dnsext
Internet-Draft
Intended status: Standards Track
Expires: March 17, 2012

D. Barton, Ed.
GridFury, LLC

September 14, 2011

Cloning Domain Name System (DNS) Labels for Fun and Profit
draft-barton-clone-dns-labels-fun-profit-02.txt

Abstract

This document describes a method for making one or more Domain Name System (DNS) labels behave in the DNS "as if" they were actually an entirely different label. E.g., the delegee for the example.org zone could define bar.example.org to be a CLONE of foo.example.org. This method is designed to meet the needs of those managing Internationalized Domain Name (IDN) zones that have been determined to be semantically similar, and therefore should be treated "as if" they were identical. This method can also be used more generally to handle situations where either CNAME or DNAME Resource Records are currently being used.

A key design goal for the CLONE method is that all of the semantic benefits are available by updating only the authoritative servers for the zone. Domain managers who want to support DNSSEC for the CLONEd labels/zones may do so with dynamic signing of the CLONEs, or rely on users being behind a CLONE-Aware resolving name server.

Foreword

[RFC Editor, please remove this Section at publication time. Thanks.]

This is my first draft, please be gentle. :) I'm definitely open to the possibility that there are better ways to accomplish the concepts presented herein. I'm sure that there are a non-zero number of errors in the formatting, references, etc. Also Sections 2 and 3 may be under-specified, unclear, or unworkable. So please don't be afraid to offer (constructive) criticism.

TODO:

- Update/add/improve references?
- Add/improve examples?

Revision History:

1. -00 Initial version

2. -01 Minor textual edits, add support for dynamic signing, clarify CLONE labels that are not zone cuts

3. -02 Bump date to avoid expiry

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

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 March 17, 2012.

Copyright Notice

Table of Contents

1. Introduction

The DNS was initially designed and implemented during a period when the American Standard Code for Information Interchange [ASCII] text was the lingua franca, and certain assumptions about the characteristic behavior of ASCII text, and how it is commonly understood in written form, were baked into the protocol. For example, while the following may not be stylistically appealing on the printed page; not only would all of the following be handled the same by the DNS, there would not be any confusion that all of the following representations refer to the same hostname:

- example.org
- Example.Org
- eXaMpLe.oRg
- EXAMPLE.ORG

Because of the way that Internationalized Domain Names (IDNs) [RFC5890] work it is not possible for the DNS to provide the same level(s) or type(s) of equivalence for different Unicode Code Points that upper and lower case ASCII letters enjoy. Furthermore, there are unique issues with Unicode representations of DNS labels that have no equivalents in ASCII text. More information about the problems that this document attempts to provide a solution for can be found in DNS Resolution of Aliased Names [I-D.ietf-dnsext-aliasing-requirements].

In addition to solving the DNS part of the problem of IDN equivalence, being able to use a more complete solution to the problem of "aliasing" DNS labels than CNAMEs [RFC1035] and DNAMEs [RFC2672] currently provide also has appeal.

1.1. Terminology

There is some feeling in the IDN community that a DNS solution for IDN equivalence must treat (and consider) all versions of a label as truly equal. However this document describes a procedure that relies on one version of a label being configured in the familiar way, and the CLONE(s) configured in a way that refers to the traditionally configured label. Therefore this document will adopt the term used in the Joint Engineering Team (JET) Guidelines [RFC3743] and refer to the label configured in the typical way as the "preferred" label. While on the one hand it is easy to see how a solution that treats all versions of the label as truly equal would be desirable, this document intentionally sacrifices the goal of true equality in the

interest of providing a solution that can get the maximum possible benefit available to the largest number of end users while requiring only that the authoritative name servers are upgraded. It will ultimately be up to the community to decide whether this is a sacrifice worth making.

The terms "authoritative name server" and "resolving name server" are used with their commonly understood meanings. A CLONE-Aware Resolving Name Server will hereinafter be referred to as a CARNS.

1.2. CLONE Overview

1.2.1. Common And Non-DNSSEC Cases

There are two sides of the CLONE method, the authoritative and resolving name servers. For clients that are not aware of the CLONE RR the authoritative server will simply respond "as if" the query for a CLONE label had actually been for the preferred name. When a CARNS queries the authoritative server it will send an EDNS [RFC2671] option that indicates that it is CLONE-Aware. The authoritative server will then add the CLONE Resource Record (RR) to the ANSWER section, which will include the preferred label. From then on when queries come into the CARNS for the CLONE it can in turn query the authoritative server for the preferred label, and respond to its querier "as if" the query had been for the preferred label.

This method also makes it possible to have CLONEs for more than one label at a given level in the DNS.

The CLONES RR is intended to aid application developers by making it easier to know when a given label has one or more other labels that are configured as part of the same "bundle."

1.2.2. DNSSEC

An authoritative server may utilize what is commonly known as "dynamic signing" to handle DNSSEC [RFC4035] signatures for the CLONE labels. Those zone managers who do not wish to (or cannot) utilize the dynamic signing method can rely on the end user being behind a CARNS, which when querying for a CLONE label can perform DNSSEC validation on the preferred version.

2. The Authoritative Name Server

2.1. Parent Zone File

2.1.1. CLONE

At any level of the DNS tree above the root itself ('.') a label MAY be specified as a CLONE. For example:

clone1 CLONE preferred

In this example "preferred" would be the preferred label, "clone1" would be the CLONE. Multiple CLONES MAY be defined for the same preferred label. The RDATA for the CLONE RR MUST be either a valid DNS label, or a valid hostname that is also served by the same authoritative name server. Compliant authoritative server implementations MUST generate a user error when attempting to load a zone that contains a CLONE RR with RDATA that is not served by that authoritative name server.

Other than the DS RR for CLONEs whose preferred label is a zone cut, the CLONE label MUST NOT have any other data associated with it. An authoritative name server above the zone cut (the "parent") MAY allow configuration of a DS record for a label that is a CLONE of the preferred label that is itself the point of the zone cut. For example:

```
preferred NS ns1.preferred

preferred DS 123456789ABCDEF

clone1 CLONE preferred

clone1 DS FEDCBA987654321
```

Compliant authoritative server implementations MUST generate a user error when attempting to load a zone that contains both a CLONE and any other RR (other than DS for a CLONE zone cut) for the same label.

2.1.2. CLONES

The CLONES RR is used to list the preferred label and all of its CLONEs. If the zone does not contain a CLONES RR for the preferred label a compliant authoritative server MUST synthesize one at the time that the zone is loaded. If the CLONES RR is already present in the zone (perhaps because the zone has been signed) the server MUST verify that it is correct. Compliant implementations MUST generate a user error when attempting to load a zone that contains an incorrect CLONES RR.

2.2. Child Authoritative Server Configuration

If the preferred label is a delegation point, and the delegee wishes to answer for the CLONE label(s), the authoritative name server for the child zone with the preferred label MUST be configured for the CLONE(s). An example that uses a BIND-style syntax follows, but this document is not attempting to specify how implementors perform this configuration.

zone "clone1.example.org" { clone preferred.example.org; [dnskey <key>;] };

Behavior of child authoritative servers which configure real zones for labels that the parent created as CLONEs of a preferred label is undefined.

2.3. Query Response For Labels That Are CLONEs

When a compliant authoritative name server implementation receives a query for a label or zone that is a CLONE, the server MUST respond "as if" it had received the query for the preferred label. In the example above if the name server receives any query for clone1.example.org other than the CLONE or CLONES RRs, or as described below the DS or DNSKEY RRs, it MUST respond "as if" the query had been for preferred.example.org.

If the authoritative name server receives the CLONE-Aware EDNS option it MUST add the CLONE RR to the ANSWER section of the query response with the preferred label as the RDATA. This is similar to the behavior when the QNAME is a CNAME and the same server is authoritative for the canonical label. If the DO bit is set in the query the server MUST include the RRSIG(s) for the CLONE RR itself.

2.3.1. DNSSEC For The Parent Of A Zone Cut

When the authoritative server which is the parent at a zone cut answers a query for a CLONE label when the querier sets the DO bit, and the CLONE label has a DS RR, a compliant server MUST return all records "as if" the QNAME had been the preferred label, except for the DS record; and the server MUST return the DS record of the CLONE with the appropriate RRSIGs. This behavior is independent of the presence of the CLONE-Aware EDNS option.

2.3.2. DNSSEC For The Dynamic-Signing Child

For the authoritative server which is the child below a zone cut for the preferred label, when all of the following are true:

- The server is configured to do dynamic DNSSEC signatures
- The query has the DO bit set
- The CLONE has a DNSKEY configured

the compliant implementation MUST return the answer for the CLONE zone "as if" the query had been for the preferred label, except that it MUST return the DNSKEY for the CLONE zone instead of the DNSKEY for the preferred label, and it MUST generate dynamic RRSIGs for all answers, signed with the CLONE's DNSKEY. This behavior is independent of the presence of the CLONE-Aware EDNS option.

2.3.3. DNSSEC For Other Authoritative Servers

If the conditions in 2.3.1 or 2.3.2 are not met an authoritative server which receives a query which does not include the CLONE-Aware EDNS option MUST NOT return DNSSEC-related records along with the response, regardless of whether the DO bit was set in the query. If the server receives both the DO bit and the CLONE-Aware EDNS option it MUST return the DNSSEC records for the answer "as if" the QNAME were the preferred label.

The behavior described in this Section is relevant whether or not the preferred label is a zone cut.

2.4. Query Response For CLONE And CLONES Resource Records

When a compliant authoritative name server receives a query for the CLONE RR with a label that is a CLONE as the QNAME it MUST return an ANSWER with the preferred label as the RDATA. When a compliant server receives a CLONE query for a label that is not a CLONE it MUST return RCODE 0 (No error).

When a compliant server receives a query for the CLONES RR with a label that is a CLONE or a preferred label as the QNAME it MUST return an ANSWER with the preferred label listed first in the RDATA, followed by all of the labels that are configured as a CLONE of the preferred label. If the label in the QNAME is neither a preferred label nor a CLONE the server MUST return RCODE 0 (No error).

3. The CLONE-Aware Resolving Name Server

When sending queries a compliant CARNS MUST send the EDNS option for CLONE-Aware. When a compliant CARNS receives a query response which contains a CLONE RR as described in Section 2.3 it MUST "transform" future queries for hostnames or labels which it knows contain CLONE

labels to the preferred version(s). However regardless of whether the CARNS knows that a hostname it is queried for contains a CLONE label or not, the response to its client MUST be for the same QNAME it was queried for.

3.1. CARNS DNSSEC Behavior For "Typical" Queries

When a CARNS receives a response to a query that originally contained one or more CLONE labels that is signed with DNSSEC it MAY indicate that the response is authentic by setting the AD bit if all other conditions for setting it are otherwise met (i.e., the DO bit was set in the query originally received by the CARNS, etc.). Local policy SHALL be the determining factor for whether to set the AD bit in the query response for the hostname which contains one or more CLONE labels if it were otherwise appropriate to do so.

3.2. CARNS Behavior for DNSSEC Resource Record Queries

When a CARNS receives a direct query for a DNSSEC-related RR for a hostname that contains one or more CLONE labels (e.g., RRSIG, DNSKEY, etc.), and those RRs are not configured as described in Sections 2.3.1 and 2.3.2, it MUST return RCODE 0 (No answer) and include the CLONE RR with the preferred label as RDATA in the ADDITIONAL section of the response

4. Examples

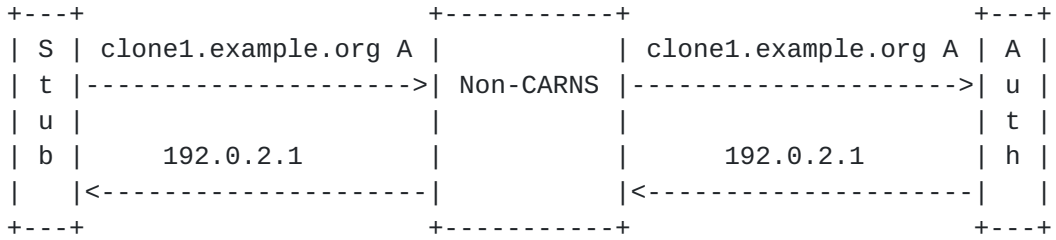
Assuming a zone example.org with the following records:

preferred A 192.0.2.1

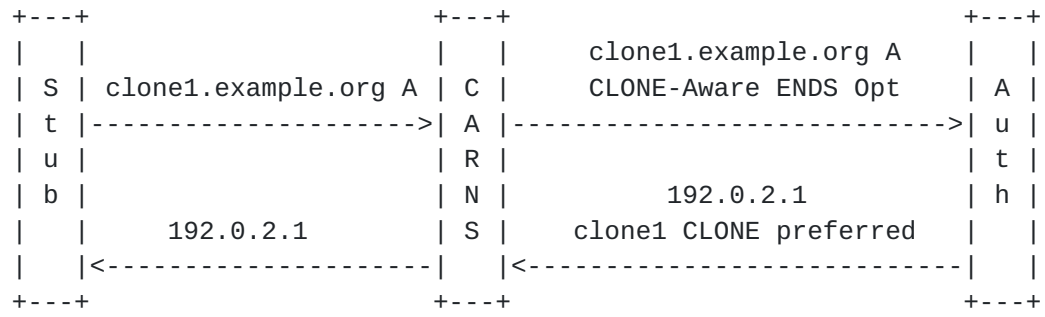
clone1 CLONE preferred

clone2 CLONE preferred

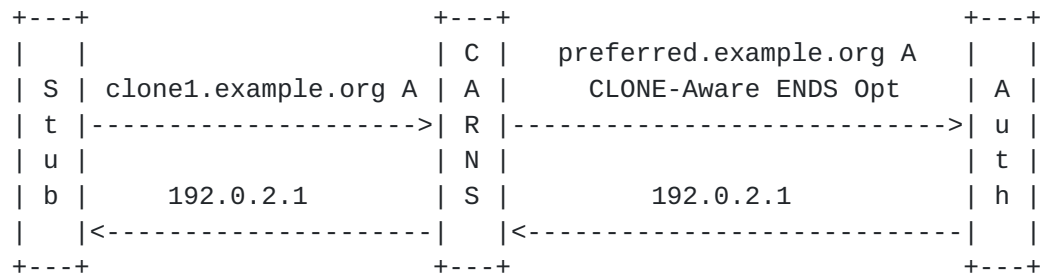
4.1. Non-CARNS



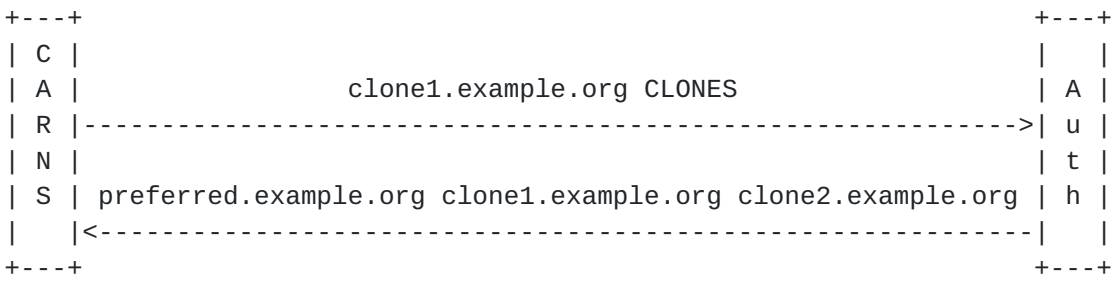
4.2. CARNS - First Query For CLONE



4.3. CARNS - Second Query For CLONE



4.4. CLONES Response



5. IANA Considerations

This document requests that the IANA assign the Resource Record (RR) Type Codes [RFC1035], [I-D.ietf-dnsext-5395bis] 77 and 88 to the CLONE and CLONES RRs, respectively; and the EDNS0 Option [RFC2671] 11 for CLONE-Aware.

6. Security Considerations

There are currently (at least) two widely used solutions to the equivalence problem at the zone level. For both of these solutions the preferred label and all of the variations need to be delegated,

usually to the same set of name servers. The obvious, albeit potentially the most difficult method of keeping the zones "the same" is to create multiple zone files that contain records that are identical to the extent possible. This solution allows for the possibility of having DNSKEY records for each zone, thereby allowing each label's zone to be signed.

The other solution that takes advantage of identical delegation is to use the exact same "generic" zone file for multiple zones. This method provides for DNSSEC configuration in the typical way for the preferred label, but does not allow different DNSKEY records for the other labels in the same "bundle." The records in the preferred version of the zone can be signed, but validation would fail for the other labels since the DNSKEY record would not be for that zone. This behavior is similar to the CLONE solution in the absence of both dynamic signing at the authoritative level and a validating CARNS.

For parents (such as TLD registries) that allow the delegee/ registrant to choose what method of "bundling" semantically similar labels to use, the techniques described in this document do not reduce security in any way. The delegee can either decide as a matter of local policy that the DNSSEC capability of the CLONE technique is sufficient, or they can choose to have the non-preferred versions of the label delegated and maintain separate zone files. In a context where the delegee is required to accept the CLONE option DNSSEC validation for the non-preferred versions of the label can be provided without relying on end users being behind a CARNS by utilizing dynamic signing.

No negative security implications for the CLONE or CLONES RRs themselves are known, other than the possibility that the CLONES RR could be used as a Distributed Denial Of Service amplifier if it contained a sufficiently large ANSWER section. It is envisioned that in certain contexts being able to verify that the non-preferred versions of a label have been listed as CLONEs rather than using some other method of "aliasing" (such as delegation, CNAME, etc.) could be beneficial.

7. Acknowledgements

I would like to thank all of the participants in the dnsext and dnsop working groups who discussed and fleshed out the ideas this document is responding to. Particularly Suzanne Woolf and Xiaodong LEE for producing the Problem Statement [I-D.ietf-dnsext-aliasing-requirements] that this document is trying to provide a solution for; both for their diligent work on the topic, and for making it much simpler for me to write my Introduction. I

would also like to thank Nicholas Weaver for pushing me hard to think about how dynamic DNSSEC could fit into the CLONE idea.

8. References

8.1. Normative References

[I-D.ietf-dnsext-5395bis]
3rd, D., "Domain Name System (DNS) IANA Considerations", draft-ietf-dnsext-5395bis-03 (work in progress), January 2011.

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

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2671] Vixie, P., "Extension Mechanisms for DNS (EDNS0)", RFC 2671, August 1999.

[RFC2672] Crawford, M., "Non-Terminal DNS Name Redirection", RFC 2672, August 1999.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

[RFC5890] Klensin, J., "Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework", RFC 5890, August 2010.

8.2. Informative References

[ASCII] American National Standards Institute (formerly United States of America Standards Institute), "USA Code for Information Interchange", ANSI X3.4-1968, 1968.

[I-D.ietf-dnsext-aliasing-requirements]
Woolf, S. and X. Lee, "Problem Statement: DNS Resolution of Aliased Names", draft-ietf-dnsext-aliasing-requirements-00 (work in progress), February 2011.

[RFC3743] Konishi, K., Huang, K., Qian, H., and Y. Ko, "Joint Engineering Team (JET) Guidelines for Internationalized Domain Names (IDN) Registration and Administration for

Chinese, Japanese, and Korean", RFC 3743, April 2004.

Author's Address

Douglas Barton (editor)
GridFury, LLC
11901 Santa Monica Boulevard, Unit 612
Los Angeles, CA 90025
USA

Email: dougb@dougbarton.us