home, host, corp, mail, and exchange.	Two revisions, Expired I-D[48]
Mar 2015	E. Lewis	Add the alpha-2 user-assigned codes XA to XZ to the Special Use Domain Names registry, designated as "Private Use"; add the alpha-2 user-assigned codes AA, QN to QZ, and ZZ as "Future Use".	Expired I-D[49]
Jun 2015	W. Kumari and A. Sullivan	Reserve a string (ALT) to be used as a TLD label in non-DNS contexts or for names that have no meaning in a global context.	Twelve revisions, expired I-D[50]
Jun 2015	J.Appelbaum and A. Muffett	Register the ".onion" Special-Use Domain Name.	Published as RFC7686[51]
Apr 2016	M. Stenberg S. Barth P. Pfister	Specify .home for home networking control use. A mistake[52] was made with RFC 7788 and .HOME that was resolved through RFC 8375, which reserved “home.arpa” instead.	RFC7788[53] RFC8375[54]
Jul	W. Kumari	Propose reserving the string ".internal" for internal	General

[47] See RFC 6762, Multicast DNS, https://datatracker.ietf.org/doc/rfc6762/
[48] See draft-chapin-additional-reserved-tlds-00, Additional Reserved Top Level Domains, https://datatracker.ietf.org/doc/draft-chapin-additional-reserved-tlds/
[49] See draft-lewis-user-assigned-tlds-00, User Assigned ISO 3166-1 Alpha-2 Codes and the DNS Root Zone, https://datatracker.ietf.org/doc/draft-lewis-user-assigned-tlds/
[50] See draft-ietf-dnsop-alt-tld-12, The ALT Special Use Top Level Domain, https://datatracker.ietf.org/doc/draft-ietf-dnsop-alt-tld/
[51] See RFC 7686, The ".onion" Special-Use Domain Name, https://datatracker.ietf.org/doc/rfc7686/
[52] See RFC Errata 4677, https://www.rfc-editor.org/errata/eid4677
[53] See RFC 7788, Home Networking Control Protocol, https://datatracker.ietf.org/doc/rfc7788/
[54] See RFC 8375, Special-Use Domain 'home.arpa.', https://datatracker.ietf.org/doc/rfc8375/

2017		use.[55]	feedback was that the work should be discussed at ICANN. This is the impetus for this advisory.[56]
May 2020	R. Arends and E. Lewis	Designate ISO 3166-1 alpha-2 user-assigned codes as reserved for private use purposes.	Current I-D,[57] intended status: BCP

Risk Analysis and Mitigations

Some of the risks associated with name collisions and namespace issues are described in SSAC Advisories SAC045,[58] SAC057,[59] SAC062,[60] SAC064,[61] SAC078,[62] and SAC090.[63] ICANN has established the Name Collision Analysis Project (NCAP) to understand the causes, magnitude, and mitigations for name collisions.

To mitigate the risks of collisions, ICANN has published a guide for IT professionals,[64] as well as instructing registries to implement a name collision occurrence management framework.[65] To mitigate the risks of namespace instability, SSAC in SAC090 called for more cooperation and collaboration amongst standards bodies.

[55] See draft-wkumari-dnsop-internal, The .internal TLD.,
https://datatracker.ietf.org/doc/draft-wkumari-dnsop-internal/
[56] See [DNSOP] A quick update on ICANN SSAC and .internal...,
https://mailarchive.ietf.org/arch/msg/dnsop/7AzjYP3XoLaPYKPjPzQzEn6k7L4/
[57] See draft-arends-private-use-tld-02, Top-level Domains for Private Internets,
https://datatracker.ietf.org/doc/draft-arends-private-use-tld/
[58] See SAC045: Invalid Top Level Domain Queries at the Root Level of the Domain Name System
[59] See SAC057: SSAC Advisory on Internal Name Certificates
[60] See SAC062: SSAC Advisory Concerning the Mitigation of Name Collision Risk
[61] See SAC064: SSAC Advisory on Search List Processing
[62] See SAC078: SSAC Advisory on Uses of the Shared Global Domain Name Space
[63] See SAC090: SSAC Advisory on the Stability of the Domain Namespace
[64] See Guide to Name Collision Identification and Mitigation for IT Professionals,
https://www.icann.org/en/system/files/files/name-collision-mitigation-01aug14-en.pdf
[65] See Name Collision Occurrence Management Framework,
https://www.icann.org/en/system/files/files/name-collision-framework-30jul14-en.pdf