DNS Scoped Data Through "Underscore" Naming of Attribute Leaves
draft-ietf-dnsop-attrleaf-14

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

Copyright Notice

Table of Contents

[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 BCP
   14 [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:

                         domain-name.example
                           /
                          RRset

   the arrangement is:

                        _branch.domain-name.example
                          /
                         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.

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.

o 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.

o 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 |
              |     _useX._protoD._service4 |
              | _protoE._region._authority |
              +----------------------------+
```

             Table 1: Examples of Underscored Names

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

   o 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.

   o 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

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.

o This registry is to operate under the IANA rules for "Expert
   Review" registration; see Section 5.

o The contents of each entry in the Global registry are defined in
   Section 4.2.

o Each entry in the registry MUST contain values for all of the
   fields specified in Section 4.2.

o Within the registry, the combination of RR Type and _Node Name
   MUST be unique.

o The table is to be maintained with entries sorted by the first
   column (RR Type) and, within that, the second column (_Node Name).

o 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 specification that defines a record type and its
               use under this Name. The organization producing the
               specification retains control over the registry entry for
               the _Node Name

   Each RR type that is to be used MUST have a separate registry entry.

4.3. Initial entries

   Initial entries in the registry are:

```
        +------------+------------------+------------+
        | RR Type    | _NODE NAME       | REFERENCE  |
        +------------+------------------+------------+
        | NULL       | _ta-* {see note} | [RFC8145]  |
        | OPENPGPKEY | _openpgpkey      | [RFC7929]  |
        | PTR        | _tcp             | [RFC6763]  |
        | PTR        | _udp             | [RFC6763]  |
        | SMIMEA     | _smimecert       | [RFC8162]  |
        | SRV        | _dccp            | [RFC2782]  |
        | SRV        | _ipv6            | [RFC5026]  |
        | SRV        | _sip             | [RFC5509]  |
        | SRV        | _sctp            | [RFC2782]  |
        | SRV        | _tcp             | [RFC2782]  |
        | SRV        | _udp             | [RFC2782]  |
        | SRV        | _xmpp            | [RFC3921]  |
        | TLSA       | _dane            | [RFC7671]  |
        | TLSA       | _sctp            | [RFC6698]  |
        | TLSA       | _tcp             | [RFC6698]  |
        | TLSA       | _udp             | [RFC6698]  |
        | TXT        | _mta-sts         | [MTA-STS]  |
        | TXT        | _acme-challenge  | [ACME]     |
        | TXT        | _dmarc           | [RFC7489]  |
        | TXT        | _domainkey       | [RFC6376]  |
```

```
              | TXT        | _spf            | [RFC7208]  |
              | TXT        | _vouch          | [RFC5518]  |
              | URI        | _iax            | [RFC6315]  |
              | URI        | _acct           | [RFC7566]  |
              | URI        | _dccp           | [RFC6118]  |
              | URI        | _email          | [RFC6118]  |
              | URI        | _ems            | [RFC6118]  |
              | URI        | _fax            | [RFC6118]  |
              | URI        | _ft             | [RFC6118]  |
              | URI        | _h323           | [RFC6118]  |
              | URI        | _ical-sched     | [RFC6118]  |
              | URI        | _ical-access    | [RFC6118]  |
              | URI        | _ifax           | [RFC6118]  |
              | URI        | _im             | [RFC6118]  |
              | URI        | _mms            | [RFC6118]  |
              | URI        | _pres           | [RFC6118]  |
              | URI        | _pstn           | [RFC7553]  |
              | URI        | _sctp           | [RFC7553]  |
              | URI        | _sip            | [RFC7553]  |
              | URI        | _sms            | [RFC6118]  |
              | URI        | _tcp            | [RFC6118]  |
              | URI        | _udp            | [RFC6118]  |
              | URI        | _unifmsg        | [RFC6118]  |
              | URI        | _vcard          | [RFC6118]  |
              | URI        | _videomsg       | [RFC6118]  |
              | URI        | _voice          | [RFC6118]  |
              | URI        | _voicemsg       | [RFC6118]  |
              | URI        | _vpim           | [RFC6118]  |
              | URI        | _web            | [RFC6118]  |
              | URI        | _xmpp           | [RFC6118]  |
              +-----------+-----------------+-----------+
```

              Table 3: Underscore Global Registry (initial entries)

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

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:

    o The details for creating the registry entry are sufficiently
       clear, precise and complete

    o 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

    [ACME]   Barnes, R., Hoffman-Andrews, J., McCarney, D., and J.
                Kasten, "Automatic Certificate Management Environment
                (ACME)", I-D draft-ietf-acme-acme-11, March 2018.

    [IANA]   M. Cotton, B. Leiba, and T. Narten, "Guidelines for
                Writing an IANA Considerations Section in RFCs", RFC 8126,
                June 2017.

    [MTA-STS]   Margolis, D., Risher, M., Ramakrishnan, B., Brotman, A.,
                and J. Jones, "SMTP MTA Strict Transport Security (MTA-
                STS)", I-D draft-ietf-uta-mta-sts.

    [RFC1034]   Mockapetris, P., "Domain Names - Concepts and Facilities",
                STD 13, RFC 1034, November 1987.

    [RFC1035]   Mockapetris, P., "Domain Names - Implementation and
                Specification", STD 13, RFC 1035, November 1987.

    [RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate
                Requirement Levels", BCP 14, RFC 2119, March 1997.

    [RFC2181]   Elz, R. and R. Bush, "Clarifications to the DNS
                Specification", RFC 2181, July 1997.

   [RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for
              specifying the location of services (DNS SRV)", RFC 2782,
              February 2000.

   [RFC3921] Saint-Andre, P., Ed., "Extensible Messaging and Presence
              Protocol (XMPP): Instant Messaging and Presence",
              RFC 3921, DOI 10.17487/RFC3921, October 2004,
              <https://www.rfc-editor.org/info/rfc3921>.

   [RFC5026] Giaretta, G., Ed., Kempf, J., and V. Devarapalli, Ed.,
              "Mobile IPv6 Bootstrapping in Split Scenario", RFC 5026,
              DOI 10.17487/RFC5026, October 2007,
              <https://www.rfc-editor.org/info/rfc5026>.

   [RFC5509] Loreto, S., "Internet Assigned Numbers Authority (IANA)
              Registration of Instant Messaging and Presence DNS SRV RRs
              for the Session Initiation Protocol (SIP)", RFC 5509,
              DOI 10.17487/RFC5509, April 2009,
              <https://www.rfc-editor.org/info/rfc5509>.

   [RFC5518] Hoffman, P., Levine, J., and A. Hathcock, "Vouch By
              Reference", RFC 5518, April 2009.

   [RFC6118] Hoeneisen, B. and A. Mayrhofer, "Update of Legacy IANA
              Registrations of Enumservices", RFC 6118,
              DOI 10.17487/RFC6118, March 2011,
              <https://www.rfc-editor.org/info/rfc6118>.

   [RFC6315] Guy, E. and K. Darilion, "IANA Registration for
              Enumservice 'iax'", RFC 6315, DOI 10.17487/RFC6315, July
              2011, <https://www.rfc-editor.org/info/rfc6315>.

   [RFC6335] Cotton, M., Eggert, L., Tpuch, J., Westerlund, M., and S.
              Cheshire, "Internet Assigned Numbers Authority (IANA)
              Procedures for the Management of the Service Name and
              Transport Protocol Port Number Registry", RFC 6335, Aug
              2011.

   [RFC6376] Crocker, D., Hansen, T., and M. Kucherawy, "DomainKeys
              Identified Mail (DKIM) Signatures", RFC 6376, Sept 2011.

   [RFC6698] Hoffman, J. and J. Schlyter, "The DNS-Based Authentication
              of Named Entities (DANE) Transport Layer Security (TLS)
              Protocol: TLSA", RFC 6698, August .

   [RFC6763] Cheshire, S. and M. Krochmal, "DNS-Based Service
              Discovery", RFC 6763, DOI 10.17487/RFC6763, February 2013,
              <https://www.rfc-editor.org/info/rfc6763>.

   [RFC7208] Kitterman, S., "Sender Policy Framework (SPF) for
              Authorizing Use of Domains in E-Mail, Version 1",
              RFC 7208, April 2014.

   [RFC7489] Kucherawy, M., Ed. and E. Zwicky, Ed., "Domain-based
              Message Authentication, Reporting, and Conformance
              (DMARC)", RFC 7489, March 2015.

   [RFC7553] Falstrom, P. and O. Kolkman, "The Uniform Resource
              Identifier (URI) DNS Resource Record", RFC 7553,
              ISSN 2070-1721, June 2015.

   [RFC7566] Goix, L. and K. Li, "Enumservice Registration for 'acct'
              URI", RFC 7566, DOI 10.17487/RFC7566, June 2015,
              <https://www.rfc-editor.org/info/rfc7566>.

   [RFC7671] Dukhovni, V. and W. Hardaker, "The DNS-Based
              Authentication of Named Entities (DANE) Protocol: Updates
              and Operational Guidance", RFC 7671, DOI 10.17487/RFC7671,
              October 2015, <https://www.rfc-editor.org/info/rfc7671>.

   [RFC7929] Wouters, P., , RFC 7929, August 2016.

   [RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for
              Writing an IANA Considerations Section in RFCs", RFC 8126,
              June 2017.

   [RFC8145] Wessels, D., Kumari, W., and P. Hoffman, "Signaling Trust
              Anchor Knowledge in DNS Security Extensions (DNSSEC)",
              RFC 8145, April 2017.

   [RFC8162] Hoffman, P. and J. Schlyter, "Using Secure DNS to
              Associate Certificates with Domain Names for S/MIME",
              RFC 8162, May 2017.

   [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC
              2119 Key Words", RFC 8162, May 2017.

   [RFC952]   Harrenstien, K., Stahl, M., and E. Feinler, "DOD Internet
              Host Table Specification", RFC 952, October 1985.

7.2. URIs

   [1] mailto:dnsop@ietf.org

Appendix A. **Acknowledgements**

   Thanks go to Bill Fenner, Dick Franks, Tony Hansen, Martin Hoffmann,
   Paul Hoffman, Peter Koch, Olaf Kolkman, Murray Kucherawy, John
   Levine, and Andrew Sullivan for diligent review of the (much) earlier
   drafts. For the later enhancements, thanks to: Stephane Bortzmeyer,
   Alissa Cooper, Bob Harold, Benjamin Kaduk, Mirja Kuehlewind, Warren
   Kumari, John Levine, Joel Jaeggli, Benno Overeinder, Eric Rescorla,
   Adam Roach, Petr Špaček, Ondřej Sury, Paul Vixie, Tim
   Wicinski, and Paul Wouters.

   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/