

Network Working Group
Internet-Draft
Intended status: Informational
Expires: May 1, 2017

T. Hardie
October 28, 2016

Alternative Context Resolution Pointers
draft-hardie-arc-pointers-00

Abstract

In [RFC 2826](#), the IAB set out the benefits of a globally unique public name space. As alternative contexts of resolution emerge, such as those implied by [RFC 7686](#), maintaining a single namespace for the Internet requires a method to indicate the context of resolution for a name. This document proposes a registry for such alternative resolution contexts as well as a set of pointer resource record types useful for allowing conformant resolvers which query for the name in the DNS to be redirected to the appropriate alternative resolution context.

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 <http://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 May 1, 2017.

Copyright Notice

Copyright (c) 2016 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 (<http://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

Internet-Draft

arc-pointers

October 2016

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.

1. Introduction

[RFC 2826](#)[\[RFC2826\]](#) begins "To remain a global network, the Internet requires the existence of a globally unique public name space". At the time it was written, that global name space was expressed almost completely in the DNS, which achieves uniqueness by descent from a single root.

As new naming methods have emerged, the distinction between a DNS name and a name in the Internet name space but not in the DNS has been difficult to draw. The Special Use Names registry [\[RFC6761\]](#) has been used to note some alternative name resolution contexts, for example those used by TOR [\[RFC7686\]](#). This registry is, however, problematic for this use because it permanently links a particular name or label with the resolution method. It is also strongly focused on resolution systems which occupy a place parallel to names in the root zone, creating policy considerations which would not apply to other parts of the Internet name space.

This document proposes a set of mechanisms to address the addition of alternative contexts of resolution, with the intent that this be possible at multiple levels of the Internet namespace.

2. Basic Approach

This document proposes the creation of a registry for alternative resolution contexts which share the Internet's global name space. Entry into this registry will be specification required, with the IESG as the approver of new entries.

This document also proposes the creation of a subdomain under .arpa, arc.arpa. Each label under arc.arpa will have an ARC resource record storing a URN from the IETF protocol parameter registry [\[RFC3553\]](#) that identifies the registry entry for the alternative resolution context. Lastly, this document propose the creation of an ARCPINTER resource recorder.

To indicate that part of the Internet namespace uses an alternative

resolution context, an ARCPINTER resource record is placed at the appropriate label. The ARCPINTER resource record should be the only resource record for that label other than those needed to secure the entry.

A system encountering the name first receives the ARCPINTER resource record, then retrieves the ARC resource record at the domain name to which the ARCPINTER record referred, if it does not have a cached entry. The URN present at the ARC record is used as a stable identifier with which to index the name resolver's capabilities, so that it asks the right resolution system to provide answers for the name. If it has no match for the URN, the resolution fails.

If it does find a match, it resolves the name by presenting the identifier to the alternative resolution system.

This allows alternative resolution contexts to be part of the Internet name space at multiple levels of the hierarchy while still matching the syntax expected by URIs and common Internet protocols like HTTP or SMTP.

[3.](#) Example

Imagine that a provider of names based on cryptographic identifiers, the Allium Identifiers Foundation, wishes to reference these names as part of the Internet namespace. The provider furnishes a specification of how these names are dereferenced to IANA, which asks the IESG to review. Upon approval, a new entry is created in the registry and a URN, urn:iETF:params:arc:allium, is assigned. Concurrently, a new label, allium.arc.arpa, is created and populated with an ARC resource record containing the URN.

If example.com wishes to use Allium identifiers, it can do so by placing an ARCPINTER record at the label in their portion of the Internet name space below which the identifiers will appear. An ARCPINTER record at secid.example.com, for example, means that the Internet name 88917287893.secid.example.com should be interpreted as being the Allium identifier 88917287893, and the Allium resolution context consulted rather than the DNS.

An ARC-aware resolver presented with 8917287893.secid.example.com

will encounter the ARCPINTER record pointing to allium.arc.arpa upon attempting to iteratively resolve secid.example.com within the DNS. It will then use the ARC record present at allium.arc.arpa to retrieve the URN urn:ietf:params:arc:allium. The ARC-aware resolver will then match its local capabilities against that index value (Note that the ARC records at a label under arc.arpa should be highly cacheable, so it should not need to retrieve these often). If it has an allium-capable resolution method available, it will present the identifier in the form required by that resolution method. In this case, it might present 88917287893 to the allium subsystem for resolution. In other cases, the fully qualified Internet name will be presented to the identified alternative resolution system.

[4.](#) A note on Indirection

There is a layer of indirection in this approach that may or may not be needed. It is possible to avoid creating the ARCPINTER resource record and dereferencing labels under arc.arpa entirely, simply by placing ARC records at the same label at which this proposal places ARCPINTER records. This proposal chose this approach in order to ensure that ARC record entries present in the system were drawn from the registered set. For the Internet name space to remain unique in the presence of alternative resolution systems, both elements of the tuple (name, alternative resolution system identifier) must remain unique. This approach is based on the assumption that having a limited set of places to retrieve the identifiers for alternative resolution systems improves the odds that they will not drift over time. Other methods to achieve this, such as configuring ARC-aware resolvers to reject values not beginning with urn:ietf:params:arc, may be equivalent or needed in any case.

[5.](#) Applicability

There is currently no way to assess the number of systems which are using a portion of the Internet namespace without using DNS resolution, and there is, therefore, an unknown risk of collision as the DNS portion of the namespace grows. Providing a mechanism to permit alternative name resolution to be expressed within the DNS at multiple levels of the hierarchy may mitigate this risk, by allowing the name resolution to start at an arbitrary depth.

This approach may also allow for the creation of fairly simple

alternative resolution mechanisms. One potential use case is the variant problem. In that use case, a party controls two different identifiers within the Internet namespace and wishes to have them treated as entirely equivalent, so that a resolution request is indifferent to whether or one or the other is used. Within the DNS, this is very difficult to achieve, requiring tight integration at the registries of every level of the namespace involved. It is, however, a very simple alternative resolution.

Imagine, for example, that a particular party controls both `.colour.example` and `.color.example` and wishes all identifiers using `.color.example` to be mapped to `.colour.example` on resolution. By registering an alternative resolution context and placing the appropriate ARCPINTER and ARC records, that party ensures that any ARC-aware resolver will present names like `blue.ismy.favorite.color` to an alternative resolution context, which knows to query `blue.ismy.favorite.colour` and return the answer there.

The difficulty with using this for variants is that one answer comes from the DNS and one from an alternative resolution context, so it is not truly a bundled DNS name (even if implemented by consulting the DNS after a transformation). Since the alternative resolution mechanism will have a long road to deployment equivalence with the DNS, this is really only useful when one variant is strongly preferred and the other a permitted alternative. Two equally preferred variants would be hard to assign to a resolution system without implicitly assigning a preference.

[6.](#) Indicating support for Alternative Resolution

Indicating supporting for alternative resolution is one of the most difficult problems in constructing a multi-resolution system for Internet names, as deployment of end-to-end extensions to the DNS is very difficult. As an initial proposal, this document suggests nodes test for support by sending an EDNS[RFC6891] Option Code of (TBD). A resolver capable of alternative resolution should include this Option when sending requests, unless it has cached information which indicates the Internet name is within the DNS. A responder which understands the option must include the Option in its reply.

An authoritative server for a zone containing an ARCPINTER record must not send that record in a response to a request from a system that does not speak EDNS or does not include the relevant option. Instead, it should send an NXDOMAIN response for any name covered by the ARCPINTER record. This answers the narrow question: "Is this name in the domain name system?" asked by DNS-only resolvers, rather than the broader question "Is this a known Internet name?" which may be asked by systems aware of alternative resolution mechanism.

If an alternative-aware requester is speaking to a responder that does not speak EDNS or does not include this option in a reply, it must treat an NXDOMAIN response as a partial answer to the broader question above and should cache such an answer only as a narrow response; it should not assume that there is no such Internet name in any context. It should cache NSEC-validated negative answers, however, as a zone maintainer for a zone containing an ARCPINTER would not foster aggressive negative caching for the names covered by an ARCPINTER.

The approach laid out above allows for incremental deployment. It has, however, known failure modes that mean a system aware of alternative resolution systems would likely have to manage uncertainty for a long transition. Sending an ARCPINTER record as additional data to an NXDOMAIN response might be possible, as the semantics of both responses are true, but support for this approach is harder to gauge.

The author invites further discussion of this point.

[7.](#) IANA Considerations

This memo, if approved, asks IANA to set up a registry for resolution methods, populate URN parameters for those methods, as well as to register two new DNS resource record types and an EDNS Option.

It also asks the IAB to create a new subdomain under .arpa, to be named arc.arpa. Registration of a label under arc.arpa will be permitted on creation of a new entry in the registry noted above, with the only permitted resource records being the ARC record along with the records necessary to secure the entry.

[7.1.](#) ARC Resource Record

=====

TODO: Specify syntax which allows the relevant URNs and, if possible, disallows other options.

[7.2.](#) ARCPINTER Resource Record

=====

TODO: Specify syntax which permits a pointer to the relevant name under arc.arpa and, if possible, disallows other pointers.

[7.3.](#) ARC EDNS Option

=====

TODO: Specify syntax.

[8.](#) Security Considerations

This method allows for a different resolution mechanism to replace the standard DNS mechanisms for names in the Internet name space. An attacker capable of redirecting a name into an alternative resolution service will be able to deny name resolution or cause the wrong results to be returned. Because the results must come from a specified alternative resolution service, this does not result in attacker capable of returning completely arbitrary results, but the effect is similar.

[9.](#) Contributors {Contributors}

This document was discussed Warren Kumari, Andrew Sullivan, and Suzanne Wolfe, but all errors are those of the author.

[10.](#) References

[10.1.](#) Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.
- [RFC6891] Damas, J., Graff, M., and P. Vixie, "Extension Mechanisms for DNS (EDNS(0))", STD 75, [RFC 6891](#), DOI 10.17487/RFC6891, April 2013, <<http://www.rfc-editor.org/info/rfc6891>>.

10.2. Informative References

- [RFC2826] Internet Architecture Board, "IAB Technical Comment on the Unique DNS Root", [RFC 2826](#), DOI 10.17487/RFC2826, May 2000, <<http://www.rfc-editor.org/info/rfc2826>>.
- [RFC7686] Appelbaum, J. and A. Muffett, "The ".onion" Special-Use Domain Name", [RFC 7686](#), DOI 10.17487/RFC7686, October 2015, <<http://www.rfc-editor.org/info/rfc7686>>.
- [RFC6761] Cheshire, S. and M. Krochmal, "Special-Use Domain Names", [RFC 6761](#), DOI 10.17487/RFC6761, February 2013, <<http://www.rfc-editor.org/info/rfc6761>>.
- [RFC3553] Mealling, M., Masinter, L., Hardie, T., and G. Klyne, "An IETF URN Sub-namespace for Registered Protocol Parameters", [BCP 73](#), [RFC 3553](#), DOI 10.17487/RFC3553, June 2003, <<http://www.rfc-editor.org/info/rfc3553>>.

Author's Address

Ted Hardie

Email: ted.ietf@gmail.com