dnsop
Internet-Draft
Intended status: Best Current Practice
Expires: September 23, 2018

D. Crocker
Brandenburg InternetWorking

March 22, 2018

DNS Scoped Data Through '_Underscore' Naming of Attribute Leaves
draft-ietf-dnsop-attrleaf-04

Abstract

Formally, any DNS resource record may occur for any domain name. However some services have defined an operational convention, which applies to DNS leaf nodes that are under a DNS branch having one or more reserved node names, each beginning with an underscore. The underscore naming construct defines a semantic scope for DNS records 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 September 23, 2018.

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 records (RRs) are permitted to be associated with particular names.[RFC1035] 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 records, on the expectation that new ones would be added as needed. Unfortunately, the addition of new resource records has proved extremely challenging, over the life of the DNS, with significant adoption and use barriers.

1.1. _Underscore Scoping

As an alternative to defining new RRs, some DNS service enhancements call for using an existing resource record, but specify a restricted scope for its occurrence. That scope is a leaf node, within which the uses of specific resource records 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) are not allowed to use the underscore character, this distinguishes the underscore name from all legal host names [RFC1035]. Effectively, this convention for leaf node naming creates a space for the listing of 'attributes' -- in the form of resource records -- that are associated with the parent domain, above the underscore sub-branch.

The scoping feature is particularly useful when generalized resource records 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 "RR"s 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 the records do not adequately self-identify. With underscore-based scoping, only the relevant "RR"s are returned.

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

This specification formally defines how underscore labels are used as "attribute" enhancements for their parent domain names. For example, domain name "_domainkey.example." acts as attribute of parent domain name "example." To avoid collisions resulting from the use of the same underscore-based labels for different applications, this document establishes DNS Underscore Global Scoped Entry IANA Registry for the highest-level reserved names that begin with _underscore; _underscore-based names that are farther down the hierarchy are handled within the scope of the highest-level _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.

1.2. Scaling Benefits for TXT, SRV, and URI Resource Records

Some resource records are generic and support a variety of uses. Each additional use defines its own rules and, possibly, its own internal syntax and node-naming conventions to distinguish among particular types. The "TXT", "SRV", and "URI" records are notable examples. Their use can scale poorly, particularly when the same "RR" can be present in the same leaf node, but with different uses.

An increasingly-popular approach, with excellent scaling properties, place the RR under a node with an underscore-based name, at a defined place in the DNS tree, so as to constrain the use of particular "RR"s farther down the branch with that name. This means that a direct lookup produces only the desired records, at no greater cost than a typical DNS lookup.

The definition of a underscore global registry, provided in this specification, primarily attends to the top-most names used for RRs; that is the _underscore "global" names.

2. DNS Underscore Scoped Entry Registries Function

A global registry for DNS nodes names that begin with an _underscore is defined here.

> The 'global' (right-most) node name that uses an _underscore prefix MUST be entered into this registry.

The names define scope of use for specific resource records, which are associated with the domain name that is the "parent" to the branch defined by the _underscore naming.

> A given name defines a specific, constrained context for one or more RR records, in which use of such records MUST conform to the defined constraints. Within this scope, other resource records that are not specified MAY be used.

The purpose of the Underscore Global Registry is to avoid collisions resulting from the use of the same _underscore-based name, for different applications.

Structurally, the registry is defined as a single, flat table of names that begin 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 underscore names. Semantically, that sequence represents a hierarchical model and it is theoretically reasonable to allow re-use of a subordinate underscore name in different underscore context; that is, a subordinate name is meaningful only within the scope of the first (top-level) underscore name. Therefore they are ignored by this DNS Underscore Global Scoped Entry Registry. This registry is for the definition of highest-level -- ie, global -- underscore node name used.

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

Example of Underscore Names

Only the right-most _underscore names are registered in the IANA Underscore Global table.

Definition and registration of the subordinate underscore node names is the responsibility of the specification that creates the highest-level (right-most) global registry entry.

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

2.1. DNS Underscore Global Scoped Entry Registry Definition

Additions/Removals/Changes: Please post to the list or send the author direct email, that indicates the exact details of changes needed to this table. If a reference needs to be added or changed, the xml for this would be ideal. Thanks. /d .

NOTE TO RFC EDITOR: Please remove "Additions/Removals/ Changes" paragraph prior to publication.

A registry entry contains:

ID: Specifies a textual name for a scoped portion of the DNS. The name will usually be taken from the specification cited in the "Purpose" column and is intended for use in discussions about the entry.

_Node Name: Specifies a single _underscore name that defines a reserved name; this name is the "global" entry name for the scoped resource records that are associated with that name.

Constraints: Specifies any restrictions on use of the DNS Label.

RR(s): Lists the RRs that are defined for use within this scope.

Purpose: Specifies the particular purpose/use for specific "RR"(s), defined for use within the scope of the registered underscore name.

References Lists specifications that define the records and their use under this Name.

Control Name of the organization with authority to make changes for this registration

3. IANA Considerations

Per [RFC8126], IANA is requested to establish two registries:

1. DNS Underscore Global Scoped Entry Registry

2. DNS Underscore Common Second-Level Scoped Entry Registry

This section describes actions requested of IANA. The guidance in [IANA] is used.

3.1. DNS Underscore Global Scoped Entry Registry

The DNS Global Underscore Scoped Entry Registry is for DNS node names that begin with the underscore character (_) and occur at the "top" of a DNS branch -- ie, are right-most -- under a "parent" domain name.

This registry is to operate under the IANA rules for "First Come First Served" registration.

The contents of each entry in the Global registry are defined in Section 2.1.

Additions/Removals/Changes: Please post to the list or send the author direct email, that indicates the exact details of changes needed to this table. If a reference needs to be added or changed, the xml for this would be ideal. Thanks. /d .

NOTE TO RFC EDITOR: Please remove "Additions/Removals/ Changes" paragraph prior to publication.

Initial entries in the registry are:

ID	_NODE NAME	RR	PURPOSE	REFERENCE	CONTROL
SRV TCP	_tcp	SR V	Use of SRV for a TCP-based service	[RFC2782]	IETF
SRV UDP	_udp	SR V	Use of SRV for a UDP-based service	[RFC2782]	IETF
DKIM	_domainkey	TXT	Public key for verifying DKIM signature.	[RFC6376]	IETF
SPF	_spf	TXT	Authorized IP addresses for sending mail	[RFC7208]	IETF
DMARC	_dmarc	TXT	Published DKIM usage practices	[RFC7489]	IETF
VBR	_vouch	TXT	Vouch-by-refererence domain assertion	[RFC5518]	IETF

Table 1: Underscore Global Registry (initial entries)

4. Security Considerations

This memo raises no security issues.

5. References

5.1. Normative References

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

5.2. References -- Informative

[IANA] M. Cotton, B. Leiba, and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", I-D draft-leiba-cotton-iana-5226bis-11, 2017.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

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

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

[RFC6335] Cotton, M., Eggert, L., Tpuch, J., Westerlund, M., and S. Cheshire, "nternet 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.

[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.

5.3. URIs

[1] mailto:dnsop@ietf.org

Appendix A. Acknowledgements

Thanks go to Bill Fenner, Tony Hansen, Peter Koch, Olaf Kolkman, and Andrew Sullivan for diligent review of the (much) earlier drafts. For the later enhancements, thanks to: Stephane Bortzmeyer, Bob Harold, John Levine, Joel Jaeggli, Petr Špaček, Ondřej Surř, Tim Wicinski, and Paul Wouters.

Special thanks to Ray Bellis for more than 12 years of 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/