dnsop
Internet-Draft
Intended status: Best Current Practice
Expires: September 20, 2018

D. Crocker
Brandenburg InternetWorking

March 19, 2018

DNS Scoped Data Through '_Underscore' Naming of Attribute Leaves
draft-ietf-dnsop-attrleaf-03

Abstract

Formally, any DNS resource record may occur for any domain name. However some services have defined an operational convention that applies to DNS leaf nodes that are under a DNS branch that has one or more reserved node names that begin 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 20, 2018.

Copyright Notice

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

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

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],[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 undr a node wit an underscore-based name, at a defined place in the DNS tree, so as to constrain to the use of particular "RR"s farther down the branch using 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 "upper-level" names used for RRs; that is the _underscore "global" names. For efficiency, a single, subordinate _underscore second-level table also is defined, for use with a common set of applications.

2. DNS Underscore Scoped Entry Registries Function

A global registry for DNS nodes names that begin with an _underscore is defined here. The names are used to define scope of use for specific resource records, 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 names are registered in the IANA Underscore Global table. Definition and registration of the subordinate names is the responsibility of the specification that creates the highest-level (right-most) registry entry.

For convenience, an Underscore Common Second-Level Names table is also defined, to cover some popular cases involving the subordinate name used with two-level _underscore naming. In particular, this table covers uses of second-level names that scope SRV RRs use.

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.

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

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

2.2. DNS Common Second-Level Underscore Scoped Entry Registry Definition

A registry entry contains:

ID: Specifies a textual name for a scoped portion of the DNS, occurring under a 'global' -- right-most -- _underscore node name. 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 "second-level" entry name for the scoped resource records that are associated with that name.

Constraints: Specifies any restrictions on use of the name.

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

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

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

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	REFERENCE	PURPOSE
SRV TCP	_tcp	SRV	[RFC2782]	Use of SRV for a TCP-based service
SRV UDP	_udp	SRV	[RFC2782]	Use of SRV for a UDP-based service
SPF	_spf	TXT	[RFC7208]	Authorized IP addresses for sending mail
DKIM	_domainkey	TXT	[RFC6376]	Public key for verifying DKIM signature.
VBR	_vouch	TXT	[RFC5518]	Vouch-by-refererence domain assertion

Table 1: Underscore Global Registry (initial entries)

3.2. DNS Common Second-Level Underscore Scoped Entry Registry

A DNS Common Second-Level Underscore Scoped Entry Registry is for DNS node names that begin with the underscore character (_) and occur immediately below a Global ("top-level") node name beginning with an _underscore.

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

The contents of each entry in the Common, Second-Level registry are defined in Section 2.2.

Initial entries in the registry are:

ID	_NODE NAME	RR	REFERENCE	PURPOSE
LDAP	_ldap	SRV	[RFC2782]	LDAP server
SIP	_sip	NAPTR	[RFC3263] [RFC6011]	Locating SIP Servers and UA configuration
PKI LDAP	_PKIXREP	SRV	[RFC4386]	PKI Repository
DDDS	--???!--	SRV	[RFC3404]	Mapping DDDS query to DNS records
SOAP BEEP	_soap-beep	SRV	[RFC4227]	SOAP over BEEP lookup, when no

				port specified
XMLRPC BEEP	_xmlrpc-beep	SRV	[RFC3529]	Resolve url for XML-RPC using BEEP
Diameter	_diameter	SRV	[RFC6733]	Diameter rendezvous
Tunnel	_tunnel	SRV	[RFC3620]	Finding the appropriate address for tunneling into a particular domain
SLP	_slpda	SRV	[RFC3832]	Discovering desired services in given DNS domains
Msg Track	_mtqp	SRV	[RFC3887]	Assist in determining the path that a particular message has taken through a messaging system
XMPP Client	_xmpp-client	SRV	[RFC6120]	XMPP client lookup of server
XMPP Server	_xmpp-server	SRV	[RFC6120]	XMPP server-server lookup
DDDS SRV	_???	SRV (and NAPTR?)	[RFC3958]	Map domain name, application service name, and application protocol dynamically to target server and port
Kerberos	_kerberos	SRV	[RFC4120]	purpose
PKI	_pkixrep	SRV	[RFC4386]	Enables certificate-using systems to locate PKI repositories
Certificates	_certificates	SRV	[RFC4387]	Obtain certificates

				and certificate revocation lists (CRLs) from PKI repositories
PGP Key Store	_pgpkeys	SRV	[RFC4387]	Obtain certificates and certificate revocation lists (CRLs) from PKI repositories
MSRP Relay Locator	_msrp	SRV	[RFC4976]	purpose
Mobile IPv6 Bootstrap	_mip6	SRV	[RFC5026] [RFC5555]	Bootstrap Mobile IPv6 Home Agent information from non-topological information
Digital Video Broadcasting	_dvbservdsc	SRV	[RFC5328]	Discover non-default DVB entry points addresses
CAPWAP AC	_capwap-control	rrs	[RFC5415]	Discover the CAPWAP AC address(es)
IEEE 802.21 Mobility	_mihis	NAPTR, SRV	[RFC5679]	Discovering servers that provide IEEE 802.21-defined Mobility Services
STUN Client/Server	_stun	SRV	[RFC5389]	Find a STUN server
TURN	_turn	SRV	[RFC5766] [RFC5928]	Control the operation of a relay to bypass NAT
STUN NAT Behavior Discovery	_stun-behavior	SRV	[RFC5780]	Discover the presence and current behavior of NATs and firewalls between the STUN client and

				the STUN server
Sieve Management	_sieve	SRV	[RFC5804]	Manage Sieve scripts on a remote server
AFS VLDB	_afs3-vlserver	SRV	[RFC5864]	Locate services for the AFS distributed file system
AFS PTS	_afs3-prserver	SRV	[RFC5864]	Locate services for the AFS distributed file system
Mail MSA Submission	_submission	SRV	[RFC6186]	Locate email services
IMAP	_imap	SRV	[RFC6186]	Locate email services
POP	_pop3	SRV	[RFC6186]	Locate email services
POP TLS	_pop3s	SRV	[RFC6186]	Locate email services

Table 2: Underscore 2d-Level 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.

[RFC3263] Rosenberg, J. and H. Schulzrinne, "Session Initiation Protocol (SIP): Locating SIP Servers", RFC 3263, June 2002.

[RFC3404] Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part Four: The Uniform Resource Identifiers (URI) Resolution Application", RFC 3404, October 2002.

[RFC3529] Harold, W., "Using Extensible Markup Language-Remote Procedure Calling (XML-RPC) in Blocks Extensible Exchange Protocol (BEEP)", RFC 3529, April 2003.

[RFC3620] New, D., "The TUNNEL Profile", RFC 3620, October 2003.

[RFC3832] Columbia University, Columbia University, Sun Microsystems, IBM, and IBM, "Remote Service Discovery in the Service Location Protocol (SLP) via DNS SRV", RFC 3832, July 2004.

[RFC3887] "Message Tracking Query Protocol", RFC 3887, September 2007.

[RFC3958] Daigle, L. and A. Newton, "Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS)", RFC 3958, January 2005.

[RFC4120] USC-ISI, MIT, MIT, and MIT, "The Kerberos Network Authentication Service (V5)", RFC 4120, July 2005.

[RFC4227] O'Tuathail, E. and M. Rose, "Using the Simple Object Access Protocol (SOAP) in Blocks Extensible Exchange Protocol (BEEP)", RFC 4227, January 2006.

[RFC4386] Boeyen, S. and P. Hallam-Baker, "Internet X.509 Public Key Infrastructure: Repository Locator Service", RFC 4386, February 2006.

[RFC4387] Gutmann, P., Ed., "Internet X.509 Public Key Infrastructure Operational Protocols: Certificate Store Access via HTTP", RFC 4387, February 2006.

[RFC4976] Jennings, C., Mahy, R., and Roach, "Relay Extensions for the Message Session Relay Protocol (MSRP)", RFC 4976, September 2007.

[RFC5026] Giaretta, G., Ed., Kempf, J., and V. Devarapalli, Ed., "Mobile IPv6 Bootstrapping in Split Scenario", RFC 5026, October 2007.

[RFC5328] Adolf, A. and P. MacAvock, "A Uniform Resource Name (URN) Namespace for the Digital Video Broadcasting Project (DVB)", RFC 5328, September 2008.

[RFC5389] Rosenberg, Mahy, Matthews, and Wing, "Session Traversal Utilities for NAT (STUN)", RFC 5389, October 2008.

[RFC5415] Calhoun, P., Ed., Montemurro, M., Ed., and D. Stanley, Ed., "Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification", RFC 5415, March 2009.

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

[RFC5555] Soliman, H., Ed., "Mobile IPv6 Support for Dual Stack Hosts and Routers", RFC 5555, June 2009.

[RFC5679] Bajko, G., "Locating IEEE 802.21 Mobility Services Using DNS", RFC 5679, December 2009.

[RFC5766] Mahy, R., Matthews, P., and J. Rosenberg, "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)", RFC 5766, April 2010.

[RFC5780] MacDonald, D. and B. Lowekamp, "NAT Behavior Discovery Using Session Traversal Utilities for NAT (STUN)", RFC 5780, May 2010.

[RFC5804] Melnikov, A., Ed. and T. Martin, "A Protocol for Remotely Managing Sieve Scripts", RFC 5804, July 2010.

[RFC5864] Allbery, R., "NS SRV Resource Records for AFS", RFC 5864, April 2010.

[RFC5928] Petit-Huguenin, M., "Traversal Using Relays around NAT (TURN) Resolution Mechanism", RFC 5928, August 2010.

[RFC6011] Lawrence, S., Ed. and J. Elwell, "Session Initiation Protocol (SIP) User Agent Configuration", RFC 6011, October 2010.

[RFC6120] Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 6120, March 2011.

[RFC6186] Daboo, C., "Use of SRV Records for Locating Email Submission/Access Services", RFC 6186, March 2011.

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

[RFC6733] Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, "Diameter Base Protocol", RFC 6733, October 2012.

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

[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/