Network Working Group	S. Woolf	
Internet-Draft	Internet Systems Consortium, Inc.	
Intended status: Informational	J. Yao	
Expires: April 28, 2011	X. Lee	
	CNNIC	
	October 25, 2010	

TOC

Problem Statement: DNS Resolution of Aliased Names
draft-yao-dnsext-identical-resolution-02.txt

Abstract

This document attempts to describe a set of issues that arises from the desire to treat a set or group of names as "aliases" of each other, "bundled," "variants," or "the same," which is problematic in terms of corresponding behavior for DNS labels.
With the emergence of internationalized domain names, among other potential use cases, two or more names that users will regard as having identical meaning will sometimes require corresponding behavior in the DNS. It's not clear how to accommodate these requirements for behavior of such names in DNS resolution; in particular, it's not clear when they are best accommodated in registry practices for generating names for lookup in the DNS, existing DNS protocol elements and behavior, or some set of protocol elements or behavior not yet defined. This document attempts to describe some of these cases and the behavior of some of the possible solutions discussed to date.
NOTE: Even more than usual, version -02 of this document is a "work in progress". Additional updates may be expected between the date of this document and the DNSEXT meeting in Beijing, and can be found at http://users.isc.org/~woolf.

Status of this Memo

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 April 28, 2011.

Table of Contents

---

1. Introduction

TOC

As the Internet and the DNS have evolved beyond their original realms of use, a set of needs and expectations has appeared about how DNS labels behave that is informed significantly by common human assumptions about how "names" or "words" work. One aspect of this is the notion or expectation that multiple sets of names may be similar to a human user, and expected to behave "the same" or as "aliases" of one another. The DNS was designed with the implicit expectation that names would be based on ASCII characters, and the "similarity" or "sameness" property doesn't seem to arise terribly often in the names people originally wanted to use in the DNS; thus the requirements of identical resolution of "aliased" or "bundled" names hasn't figured prominently as an attribute that needed to be accommodated in the generation or lookup of DNS names. However, with the standardization of internationalized domain names protocols (ref: IDNA and IDNAbis), more and more internationalized domain name labels [RFC3490] (Faltstrom, P., Hoffman, P., and A. Costello, “Internationalizing Domain Names in Applications (IDNA),” March 2003.) are appearing in DNS zones. In some cases, these labels [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,” April 2004.) are accompanied by the expectation that they are "equivalent" or should behave "the same," often because these labels are derived from names or strings that users consider "the same" in some languages. Accordingly, Internet users hope for such labels to behave in DNS contexts as they expect the corresponding human constructs to behave.

The general issues of what "the same" means, or of defining "variants" in human scripts as codified in Unicode (or anywhere else) are well outside the scope of the DNS or the expertise of most of the people who work on it. They are matters for philosophers and applications developers, respectively. However, to the extent that these issues can be specified as involving the resolution of names in the DNS, it's

reasonable to describe those expectations and attempt to accomodate them.

There is some existing technology defined in the DNS for behavior that can be described as one name behaving "the same" as another. For a single node in the DNS tree, CNAME can be used to map one name as an "alias" to another, "canonical" name. If there is a need to map a subtree of the DNS-- a zone, or a domain and its subdomains-- to another domain, DNAME has been defined to allow this behavior. However, there is no way currently defined to do both, as CNAME is required to be the record at its node in the tree. Behavior that combines their characteristics is not currently defined in the DNS.

If existing protocol does not meet the zone administrator's need to be able to treat one label, name, or zone as "the same" as another, there are also administrative mechanisms available for manipulating databases underlying the generation and resolution of DNS names. Registry operators have many mechanisms for working around DNS protocol in order to get behavior they want for names in DNS zones, and management of "aliases" is no exception. However, it is not clear how much of the user and operator requirements for "aliases" can be met by mechanisms for provisioning DNS zones, at acceptable cost. Concerns have been raised about this approach particularly at large scales.

1.1. What this document does

TOC

Attempts to think about "aliases" or similar concepts as applied to the DNS have been difficult, both because use cases have been unclear and because terminology for describing and distinguishing them has not been readily available. This document attempts to provide both brief descriptions of identified use cases, and a rough organization for how to think about behavior in the DNS that might correspond to the requirements derived from them as a way of evaluating proposed solutions. This includes existing and additional possible solutions.

As a departure point, we attempt to be rigorous about distinguishing DNS "labels" from "words" (a human construct) and "strings" (which we use here as machine-readable constructs that nonetheless may not conform to DNS label constraints, such as IDNA U-labels).

We also review existing constructs (CNAME, DNAME) and proposed new ones ("BNAME," "zone clones").

1.2. What this document does not do

TOC

This document makes no attempt to solve or even describe "translation" of one name into another in the DNS, which is likely to be impossible. "Translation" in general, or even the particular problem of determining

when or why two DNS labels (or even FQDNs) should be considered "the same", are simply not in scope for the DNS protocol. We pre-suppose those decisions are made elsewhere and that the DNS needs to deliver behavior in conformance with that external decision.
Accordingly, this document makes no comment on policy regarding when two names are "the same," what restrictions should be placed on their generation or use outside those imposed by the DNS protocol, or the ability of one approach over another to instantiate what a given user regards as "the same" for a language, script, culture, or community.

1.3. Terminology

TOC

All the basic terms used in this specification are defined in the documents [RFC1034] (Mockapetris, P., “Domain names - concepts and facilities,” November 1987.), [RFC1035] (Mockapetris, P., “Domain names - implementation and specification,” November 1987.), [RFC2672] (Crawford, M., “Non-Terminal DNS Name Redirection,” August 1999.) and [RFC3490] (Faltstrom, P., Hoffman, P., and A. Costello, “Internationalizing Domain Names in Applications (IDNA),” March 2003.).
We also note that there is a wide variety of terminology in use to describe the issues we attempt to treat in this document, and no consensus on which apply under what conditions. Terms for "a set of domain names that somehow need to be treated as similar" include "bundle," "variants," or "clones". As uniformity of terms is one of the goals of any work on this topic in the DNS, we try not to add to the confusion in the problem statement but can't claim to have finalized a recommendation in early versions of this document.

---

2. Problem Statement

TOC

From the point of view of the DNS, a number of attributes suggest themselves as important dimensions for evaluating what "the same" might mean.
One question is exactly what it is that's to be defined as "the same"? Are the end results to be identical, and if so from what perspective: that of the recursive resolver? The application? The human consumer of content? Is it enough that lookups on the FQDN portion of an email address result in the same A or AAAA records, or does some intermediate mapping need to be maintained between MX records in the resolution chain? What about the FQDN portion of a URL handed back to an application, or in resolution processes that include multiple lookups of records that may include FQDNs? Do there need to be general rules specified for the handling of FQDNs in RDATA of present and future RRtypes?

Another question is the behavior of multiple names with respect to one another: is it enough to define one as "canonical" or "preferred," with the others considered as "variants" that are transformed to the "preferred" form? Or is there a real need for multiple names to be "equivalent", interchangeable, with none considered "preferred" over the others? (We note here that no requirement for complete interchangeability or identity has been articulated, except anecdotally, and such equivalence would be extremely difficult to define in the DNS.)

In addition, the tree structure of the DNS requires that we consider the behavior of "identical" names across multiple zones in the hierarchy. Are mappings to be maintained in names more than a level, or two, deep? If so, with what characteristics, and what characteristics are required for scalability?

A further question arises with respect to how applications should interact with alias-specific DNS behavior. A basic requirement would seem to be "First, do no harm," or in other words, any extensions to DNS protocol in support of the desired "alias" behavior should not interfere with applications that expect to do such interpretation on their own. This concern is based in the expectation that DNS is simple and predictable, operating strictly as infrastructure under the process of creating "the user experience," not as part of it.

2.1. Registration of Domain Name Variants

TOC

The introduction of IDN has provided a forcing function for defining how "variants" might behave as DNS names. It's generally conceded that recognition and careful management of cases where multiple names are associated together as "variants" in the expectation or preference of users are important; without such management of grouped domain names, security risks may be increased and the quality of user experience may be compromised. [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,” April 2004.) developed by JET (Joint Engineering Team) gives one possible solution of how to manage registration of a domain name, intended to be applied to the script and usage common across Chinese, Japanese, and Korean users. [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,” April 2004.) proposed an algorithm which will allocate a group of names, consisting of a domain name and its variants, to the same domain holder. It means that the domain holder will get control of the domain name and its variants. [RFC4290] (Klensin, J., “Suggested Practices for Registration of Internationalized Domain Names (IDN),” December 2005.) suggests the

practice in [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," April 2004.) to be used in registrations of internationalized domain names. But [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," April 2004.) and [RFC4290] (Klensin, J., "Suggested Practices for Registration of Internationalized Domain Names (IDN)," December 2005.) do not define how, exactly, these bundles of names are to be treated by the registry or the DNS in order to obtain the desired "identical" behavior. [RFC4690] (Klensin, J., Faltstrom, P., Karp, C., and IAB, "Review and Recommendations for Internationalized Domain Names (IDNs)," September 2006.) said that the "variant" model introduced in [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," April 2004.) and [RFC4290] (Klensin, J., "Suggested Practices for Registration of Internationalized Domain Names (IDN)," December 2005.) can be used by a registry to prevent the most negative consequences of possible confusion, by ensuring either that both names are registered to the same party in a given domain or that one of them is completely prohibited. The principles described in [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," April 2004.), [RFC4290] (Klensin, J., "Suggested Practices for Registration of Internationalized Domain Names (IDN)," December 2005.) and [RFC4690] (Klensin, J., Faltstrom, P., Karp, C., and IAB, "Review and Recommendations for Internationalized Domain Names (IDNs)," September 2006.) have been accepted by many registries. But the technical details of how to guarantee that a bundle of domain names are "identical" in the DNS remain unspecified.

2.2. Identical DNS Resolution for Bundled DNS Names

TOC

To some extent, the desired behavior can be described: "identical DNS resolution" means that the process of resolving two domain names will end with the same result, in most cases the same IP address. In the history of DNS protocol development, there have been two attempts to specify such "identical resolution" behavior:CNAME[RFC1034] (Mockapetris, P., "Domain names - concepts and facilities," November 1987.) which maps or redirects itself, and DNAME[RFC2672] (Crawford, M., "Non-Terminal DNS Name Redirection," August 1999.) which maps or redirects its descendants. In the case of bundles or groups of

names, however, some operators have asserted they need identical DNS resolution at all levels' domain names, including the domain name itself and its descendants. As alluded to above, registries are left with ad hoc provisioning and database management mechanisms for managing variant names, with some help from existing DNS protocol mechanisms for mapping labels or FQDNs to each other. However, some are finding the existing mechanisms to have unsatisfactory limitations; they are seeking more guidance on the use of existing mechanisms, and perhaps the addition of new ones in the DNS protocol.

2.3. Character Variants

TOC

Many defined scripts as used in many different languages have "character variants" included. There is no uniform definition of variants, and in fact their characteristics differ widely, but it's possible to define some. For example, the definition of variant characters in the JET Guidelines [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,” April 2004.), intended for use with the CJK language/script communities, is roughly this: One conceptual character can be identified with several different Code Points in character sets for computer use. In UNICODE definitions of some scripts, including Han (chinese), some characters can be identified as "compatibility variants" of another character, which usually implies that the first can be remapped to the second without the loss of any meaning. In this document, variant characters are two or more characters that may be similar in appearance or identical in meaning (similarity in appearance is not required by the definition but often occurs).
With the introduction of IDNs in the DNS, perhaps most prominently in the root zone, decisions about how to deal with IDN variants is a significant challenge ahead of us. We describe here a couple of examples, Chinese and Greek; [STW: ....and additional cases (Arabic, Cyrillic, etc.)should be described in future versions by experts in those scripts and languages].

2.3.1. An example: Simplified and Traditional Chinese

TOC

For example, if the IDN TLD "China"(U+4E2D U+56FD) and its variant (U+4E2D U+570B) are put into the root, the first one (U+4E2D U+56FD) can be considered the "original" IDN TLD and the second one (U+4E2D U+570B) can be considered the IDN TLD "variant". Ideally, it should be possible to treat the original IDN TLD and its IDN TLD variant as

"identical" for purposes of DNS resolution, in a way similar to the case mapping most DNS users take for granted, in which the uppercase "A" is the variant of lowercase "a". For example, the string ".COM" can be considered a variant of ".com", and the corresponding DNS labels are treated as identical. However, for the historical reasons already discussed, and technical reasons having to do with the underpinnings of the IDNAbis protocol (ref: IDNAbis rationale), there's no generalization of the "case" mapping available for situations where it might be useful for IDNs. In addition, it's perilous because DNS rules around "case insensitivity" and "case preservation" are not intuitively consistent.
At this writing, four Chinese script IDN TLDs are in the root, including two pairs comprising a Traditional Chinese name and its Simplified counterpart, which should allow future versions of this document to include those operators' experience of managing maintenance of those names as "the same."

2.3.2. An example: Greek

TOC

In Greek, almost every word has the "tonos" accent sign, but where it is placed (on which character) can vary. Further, some words end in a final sigma, which is represented differently to sigma appearing elsewhere in the word. If a registry wishes to be able to enforce the association among all of the domain names that correspond to a "word" in Greek, with all its possible Unicode strings, some mechanism must be used to enumerate the "variant" names and tie them together. This makes sense from the human factors perspective, as depending on how the user types something, results may include a different domain to what was expected, although the user may have the firm belief that "the same word" was input in multiple cases.
As an example, the domain names "xn--0xadhj4a.gr" and "xn--0xaafjl.gr" appear to a native speaker/reader of Greek to represent "the same word," in a sense very much like the case insensitivity that native users of Latin script take for granted in the DNS.

2.3.3. An Example: Arabic

TOC

[STW: [to be added]

TOC

3. Possible Solutions

Currently, there are several possible mechanisms to support identical DNS resolution of "bundled" or "variant" names as "aliases" in the DNS. Existing mechanisms in the DNS include CNAME and DNAME. In addition, as described briefly above, registry operators have a great many techniques for applying policy to what names can be registered, and provisioning technology to how they are instantiated in the DNS, in support of keeping "variant" names behaving similarly to each other, or in preventing the use of such variants as might be considered confusing or dangerous.

In addition, there are new proposals for DNS protocol to support "aliases" in the DNS as part of the desired behavior of "variant" names: Names direction[BNAME] (Yao, J., Lee, X., and P. Vixie, “Bundle DNS Name Redirection,” 12 2009.), and "Zone clone".

All of the solutions have their advantages and disadvantages. In particular, there are a couple of limitations they all share. Every mechanism existing or proposed to support "aliases" in the DNS requires that one name be designated as the "canonical" name ("preferred" in the terminology of the JET variant mechanism) and any others bundled with it are to be considered "variants" or "aliases". The only known way to enforce a symmetrical or equivalent association is via careful registry provisioning within and across domains. In addition, the different "alias" mechanisms differ in subtle ways that have to be carefully reviewed against the desired behavior of the DNS in support of different types of "variants".

3.1. Mapping or Redirection of Domain Names

TOC

3.1.1. Mapping itself

TOC

It was recognized as part of the original specification of the DNS that a host can have many names; in fact this expectation predates the DNS, referring to the earlier specification of host names. In the simplest case for "aliases", Internet users need these multiple names to be resolved to the same IP address by a DNS server. The CNAME record [RFC1034] (Mockapetris, P., “Domain names - concepts and facilities,” November 1987.), where "CNAME" is an abbreviation for "Canonical Name", is a way to designate aliases of the "real" or canonical name of a host. In some cases, CNAME can be used to produce the necessary association a bundle of variant domain names. But the CNAME only maps itself, not its descendants; in fact it is defined to not have descendants, as it is the only name at a node in the DNS tree and can't

exist at the same name as delegation. In the case of IDN variants, however, it is often desirable that the name map both itself and its descendants.

3.1.2. Mapping its descendants

TOC

In order to maintain the address-to-name mappings in a context of network renumbering, a DNAME record or Delegation Name record defined by [RFC2672] (Crawford, M., “Non-Terminal DNS Name Redirection,” August 1999.) was invented to create an alias for all its subdomains. In contrast, the CNAME record creates an alias only of a single name (and not of its subdomains). As with the CNAME record, the DNS lookup will continue by retrying the lookup with the new name. If a DNS resolver sends a query without EDNS[EDNS0] (Vixie, P., “Extension Mechanisms for DNS (EDNS0),” August 1999.), or with EDNS version 0, then a name server synthesizes a CNAME record to simulate the semantics of the DNAME record. A DNAME record is very much like the CNAME record, but while the CNAME record only applies for one name, with a DNAME record one can create aliases for all the records for its subdomain.

3.1.3. Mapping itself and its descendants

TOC

Bundling of "variant" strings or names as domain names, possibly along with other use cases not yet identified, require the ability to map a whole tree of the domain space to another domain. The current DNS protocols do not support this function. A new DNS resource record [BNAME] (Yao, J., Lee, X., and P. Vixie, “Bundle DNS Name Redirection,” 12 2009.) has been proposed to deal with this problem.
The advantage of BNAME is that it would enable a class of "aliasing" behavior that some operators find desirable, particularly in preference to some of the provisioning overhead they describe having to deploy to support potentially large numbers of "bundles" of variants at multiple levels of the DNS tree. The disadvantage is that it may not provide the behavior people really want while requiring the time and resources to code and deploy any new DNS facility.
Alternatively, a proposal has been made that would leave CNAME as already specified, but eliminating the constraint that a CNAME must be alone at a node in the DNS tree. This would avoid any coding and deployment overhead associated with new RRtypes, while obtaining the desired behavior. Concerns expressed about it, however, include the possible (but not yet specified) effort required for backwards compatibility to avoid harm to implementations that expect, and use, the old behavior.

3.2. Zone Clone

TOC

The proposal of "zone clone" or "dns shadow", is an alternative solution for a higher level of support than the DNS currently provides for "alias" behavior across zones. In this scheme, a new RRtype, SHADOW, is specified; it can exist at a zone apex and can be used to define "clones" or "shadows" of the zone content so that records in the zone are reachable via lookups from multiple delegations. This mechanism varies fundamentally from CNAME/DNAME/BNAME in that it creates a local copy on each cooperating authoritative server that has the original zone, reachable by the names specified in the SHADOW RR. Its scope, then, is the zone as maintained by an authoritative server rather than a single RRset (even one corresponding to a delegation). This scheme has the advantage that it allows a SHADOW zone to be used in all the same contexts as the canonical or underlying zone, including contexts where a CNAME or DNAME (or, presumably, a BNAME) cannot appear, such as in the RDATA of certain RRtypes. Of the proposed DNS protocol mechanisms, it probably comes closest to the behavior some have requested as "equivalence," where none of the bundled or SHADOW names is canonical or preferred over the others. It does implicate an unknown level of effort to implement and support.

4. IANA Considerations

TOC

There are no obvious IANA considerations in this memo; we reiterate that the determination of which names are to be considered "the same" is explicitly out of scope.

5. Security Considerations

TOC

[STW: Looking for examples for this section.]
Unsolved issues that will have to be considered in the definition of what "the same" means for the DNS include the implications for DNSSEC, and whether "identical" resolution includes DNSSEC validation in the expected "identical" behavior.
Another area of possible peril includes SSL certificates, "Host" headers as seen by web servers, and other security-relevant data often associated with domain names. It will have to be considered whether, and how, the "sameness" property maps into the expected behavior of security-related protocols that use domain names, particularly given that it's unlikely that all operators will ever use the same set of constructs (whether in the DNS or elsewhere) to signal whether

different "names" are "the same" for purposes of the function of a particular application or protocol.
In addition, there is a large cluster of security risks at the user and application levels that motivate significant portions of the interest in what it means to treat a set of names as "aliases" of each other. One set of issues is around the expectation that two strings are seen as "different" by the user in some obvious way (such as visually) but need to be treated as "the same". The potential for user confusion and subversion is not hard to imagine in cases where two visually distinct strings are nonetheless likely to be expected by the user to behave "the same" in some functional way. This is the case we have attempted to address here.
There is a separate but complementary set of issues that arise around cases where strings that look "the same" should nonetheless be treated as different-- the so-called "confusing visual similarity" problem. The easy example is substituting the Unicode codepoint for a character in one script, or a string of them, for the Unicode codepoints for similar-looking characters in an altogether different script. This has a different set of potential risks to users, and has not been discussed here. It's often closely related to the "alias" issue we have attempted to deal with, however, which poses risks of its own to analysis of the either subject.

---

6. Acknowledgements

TOC

Most of the ideas here and much of the text is taken from discussions on the DNSEXT and DNSOP WG mailing lists. Particular help is acknowledged from the authors of the proposed solutions drafts, and from the many contributors to the IDNAbis work and its underpinnings. Special thanks at the intersection of DNS and IDNAbis is owed to Patrik Faltstrom, Cary Karp, John Klensin, Vaggelis Segredakis, and Andrew Sullivan for their patient explanations.

---

7. Change History

TOC

[anchor20] (RFC Editor: Please remove this section.)

7.1. draft-yao-dnsext-identical-resolution: Version 00

TOC

*Domain Name Identical Resolution Problem Statement (initial attempt)

7.2. draft-yao-dnsext-identical-resolution: Version 01

TOC

*Expanded introduction

*Added Greek example

*Added some detail to descriptions of proposed solutions

8. References

TOC

8.1. Normative References

TOC

[ASCII]	American National Standards Institute (formerly United States of America Standards Institute), “USA Code for Information Interchange,” ANSI X3.4-1968, 1968.
[EDNS0]	Vixie, P., “Extension Mechanisms for DNS (EDNS0),” RFC 2671, August 1999 (TXT).
[RFC1034]	Mockapetris, P., “Domain names - concepts and facilities,” STD 13, RFC 1034, November 1987 (TXT).
[RFC1035]	Mockapetris, P., “Domain names - implementation and specification,” STD 13, RFC 1035, November 1987 (TXT).
[RFC2119]	Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC2136]	Vixie, P., Thomson, S., Rekhter, Y., and J. Bound, “Dynamic Updates in the Domain Name System (DNS UPDATE),” RFC 2136, April 1997 (TXT, HTML, XML).
[RFC2672]	Crawford, M., “Non-Terminal DNS Name Redirection,” RFC 2672, August 1999 (TXT).
[RFC3490]	Faltstrom, P., Hoffman, P., and A. Costello, “Internationalizing Domain Names in Applications (IDNA),” RFC 3490, March 2003 (TXT).
[RFC3597]	Gustafsson, A., “Handling of Unknown DNS Resource Record (RR) Types,” RFC 3597, September 2003 (TXT).
[RFC3629]	Yergeau, F., “UTF-8, a transformation format of ISO 10646,” RFC 3629, November 2003 (TXT).
[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 (TXT).
[RFC4033]	Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “DNS Security Introduction and Requirements,” RFC 4033, March 2005 (TXT).
[RFC4034]	Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “Resource Records for the DNS Security Extensions,” RFC 4034, March 2005 (TXT).
[RFC4035]	Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “Protocol Modifications for the DNS Security Extensions,” RFC 4035, March 2005 (TXT).
[RFC4290]	Klensin, J., “Suggested Practices for Registration of Internationalized Domain Names (IDN),” RFC 4290, December 2005 (TXT).
[RFC4690]	Klensin, J., Faltstrom, P., Karp, C., and IAB, “Review and Recommendations for Internationalized Domain Names (IDNs),” RFC 4690, September 2006 (TXT).

8.2. Informative References

TOC

[BNAME]	Yao, J., Lee, X., and P. Vixie, "Bundle DNS Name Redirection," draft-yao-dnsext-bname-01.txt (work in progress), 12 2009 (TXT).
[CNAME-DNAME]	Sury, O., "CNAME+DNAME Name Redirection," draft-sury-dnsext-cname-dname-00.txt (work in progress), 4 2010 (TXT).
[IDN-TLD-Variants]	Yao, J. and X. Lee, "IDN TLD Variants Implementation Guideline," draft-yao-dnsop-idntld-implementation-01.txt (work in progress), 11 2009 (TXT).
[RFC2672bis]	Rose, S. and W. Wijngaards, "Update to DNAME Redirection in the DNS," Internet-Draft ietf-dnsext-rfc2672bis-dname-17.txt, 6 2009.
[SHADOW]	Vixie, P., "Use of DNS to Carry Configuration Metadata Concerning Automatic Replication of Zones," draft-vixie-dnsext-dnsshadow-00.txt (work in progress), 2 2010 (TXT).

Authors' Addresses

TOC

	Suzanne Woolf
	Internet Systems Consortium, Inc.
	950 Charter St.
	Redwood City, CA 94063
Phone:	+1 650 423 1333
Email:	woolf@isc.org
	Jiankang YAO
	CNNIC
	No.4 South 4th Street, Zhongguancun
	Beijing
Phone:	+86 10 58813007
Email:	yaojk@cnnic.cn
	Xiaodong LEE
	CNNIC
	No.4 South 4th Street, Zhongguancun
	Beijing
Phone:	+86 10 58813020
Email:	lee@cnnic.cn