DNS Scoped Data Through "Underscore" Naming of Attribute Leaves
draft-ietf-dnsop-attrleaf-15

Abstract

Formally, any DNS resource record may occur under any domain name. However some services use an operational convention for defining specific interpretations of an RRset, by locating the records in a DNS branch, under the parent domain to which the RRset actually applies. The top of this subordinate branch is defined by a naming convention that uses a reserved node name, which begins with an _underscore. The underscored naming construct defines a semantic scope for DNS record types that are associated with the parent domain, above the underscored branch. This specification explores the nature of this DNS usage and defines the "DNS Global Underscore Scoped Entry Registry" with IANA. The purpose of the Underscore registry is to avoid collisions resulting from the use of the same underscore-based name, for different services.

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 May 7, 2019.

Copyright Notice

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

The core Domain Name System (DNS) technical specifications assign no semantics to domain names or their parts, and no constraints upon which resource record (RR) types are permitted to be stored under particular names [RFC1035], [RFC2181]. Over time, some leaf node names, such as "www" and "ftp" have come to imply support for particular services, but this is a matter of operational convention, rather than defined protocol semantics. This freedom in the basic technology has permitted a wide range of administrative and semantic policies to be used -- in parallel. DNS data semantics have been limited to the specification of particular resource record types, on the expectation that new resource record types would be added as needed. Unfortunately, the addition of new resource record types has
proven extremely challenging, over the life of the DNS, with significant adoption and use barriers.

1.1. Underscore Scoping

As an alternative to defining a new RR type, some DNS service enhancements call for using an existing resource record type, but specify a restricted scope for its occurrence. Scope is meant as a static property, not one dependent on the nature of the query. It is an artifact of the DNS name. That scope is a leaf node, within which the uses of specific resource record sets can be formally defined and constrained. The leaf occurs in a branch having a distinguished naming convention: At the top of the branch -- beneath the parent domain name to which the scope applies -- one or more reserved DNS node names begin with an underscore ("_`). Because the DNS rules for a "host" (host name) do not allow use of the underscore character, this distinguishes the underscored name from all legal host names [RFC952]. Effectively, this convention for leaf node naming creates a space for the listing of "attributes" -- in the form of resource record types -- that are associated with the parent domain, above the underscored sub-branch.

The scoping feature is particularly useful when generalized resource record types are used -- notably "TXT", "SRV", and "URI" [RFC1035], [RFC2782], [RFC6335], [RFC7553]. It provides efficient separation of one use of them from others. Absent this separation, an undifferentiated mass of these "RRsets" is returned to the DNS client, which then must parse through the internals of the records in the hope of finding ones that are relevant. Worse, in some cases the results are ambiguous because a record type might not adequately self-identify its specific purpose. With underscore-based scoping, only the relevant "RRsets"s are returned.

A simple example is DKIM [RFC6376], which uses "_domainkey" for defining a place to hold a "TXT" record containing signing information for the parent domain.

This specification formally defines how underscored labels are used as "attribute" enhancements for their parent domain names. For example, domain name "_domainkey.example." acts as an attribute of the parent domain name "example." To avoid collisions resulting from the use of the same underscore-based labels for different applications using the same resource record type, this document establishes the DNS Underscore Global Scoped Entry IANA Registry. Use of such node names, which begin with underscore, are reserved when they are the underscored name closest to the DNS root; they are considered "global". Underscore-based names that are farther down
the hierarchy are handled within the scope of the global underscore name.

Discussion Venue: Discussion about this draft should be directed to the dnsop@ietf.org [1] mailing list.

NOTE TO RFC EDITOR: Please remove "Discussion Venue" paragraph prior to publication.

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 BCP14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

1.2. Scaling Benefits

Some resource record types are used in a fashion that can create scaling problems, if an entire RRset associated with a domain name is aggregated in the leaf node for that name. An increasingly-popular approach, with excellent scaling properties, places the RRset under a specially named branch, which is in turn under the node name that would otherwise contain the RRset. The rules for naming that branch define the context for interpreting the RRset. That is, rather than:

\[
\text{domain-name.example} \\
/ \\
\text{RRset}
\]

the arrangement is:

\[
\text{_branch.domain-name.example} \\
/ \\
\text{RRset}
\]

A direct lookup to the subordinate leaf node produces only the desired record types, at no greater cost than a typical DNS lookup.

1.3. "Global" Underscored Node Names

As defined in [RFC1034] the DNS uses names organized in a tree-structured, or hierarchical fashion. A domain name might have multiple node names that begin with an underscore. A "global" underscored node name is the one that is closest to the root of the DNS hierarchy, also called the highest-level or top-most. In the presentation convention described in Section 3.1 of [RFC1034] this is the right-most name beginning with an underscore. In other presentation environments it might be positioned differently. To
avoid concern for the presentation variations, the qualifier "global" is used here.

1.4. Interaction with DNS wildcards

DNS wildcards interact poorly with underscored names in two ways. Since wildcards only are interpreted as leaf names, one cannot create the equivalent of a wildcard name for prefixed names. A name such as label.*.example.com is not a wildcard.

Conversely, a wildcard such as *.example.com can match any name including an underscored name. So, a wildcard might match an underscored name, returning a record that is the type controlled by the underscored name but is not intended to be used in the underscored context and does not conform to its rules.

1.5. History

Originally different uses of underscore-based node names developed largely without coordination. For "TXT" records, there is no consistent, internal syntax that permits distinguishing among the different uses. In the case of the "SRV" "RR" and "URI" "RR", distinguishing among different types of use was part of the design [RFC2782], [RFC7553]. The "SRV" and "URI" specifications serve as templates, defining "RR"s that might only be used for specific applications when there is an additional specification. The template definition included reference to two levels of tables of names from which underscore-names should be drawn. The lower-level (local scope) set of "_service" names is defined in terms of other IANA tables, namely any table with symbolic names. The upper-level (global scope) "SRV" naming field is "_proto", although its pool of names is not explicitly defined.

The aggregate effect of these independent efforts was a long list of underscore-based names that were reserved without coordination, which invites an eventual name-assignment collision. The remedy is this base document, which defines a registry for these names, and attempts to register all those already in use, with a companion document [attrleaf-fix] developed to direct changes to the pre-registry specifications that used underscore-based (global) node names.

2. DNS Underscore Scoped Entry Registries Function

A registry for "global" DNS node names that begin with an underscore is defined here. The purpose of the Underscore Global Registry is to avoid collisions resulting from the use of the same underscore-based name, for different applications.
If a public specification calls for use of an underscore-prefixed
domain node name, the "global" underscored name -- the underscored
name that is closest to the DNS root -- MUST be entered into this
registry.

An underscored name defines the scope of use for specific resource
record types, which are associated with the domain name that is the
"parent" to the branch defined by the underscored name. A given name
defines a specific, constrained context for one or more RR types,
where use of such record types conforms to the defined constraints.

Within an underscore scoped leaf, other RRsets that are not
specified as part of the scope MAY be used.

Structurally, the registry is defined as a single, flat table of RR
types, under node names beginning with underscore. In some cases,
such as for use of an "SRV" record, the full scoping name might be
multi-part, as a sequence of underscored names. Semantically, that
sequence represents a hierarchical model and it is theoretically
reasonable to allow re-use of a subordinate underscored name in a
different, global underscored context; that is, a subordinate name is
meaningful only within the scope of the global underscored name.
Therefore they are ignored by this DNS Underscore Global Scoped Entry
Registry. This registry is for the definition of highest-level -- ie, global -- underscored node name used.

```
+----------------------------+
|                       NAME |
+----------------------------+
|                  _service1 |
|                  _protoB._service2 |
|                  _protoB._service3 |
|                  _protoC._service3 |
|          _protoD._service4 |
| _protoE._region._authority |
+----------------------------+
```

Table 1: Examples of Underscored Names

Only global underscored names are registered in the IANA Underscore
Only the global underscored names ",_service1", ",_service2", Global
table. (From the example, that would mean registering "_service3",
",_service4", and ",authority" are registered in the IANA _service1,
,_service2, _service3, _service 4, and _authority.)

The use of underscored node names is specific to each Rrtype that
is being scoped. Each name defines a place, but does not define
the rules for what appears underneath that place, either as
additional underscored naming or as a leaf node with resource records. Details for those rules are provided by specifications for individual RRTYPEs. The sections below describe the way that existing underscore labels are used with the RRTYPEs that they name.

- Definition and registration of subordinate, underscore node names is the responsibility of the specification that creates the global registry entry.

That is, if a scheme using a global underscore node name has one or more subordinate levels of underscore node naming, the namespaces from which names for those lower levels are chosen are controlled by the parent underscore node name. Each globally-registered underscore name owns a distinct, subordinate name space.

3. RRset Use Registration Template

This section provides a basic template that can be used to register new entries in the IANA DNS Underscore Global Scoped Entry Registry, if the global underscored name above the RRTYPE is not already registered. The text can be added to specifications using RRTYPE/_Node-name combinations that have not already been registered.

"Per {RFC Attrleaf} please add the following entry to the DNS Underscore Global Scoped Entry Registry:"

Note to RFC Editor: Please replace the above "{RFC Attrleaf}" text with a reference to this document’s RFC number. /d

+----------+-------------------+------------------------------------+
| RR Type  | _NODE NAME        | REFERENCE                          |
+----------+-------------------+------------------------------------+
| {RRTYPE} | _(DNS global node | (citation for the document making  |
|          | name)             | the addition.)                     |
+----------+-------------------+------------------------------------+

Table 2: Underscore Global Registry Entry Template

4. IANA Considerations

Per [RFC8126] IANA is requested to establish the:

"DNS Underscore Global Scoped Entry Registry"

This section describes actions requested of IANA. The guidance in [IANA] is used.
4.1. DNS Underscore Global Scoped Entry Registry

The DNS Global Underscore Scoped Entry Registry is any DNS node name that begin with the underscore character ("_", ASCII 0x5F) and is the underscored node name closest to the root; that is it defines the highest-level of a DNS branch, under a "parent" domain name.

- This registry is to operate under the IANA rules for "Expert Review" registration; see Section 5.
- The contents of each entry in the Global registry are defined in Section 4.2.
- Each entry in the registry MUST contain values for all of the fields specified in Section 4.2.
- Within the registry, the combination of RR Type and _Node Name MUST be unique.
- The table is to be maintained with entries sorted by the first column (RR Type) and, within that, the second column (_Node Name).
- The required Reference for an entry MUST have a stable resolution to the organization controlling that registry entry.

4.2. DNS Underscore Global Scoped Entry Registry Definition

A registry entry contains:

- RR Type: Lists an RR type that is defined for use within this scope.
- _Node Name: Specifies a single, underscored name that defines a reserved name; this name is the "global" entry name for the scoped resource record types that are associated with that name; for characters in the name that have an upper-case form and a lower-case form, the character MUST be recorded as lower-case, to simplify name comparisons.
- References: Lists the specification that defines a record type and its use under this _Node Name. The organization producing the specification retains control over the registry entry for the _Node Name.
Each RR type that is to be used with a _Node Name MUST have a separate registry entry.

4.3. Initial entries

Initial entries in the registry are:

<table>
<thead>
<tr>
<th>RR Type</th>
<th>_NODE NAME</th>
<th>REFERENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>NULL</td>
<td>_ta-* (see note)</td>
<td>[RFC8145]</td>
</tr>
<tr>
<td>OPENPGPKEY</td>
<td>_openpgpkey</td>
<td>[RFC7929]</td>
</tr>
<tr>
<td>SMIMEA</td>
<td>_smimecert</td>
<td>[RFC8162]</td>
</tr>
<tr>
<td>SRV</td>
<td>_dccp</td>
<td>[RFC2782]</td>
</tr>
<tr>
<td>SRV</td>
<td>_http</td>
<td>[RFC4386]</td>
</tr>
<tr>
<td>SRV</td>
<td>_ipv6</td>
<td>[RFC5026]</td>
</tr>
<tr>
<td>SRV</td>
<td>_ldap</td>
<td>[RFC4386]</td>
</tr>
<tr>
<td>SRV</td>
<td>_ocsp</td>
<td>[RFC4386]</td>
</tr>
<tr>
<td>SRV</td>
<td>_sctp</td>
<td>[RFC2782]</td>
</tr>
<tr>
<td>SRV</td>
<td>_sip</td>
<td>[RFC5509]</td>
</tr>
<tr>
<td>SRV</td>
<td>_tcp</td>
<td>[RFC2782]</td>
</tr>
<tr>
<td>SRV</td>
<td>_udp</td>
<td>[RFC2782]</td>
</tr>
<tr>
<td>SRV</td>
<td>_xmpp</td>
<td>[RFC3921]</td>
</tr>
<tr>
<td>TLSA</td>
<td>_dane</td>
<td>[RFC7671]</td>
</tr>
<tr>
<td>TLSA</td>
<td>_sctp</td>
<td>[RFC6698]</td>
</tr>
<tr>
<td>TLSA</td>
<td>_tcp</td>
<td>[RFC6698]</td>
</tr>
<tr>
<td>TLSA</td>
<td>_udp</td>
<td>[RFC6698]</td>
</tr>
<tr>
<td>TXT</td>
<td>_acme-challenge</td>
<td>[ACME]</td>
</tr>
<tr>
<td>TXT</td>
<td>_dmarc</td>
<td>[RFC7489]</td>
</tr>
<tr>
<td>TXT</td>
<td>_domainkey</td>
<td>[RFC6376]</td>
</tr>
<tr>
<td>TXT</td>
<td>_mta-sts</td>
<td>[MTA-STS]</td>
</tr>
<tr>
<td>TXT</td>
<td>_spf</td>
<td>[RFC7208]</td>
</tr>
<tr>
<td>TXT</td>
<td>_tcp</td>
<td>[RFC6763]</td>
</tr>
<tr>
<td>TXT</td>
<td>_udp</td>
<td>[RFC6763]</td>
</tr>
<tr>
<td>TXT</td>
<td>_vouch</td>
<td>[RFC5518]</td>
</tr>
<tr>
<td>URI</td>
<td>_acct</td>
<td>[RFC6118]</td>
</tr>
<tr>
<td>URI</td>
<td>_dccp</td>
<td>[RFC7566]</td>
</tr>
<tr>
<td>URI</td>
<td>_email</td>
<td>[RFC6118]</td>
</tr>
<tr>
<td>URI</td>
<td>_ems</td>
<td>[RFC6118]</td>
</tr>
<tr>
<td>URI</td>
<td>_fax</td>
<td>[RFC6118]</td>
</tr>
<tr>
<td>URI</td>
<td>_ft</td>
<td>[RFC6118]</td>
</tr>
<tr>
<td>URI</td>
<td>_h323</td>
<td>[RFC6118]</td>
</tr>
<tr>
<td>URI</td>
<td>_iax</td>
<td>[RFC6118]</td>
</tr>
<tr>
<td>URI</td>
<td>_ical-access</td>
<td>[RFC6118]</td>
</tr>
<tr>
<td>URI</td>
<td>_ical-sched</td>
<td>[RFC6118]</td>
</tr>
<tr>
<td>URI</td>
<td>_ifax</td>
<td>[RFC6118]</td>
</tr>
<tr>
<td>URI</td>
<td>_im</td>
<td>[RFC6118]</td>
</tr>
<tr>
<td>URI</td>
<td>_mms</td>
<td>[RFC6118]</td>
</tr>
<tr>
<td>URI</td>
<td>_pres</td>
<td>[RFC6118]</td>
</tr>
<tr>
<td>URI</td>
<td>_pstn</td>
<td>[RFC6118]</td>
</tr>
<tr>
<td>URI</td>
<td>_sctp</td>
<td>[RFC6118]</td>
</tr>
<tr>
<td>URI</td>
<td>_sip</td>
<td>[RFC6118]</td>
</tr>
<tr>
<td>URI</td>
<td>_sms</td>
<td>[RFC6118]</td>
</tr>
<tr>
<td>URI</td>
<td>_tcp</td>
<td>[RFC6118]</td>
</tr>
<tr>
<td>URI</td>
<td>_udp</td>
<td>[RFC6118]</td>
</tr>
<tr>
<td>URI</td>
<td>_unifmsg</td>
<td>[RFC6118]</td>
</tr>
<tr>
<td>URI</td>
<td>_vcard</td>
<td>[RFC6118]</td>
</tr>
<tr>
<td>URI</td>
<td>_videomsg</td>
<td>[RFC6118]</td>
</tr>
<tr>
<td>URI</td>
<td>_voice</td>
<td>[RFC6118]</td>
</tr>
<tr>
<td>URI</td>
<td>_voicemsg</td>
<td>[RFC6118]</td>
</tr>
<tr>
<td>URI</td>
<td>_vpim</td>
<td>[RFC6118]</td>
</tr>
<tr>
<td>URI</td>
<td>_web</td>
<td>[RFC6118]</td>
</tr>
<tr>
<td>URI</td>
<td>_xmpp</td>
<td>[RFC6118]</td>
</tr>
</tbody>
</table>

+----------------------------------+

Table 3: Underscore Global Registry (initial entries)

NOTE: Under the NULL RR, the entry "_ta-*" denotes all node names beginning with the string "_ta-*". It does NOT refer to a DNS wildcard specification.

4.4. Enumservices Registrations Registry

Please add a note to the Enumservice Registrations registry with the following -- or similar -- language:

"When adding an entry to this registry, strong consideration should be given to also adding an entry to the ‘DNS Underscore Global Scoped Entry Registry’.”

5. Guidance for Expert Review

This section provides guidance for expert review of registration requests in the DNS Underscore Global Scoped Entry Registry.

This review is solely to determine adequacy of a requested entry in this Registry, and does not include review of other aspects of the document specifying that entry. For example such a document might also contain a definition of the resource record type that is referenced by the requested entry. Any required review of that definition is separate from the expert review required here.

The review is for the purposes of ensuring that:

- The details for creating the registry entry are sufficiently clear, precise and complete
The combination of the underscored name, under which the listed resource record type is used, and the resource record type, is unique in the table.

For the purposes of this Expert Review, other matters of the specification’s technical quality, adequacy or the like are outside of scope.

6. Security Considerations

This memo raises no security issues.

7. References

7.1. Normative References


7.2. References — Informative

[[attrleaf-fix]]
7.3. URIs

[1] mailto:dnsop@ietf.org

Appendix A. Acknowledgements


Special thanks to Ray Bellis for his persistent encouragement to continue this effort, as well as the suggestion for an essential simplification to the registration model.

Author’s Address

Dave Crocker
Brandenburg InternetWorking
675 Spruce Dr.
Sunnyvale, CA  94086
USA

Phone: +1.408.246.8253
Email: dcrocker@bbiw.net
URI:  http://bbiw.net/