Network Working Group
Internet-Draft
Updates: lots of rfc, to be listed (if approved)
Intended status: Best Current Practice
Expires: May 17, 2016

D. Crocker
Brandenburg InternetWorking

November 14, 2015

DNS Scoped Data Through '_Underscore' Attribute Leaves
draft-crocker-dns-attrleaf-07

Abstract

Historically, any DNS RR may occur for any domain name. Recent additions have defined DNS leaf nodes that contain a reserved node name, beginning with an underscore. The underscore construct is used to define a semantic scope for DNS records that are associated with the parent domain. This specification explores the nature of this DNS usage and defines the "underscore names" registry with IANA.

Table of Contents

1. Introduction

The core 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. 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. Data semantics have been limited to the specification of particular resource records, on the expectation that new ones would be added as needed.

As an alternative to defining new RRs, some DNS service enhancements have specified a restricted scope for the occurrence of particular resource records. That scope is a leaf node, within which the uses of specific resource records can be formally defined and constrained. The leaf has a distinguished naming convention: It uses a reserved DNS node name that begins with an underscore ("_"). Because a "host" domain name is not allowed to use the underscore character, this distinguishes the name from all legal host names.[RFC1035] Effectively, this convention creates a space for attributes that are associated with the parent domain, one level up.

An established example is the SRV record [RFC2782] which generalizes concepts long-used for email routing by the MX record

[RFC0974][RFC2821]. The use of special DNS names has significant benefits and detriments. Some of these are explored in [RFC5507].

[Comment]: The terms "resolution context" and "scoping rules" have been suggested, in place of "semantic scope". In order to avoid concern for matters of semantics, this specification uses the term "scoping rules", to create a focus on the mechanics being defined, rather than nuances of interpretation for the mechanism.

The scoping feature is particularly useful when generalized resource records are used -- notably TXT and SRV. It provides efficient separation of one use of them from another. Absent this separation, an undifferentiated mass of these RRs 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; in some cases the results are ambiguous, because the records do not adequately self-identify. With underscore-based scoping, only the relevant RRs are returned.

This specification discusses the underscore "attribute" enhancement, provides an explicit definition of it, and establishes an IANA registry for the reserved names that begin with underscore. It updates the many existing specifications that have defined underscore names, in order to aggregate the references to a single IANA table.

Discussion Venue: Discussion about this draft is directed to the apps-discuss@ietf.org [1] mailing list.

2. Scaling Benefits and TXT and SRV 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 and SRV records are the notable examples. Used freely, some of these approaches 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, uses an underscore-based name, at a defined place in the DNS tree, so as to constrain to particular uses for particular RRs 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.

In the case of TXT records, different uses have developed largely without coordination. One side-effect is that there is no consistently distinguishable internal syntax for the record; even the inefficiencies of internal inspection might not provide a reliable means of distinguishing among the different uses. Underscore-based names therefore define an administrative way of separating TXT

records that might have different uses, but otherwise would have no syntactic markers for distinguishing among them.

In the case of the SRV RR distinguishing among different types of use was part of the design. [RFC2782] The SRV specification serves as a template, defining an RR that might only be used for specific applications when there is an additional specification. The template definition includes reference to tables of names from which underscore-names should be drawn. The set of <service> names is defined in terms of other IANA tables, namely any table with symbolic names. The other SRV naming field is <proto>, although its pool of names is not explicitly defined.

3. Underscore DNS Registry Function

This specification creates a registry for DNS nodes names that begin with an underscore and are used to define scope of use for specific resource records (RR). A given name defines a specific, constrained context for the use of such records. Within this scope, use of other resource records that are not specified is permitted. The purpose of the Underscore 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 SRV, an underscore name might be multi-part, as a sequence of underscore names. Semantically, this is a hierarchical model and it is theoretically reasonable to allow re-use of an underscore name in different underscore contexts. That is, a subordinate name is meaningful only within the scope of the first (parent) underscore name. As such, they can be ignored by this global Underscore registry. That is, the registry is for the definition of highest-level underscore node name used.

NAME
_service1
_service2._protoB
_service3._protoB
_service3._protoC
_service4._protoD._useX
_protoE._region._authority

Example of Underscore Names

Only the left-most names are registered in the IANA table. Definition and registration of the subordinate names is the responsibility of the specification that creates the highest-level (left-most) registry entry.

4. DNS Underscore Registry Definition

A registry entry contains:

Name: 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.

DNS Label: Specifies a single underscore name that defines a name reservation; 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 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.

5. IANA Considerations

Per [RFC2434], IANA is requested to establish a DNS Underscore Name Registry, for DNS node names that begin with the underscore character (_) and have been specified in any published RFC, or are documented by a specification published by another standards organization. The contents of each entry are defined in Section 4.

Initial entriess in the registry are:

{ Enhancement of this table to include all underscore name reservations in effect at the time this document is published is left as an exercise to the readers... /d }

NAME	LABEL	RR	REFERENCE	PURPOSE

SRV	_srv	SRV	[RFC2782]	SRV template
LDAP	_ldap	SRV	[RFC2782]	LDAP server
SIP	_sip	NAPTR	[RFC3263]	Locating SIP
			[RFC6011]	Servers and UA configuration
SPF	_spf	TXT	[RFC4408]	Authorized IP addresses for sending mail
DKIM	_domainkey	TXT	[RFC4871]	Public key for verifying DKIM signature.
ADSP	_adsp.	TXT	[RFC5617]	Published DKIM usage practices
PKI LDAP	_PKIXREP	SRV	[RFC4386]	PKI Repository
VBR	_vouch	TXT	[RFC5518]	Vouch-by-refererence domain assertion
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	[RFC3588]	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
IM	_im	SRV	[RFC3861]	Instant Messaging address resolution
Pres	_pres	SRV	[RFC3861]	Presence address resolution
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)
IM	_im	SRV	[RFC5509]	For resolving Instant Messaging and Presence services with SIP

Presence	_pres	SRV	[RFC5509]	For resolving Instant Messaging and Presence services with SIP
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 1: DNS Underscore SCOPE Name Registry (with initial values)

6. Related and Updated Registries

This section needs to contained details specification of the updates to existing underscore "registries", in order to have those specifcations point to this new registry.

Numerous specifications have defined their own, independent registries for use of underscore names. It is likely that adoption of the proposed, integrated registry should render these piecemeal registries obsolete

Registries that are candidates for replacement include:

Instant Messaging SRV Protocol Label Registry

Public Key Infrastructure using X.509 (PKIX) Parameters

Presence SRV Protocol Label Registry

7. Security Considerations

This memo raises no security issues.

8. References

8.1. Normative References

[RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", RFC 2434, October 1998.

8.2. References -- Informative

[RFC0974] Partridge, C., "Mail routing and the domain system", RFC 974, January 1986.

[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.

[RFC2821] Klensin, J., "Simple Mail Transfer Protocol", RFC 2821, April 2001.

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

[RFC3404] MMealling, 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.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", September 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", July 2004.

[RFC3861] Peterson, J., "Address Resolution for Instant Messaging and Presence", RFC 3861, August 2004.

[RFC3887] "Message Tracking Query Protocol", 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", February 2006.

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

[RFC4408] Wong, M. and W. Schlitt, "Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1", RFC 4408, April 2006.

[RFC4871] Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and M. Thomas, "DomainKeys Identified Mail (DKIM) Signatures", RFC 4871, May 2007.

[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.

[RFC5507] Faltstrom, P., Ed. and R. Austein, Ed., , RFC 5507, April 2009.

[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, April 2009.

[RFC5518] Hoffman, P., Levine, J., and A. Hathcock, "Vouch By Reference", RFC5 5518, April 2009.

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

[RFC5617] Sendmail, Inc., Cisco Systems, Inc., Yahoo! Inc., and Taughannock Networks, "DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP)", August 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.

8.3. URIs

[1] mailto:we-need-a-list

Appendix A. Acknowledgements

Thanks go to Bill Fenner, Tony Hansen, Peter Koch, Olaf Kolkman, and Andrew Sullivan for diligent review of the earlier drafts. Special thanks to Ray Bellis for nearly 10 years of persistent encouragement to pursue this document.

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/