Internet Engineering Task Force (IETF)
Request for Comments: 8552
BCP: 222
Category: Best Current Practice
ISSN: 2070-1721

D. Crocker
Brandenburg InternetWorking
March 2019

Scoped Interpretation of DNS Resource Records through "Underscored" Naming of Attribute Leaves

Abstract

Formally, any DNS Resource Record (RR) 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 the underscore character (e.g., "_name"). 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 "Underscored and Globally Scoped DNS Node Names" registry with IANA. The purpose of this registry is to avoid collisions resulting from the use of the same underscored name for different services.

Status of This Memo

This memo documents an Internet Best Current Practice.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on BCPs is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8552.

Copyright Notice

Table of Contents

1. Introduction

The core Domain Name System (DNS) technical specifications ([RFC1035] and [RFC2181]) 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, with significant adoption and use barriers occurring over the life of the DNS.

1.1. Underscore-Based Scoping

As an alternative to defining a new RR TYPE, some DNS service enhancements call for using an existing resource record type but specifying 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 containing the specific resource record sets that are formally defined and constrained. Specifically:

> The leaf occurs in a branch having a distinguished naming convention: there is a parent domain name to which the scoped data applies. The branch is under this name. The sub-branch is indicated by a sequence of one or more reserved DNS node names; at least the first (highest) of these names begins with an underscore (e.g., "_name").

Because the DNS rules for a "host" (host name) do not allow use of the underscore character, the underscored name is distinguishable from all legal host names [RFC0952]. Effectively, this convention for naming leaf nodes 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 are returned.

A simple example is DomainKeys Identified Mail (DKIM) [RFC6376], which uses "_domainkey" to define a place to hold a TXT record containing signing information for the parent domain.

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

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 the underscore character (e.g., "_name"). A global underscored node name is the one that is closest to the root of the DNS hierarchy, also called the highest level or topmost. In the presentation convention described in Section 3.1 of [RFC1034], this is the rightmost 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 are only 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 underscored 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 (see [RFC2782] and [RFC7553]). The SRV and URI specifications serve as templates, defining RRs 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 underscored 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 underscored names that were reserved without coordination, which invites an eventual name-assignment collision. The remedy is this base document and a companion document ([RFC8553]), which define a registry for these names and attempt to register all those already in use as well as to direct changes to the pre-registry specifications that used global underscored node names.

2. "Underscored and Globally Scoped DNS Node Names" Registry

A registry for global DNS node names that begin with an underscore is defined here. The purpose of the "Underscored and Globally Scoped DNS Node Names" registry is to avoid collisions resulting from the use of the same underscored name for different applications.

> If a public specification calls for use of an underscored node name, the global underscored node 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 a leaf that is underscore scoped, 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 reuse 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 node name. Therefore, they are ignored by this "Underscored and Globally Scoped DNS Node Names" registry. This registry is for the definition of highest-level -- that is, 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 node names are registered in the "Underscored and Globally Scoped DNS Node Names" registry. From the example above, that would mean _service1, _service2, _service3, _service 4, and _authority would be listed in the IANA registry.

- o The use of underscored node names is specific to each RR TYPE 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 RR TYPEs. The sections below describe the way that existing underscored names are used with the RR TYPEs that they name.

- o Definition and registration of subordinate underscored node names are the responsibility of the specification that creates the global underscored node name registry entry.

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

3. Guidance for Registering RRset Use

This section provides guidance for specification writers, with a basic template they can use, to register new entries in the "Underscored and Globally Scoped DNS Node Names" registry. The text can be added to specifications using RR TYPE / _NODE NAME combinations that have not already been registered:

Per RFC 8552, please add the following entry to the "Underscored and Globally Scoped DNS Node Names" registry:

RR Type	_NODE NAME	Reference
{RR TYPE}	_{DNS global node name}	{citation for the document making the addition.}

Table 2: Template for Entries in the "Underscored and Globally Scoped DNS Node Names" Registry

4. IANA Considerations

IANA has established the "Underscored and Globally Scoped DNS Node Names" registry. This section describes the registry, the definitions, the initial entries, the use of_ta and _example, and the use of [RFC8126] as guidance for expert review. IANA has also updated the "Enumservices Registrations" registry with a pointer to this document.

4.1. "Underscored and Globally Scoped DNS Node Names" Registry

The "Underscored and Globally Scoped DNS Node Names" registry includes any DNS node name that begins 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 operates under the IANA rules for "Expert Review" registration; see Section 4.1.5.
- o The contents of each entry in the registry are defined in Section 4.1.1.
- o Each entry in the registry MUST contain values for all of the fields specified in Section 4.1.1.
- 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.

4.1.1. Contents of an Entry in the "Underscored and Globally Scoped DNS Node Names" Registry

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 uppercase form and a lowercase form, the character MUST be recorded as lowercase to simplify name comparisons.

Reference: 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.

4.1.2. Initial Node Names

The initial entries in the registry are as follows:

RR Type	_NODE NAME	Reference
*	_example	Section 4.1.4
NULL	_ta-* {Section 4.1.3}	[RFC8145]
OPENPGPKEY	_openpgpkey	[RFC7929]
SMIMEA	_smimecert	[RFC8162]
SRV	_dccp	[RFC2782]
SRV	_http	[RFC4386]
SRV	_ipv6	[RFC5026]
SRV	_ldap	[RFC4386]
SRV	_ocsp	[RFC4386]
SRV	_sctp	[RFC2782]
SRV	_sip	[RFC5509]
SRV	_tcp	[RFC2782]
SRV	_udp	[RFC2782]
SRV	_xmpp	[RFC3921]
TLSA	_dane	[RFC7671]
TLSA	_sctp	[RFC6698]
TLSA	_tcp	[RFC6698]

TLSA	_udp	[RFC6698]
TXT	_acme-challenge	[RFC8555]
TXT	_dmarc	[RFC7489]
TXT	_domainkey	[RFC6376]
TXT	_mta-sts	[RFC8461]
TXT	_spf	[RFC7208]
TXT	_sztp	[ZEROTOUCH]
TXT	_tcp	[RFC6763]
TXT	_udp	[RFC6763]
TXT	_vouch	[RFC5518]
URI	_acct	[RFC6118]
URI	_dccp	[RFC7566]
URI	_email	[RFC6118]
URI	_ems	[RFC6118]
URI	_fax	[RFC6118]
URI	_ft	[RFC6118]
URI	_h323	[RFC6118]
URI	_iax	[RFC6118]
URI	_ical-access	[RFC6118]
URI	_ical-sched	[RFC6118]
URI	_ifax	[RFC6118]
URI	_im	[RFC6118]
URI	_mms	[RFC6118]
URI	_pres	[RFC6118]
URI	_pstn	[RFC6118]
URI	_sctp	[RFC6118]
URI	_sip	[RFC6118]
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: Initial Contents of the "Underscored and Globally Scoped DNS Node Names" Registry

4.1.3. _ta

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

4.1.4. _example

The node name "_example" is reserved across all RRsets.

4.1.5. Guidance for Expert Review

This section provides guidance for expert review of registration requests in the "Underscored and Globally Scoped DNS Node Names" registry.

> This review is solely to determine adequacy of a requested entry in this registry, and it 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.

4.2. Enumservices Registrations Registry

The following note has been added to the "Enumservice Registrations" registry:

> When adding an entry to this registry, strong consideration should be given to also adding an entry to the "Underscored and Globally Scoped DNS Node Names" registry.

5. Security Considerations

This memo raises no security issues.

6. References

6.1. Normative References

[RFC0952] Harrenstien, K., Stahl, M., and E. Feinler, "DoD Internet host table specification", RFC 952, DOI 10.17487/RFC0952, October 1985, <https://www.rfc-editor.org/info/rfc952>.

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987, <https://www.rfc-editor.org/info/rfc1034>.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/info/rfc1035>.

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

[RFC2181] Elz, R. and R. Bush, "Clarifications to the DNS Specification", RFC 2181, DOI 10.17487/RFC2181, July 1997, <https://www.rfc-editor.org/info/rfc2181>.

[RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, DOI 10.17487/RFC2782, February 2000, <https://www.rfc-editor.org/info/rfc2782>.

[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>.

[RFC4386] Boeyen, S. and P. Hallam-Baker, "Internet X.509 Public Key Infrastructure Repository Locator Service", RFC 4386, DOI 10.17487/RFC4386, February 2006, <https://www.rfc-editor.org/info/rfc4386>.

[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, DOI 10.17487/RFC5518, April 2009, <https://www.rfc-editor.org/info/rfc5518>.

[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>.

[RFC6335] Cotton, M., Eggert, L., Touch, 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", BCP 165, RFC 6335, DOI 10.17487/RFC6335, August 2011, <https://www.rfc-editor.org/info/rfc6335>.

[RFC6376] Crocker, D., Ed., Hansen, T., Ed., and M. Kucherawy, Ed., "DomainKeys Identified Mail (DKIM) Signatures", STD 76, RFC 6376, DOI 10.17487/RFC6376, September 2011, <https://www.rfc-editor.org/info/rfc6376>.

[RFC6698] Hoffman, P. and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", RFC 6698, DOI 10.17487/RFC6698, August 2012, <https://www.rfc-editor.org/info/rfc6698>.

[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 Email, Version 1", RFC 7208, DOI 10.17487/RFC7208, April 2014, <https://www.rfc-editor.org/info/rfc7208>.

[RFC7489] Kucherawy, M., Ed. and E. Zwicky, Ed., "Domain-based Message Authentication, Reporting, and Conformance (DMARC)", RFC 7489, DOI 10.17487/RFC7489, March 2015, <https://www.rfc-editor.org/info/rfc7489>.

[RFC7553] Faltstrom, P. and O. Kolkman, "The Uniform Resource Identifier (URI) DNS Resource Record", RFC 7553, DOI 10.17487/RFC7553, June 2015, <https://www.rfc-editor.org/info/rfc7553>.

[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., "DNS-Based Authentication of Named Entities (DANE) Bindings for OpenPGP", RFC 7929, DOI 10.17487/RFC7929, August 2016, <https://www.rfc-editor.org/info/rfc7929>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[RFC8145] Wessels, D., Kumari, W., and P. Hoffman, "Signaling Trust Anchor Knowledge in DNS Security Extensions (DNSSEC)", RFC 8145, DOI 10.17487/RFC8145, April 2017, <https://www.rfc-editor.org/info/rfc8145>.

[RFC8162] Hoffman, P. and J. Schlyter, "Using Secure DNS to Associate Certificates with Domain Names for S/MIME", RFC 8162, DOI 10.17487/RFC8162, May 2017, <https://www.rfc-editor.org/info/rfc8162>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8461] Margolis, D., Risher, M., Ramakrishnan, B., Brotman, A., and J. Jones, "SMTP MTA Strict Transport Security (MTA-STS)", RFC 8461, DOI 10.17487/RFC8461, September 2018, <https://www.rfc-editor.org/info/rfc8461>.

[RFC8555] Barnes, R., Hoffman-Andrews, J., McCarney, D., and J. Kasten, "Automatic Certificate Management Environment (ACME)", RFC 8555, DOI 10.17487/RFC8555, March 2019, <https://www.rfc-editor.org/info/rfc8555>.

6.2. Informative References

[RFC8553] Crocker, D., "DNS Attrleaf Changes: Fixing Specifications That Use Underscored Node Names", RFC 8553, DOI 10.17487/RFC8553, March 2019, <https://www.rfc-editor.org/info/rfc8553>.

[ZEROTOUCH] Watsen, K., Abrahamsson, M., and I. Farrer, "Secure Zero Touch Provisioning (SZTP)", Work in Progress, draft-ietf-netconf-zerotouch-29, January 2019.

Acknowledgements

Thanks go to Bill Fenner, Dick Franks, Tony Hansen, Martin Hoffmann, Paul Hoffman, Peter Koch, Olaf Kolkman, Murray Kucherawy, John Levine, Benno Overeinder, and Andrew Sullivan for diligent review of the (much) earlier draft versions. For the later enhancements, thanks to Stephane Bortzmeyer, Alissa Cooper, Bob Harold, Joel Jaeggli, Benjamin Kaduk, Mirja Kuehlewind, Warren Kumari, John Levine, Benno Overeinder, Eric Rescorla, Adam Roach, Petr Spacek, Ondrej 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
United States of America

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