Network Working Group J. Yao
Internet-Draft X. Lee
Intended status: Informational CNNIC
Expires: April 25, 2010 October 22, 2009

IDN TLD Variants Implementation Guideline
draft-yao-dnsop-idntld-implementation-01.txt

Status of this Memo

Copyright Notice

Abstract

ICANN is pushing the IDN TLD into the root server. Some IDN TLD has the variants. Currently, there are two proposals to implement the IDN TLD variants in the root servers:1, implement it with the DNAME record; 2, implement it with NS record. The IDN TLD variants may be reserved or activated. If the IDN TLD variants are activated, these variants will be allocated to the same TLD manager in order to avoid the possible phishing problems. How to deal with the IDN TLD variant issue is a big challenge ahead of us. This document discusses the IDN TLD variants implementation issues related with DNAME and NS resource record way. This memo also gives a proposal about how to avoid the possible phishing problem after putting the IDN TLD variants into the root.

Table of Contents

1. Introduction

ICANN is pushing the IDN TLD into the root server. Some IDN TLD has the variants. Currently, there are two proposals to implement the IDN TLD variants in the root servers:1, implement it with the DNAME record; 2, implement it with NS record. The IDN TLD variants may be reserved or activated. If IDN TLD variants are activated, these variants will be allocated to the same TLD manager in order to avoid the possible phishing problems. How to deal with the IDN TLD variant issue is a big challenge ahead of us. This document discusses the IDN TLD implementation issues related with DNAME and NS resource record way. This memo also gives a proposal about how to avoid the possible phishing problem after putting the IDN TLD variants into the root.

1.1. Terminology

All the basic terms used in this specification are defined in the documents [RFC1034], [RFC1035], [RFC2672], [RFC3490] and [RFC3743]. Understanding of the [RFC2672] and [RFC3743] is necessary to understand this document. In particular, the term "variant" is defined in section 1.3.2 of [RFC4290]. the "normal domain name" is the domain name which can be configured with the DNS Resource Record directly.

2. IDN TLD Variant

In ASCII [ASCII] letters, the upper case "A" and lower case 'a' are same in the meaning. In many cases, the upper case "A" and lower case 'a' are exchangeable. We can regard the upper case "A" as the variant of the lower case 'a'. In some languages, some characters has the variants, which look differently or very similar but are identical in the meaning. For example, Chinese character U+56FD and its variant U+570B look differently, but are identical in the meaning. If Internationalized Domain Label" or "IDL" [RFC3743] are composed of variant characters, we regard this kind of IDL as the IDL variant. If these IDL variants are put into the root, they are regarded as the IDN TLD variants. For example, if the IDL "China" (U+4E2D U+56FD) and its IDL variant (U+4E2D U+570B) are put into the root, the first one (U+4E2D U+56FD) is called as the original IDN TLD and the second one (U+4E2D U+570B) is called as the IDN TLD variant. In ideal way, the original IDN TLD and its IDN TLD variant SHOULD be identical in the DNS resolution. For example, the ".com" is identical to ".COM" in the DNS resolution. Currently, we can not find the ideal solution for the IDN TLD variants. Two proposals are suggested to solve the problem: DNAME record and NS record.

3. The principle of IDN TLD variants implementation

Two principle of IDN TLD variants implementation are:

- Same DNS resolution to the names under the original IDN TLD and its variants
- the same names under the original IDN TLD and its variants belong to the same registrant

Any policy or technology SHOULD be used to guarantee that the IDN TLD and its variant SHOULD belong to the same registry; the DNS administrators SHOULD try their best to make the IDN TLD and its variants be identical in the DNS resolution. There have 2 ways to deal with it. In technique, the DNS operators may use some technology to implement it; In policy, the DNS administrators can use some management policy or some guideline to make the original IDN TLD and its variants be identical in the DNS resolution. If the IDN TLD and its variants are delegated to different registry, it will cause phishing problems. In order to avoid the possible phishing, these IDN TLDs SHOULD be delegated to the same registry. Based on the current technology, there are two techniques: DNAME and NS records which can be used in the IDN TLD variants implementation. The following section will discuss the usage of DNAME and NS resource records, and its relative policy to manage the IDN TLD and its variants.

4. IDN TLD variants implementation guideline

4.1. The requirement of the root server operation

[RFC2870] points out that the resolution of domain names on the internet is critically dependent on the proper, safe, and secure operation of the root domain name servers while the root domain name servers are seen as a crucial part of the correct, safe, reliable, and secure operation of the internet infrastructure. The Internet Corporation for Assigned Names and Numbers (ICANN) are responsible for making the total system performance, robustness, and reliability in the root name servers. So the root server should guarantee that the server can run as stable as possible. Any change or update to the root servers should be done in caution.

4.2. Apply DNAME to IDN TLD variants in the root

A DNAME record is defined in [RFC2672]. The main function of the DNAME is to provide the redirection from a part of the DNS name tree to another part of the DNS name tree. The following two characters of DNAME can be considered to be two good arguments to support DNAME to be applied to the IDN TLD variants in the root.

- o redirection the whole sub-tree of the domain name tree to another one
- o DNAME does not direct itself (the owner name).

We can use the following configuration form:

< the IDN TLD variants > TTL IN DNAME < its original one >

If this model can be workable, DNAME can be considered as the simplest mechanism to make the DNS resolution of the names in the original IDN TLD and its variants to be same or identical. For the IDN TLD operators, only one ZONE is needed to be kept instead of multiple zones for the IDN TLD variants. The root helps the direction of the DNS resolution of the IDN TLD variants to the original IDN TLD. This method makes the DNS resolution of the original IDN TLD and its variants to be identical via the root solution. If DNAME is put into the root, some issues should be considered. The following section will discuss these issues.

4.2.1. DNAME issues

4.2.1.1. DNAME is a new technology

The basic DNS documents [RFC1034] and [RFC1035] were defined in the year of 1987 while the DNAME [RFC2672] was defined in the year of 1999. There are 12 years gap between them. So there are a lot of legacy DNS applications which are unaware of DNAME. Some interesting things may happen if DNAME is used.

4.2.1.2. Zero TTL

The section 4.1 of [RFC2672] specifies that the synthesized CNAME RR, if provided, MUST have TTL equal to zero. It means that the DNAME-unaware resolver will not cache this resource record. The DNAME-unaware resolver will go to other servers to lookup the relative answers every time when the DNAME record is involved. This will cause much load to the servers which provide the DNAME service. The [RFC2672bis] has updated it to " A CNAME RR with TTL equal to the corresponding DNAME RR is synthesized and included in the answer section for resolvers that did not indicate understanding of DNAME in queries." In the current implementation based on [RFC2672], the TTL for synthesized CNAME Resource record is 0, which means there will be no cache in the resolvers. So every query from DNAME-unaware resolvers has to go to the DNS servers which provide the DNAME service. This will cause a big load to the DNAME DNS servers.

4.2.1.3. Mis-configuration

DNAME RFC specifies that resource records MUST NOT exist at any sub-domain of the owner of a DNAME RR. Some DNS administrators may not know it and still configure the RR in the sub-domain of the owner of a DNAME RR, which may lead the failure resolving. The DNAMEed domain name is not a normal domain name. The normal domain name itself can be configured with the DNS resource record such as A or MX record. Many DNS administrators will mis-configure it. The registrant of this domain name may not understand the DNAME and regard the DNAMEed domain name as the normal domain name.

4.2.2. DNAME should be scrutinized before being put into the root

If the DNAME is put into the root for the IDN TLD variants, the synthesized CNAME RR for the DNAME has the TTL Zero according to [RFC2672], which will cause too much load to the root servers since many DNAME-unaware resolvers will not cache the synthesized CNAME RR for the DNAME and lookup the messages from the root when they receive the requests related to DNAME. The easy mis-configuration problem by the DNS administrator is also a problem to make the DNS administrators and the registrant be confused about the domain name availability. Whether the issues discussed above will make the root server running unreliable or unstable is unclear. So the ICANN should scrutinize all the DNAME issues and consider whether these will impact the stable running of the internet before deciding to put the DNAME into the root.

4.3. Apply NS to IDN TLD variants in the root

4.3.1. NS issues

The NS record is defined in the basic DNS documents [RFC1034] and [RFC1035]. NS resource record is deployed widely. The practice in the root has proven that the NS resource record in the root is safe and reliable. Putting the NS records in the root does not impact the root much. If the IDN TLD variants are delegated via the NS resource record way, the original IDN TLD and its variants can be delegated to totally different servers. In the DNS zone, they are the different delegation. In registration policy, the original IDN TLD and its IDN TLD variants SHOULD be allocated to the same registry.

4.3.2. Apply DNAME or NS to the second level names in the IDN TLD variants

If the NS resources records are used in the root for the IDN TLD variants, some technology combined with some policy should be applied. Whether DNAME or NS is used for the second level names in

the IDN TLD and its variants, the DNS administrator can consider the three factors:

- Are IDN TLD variants often used or resolved by the internet users?
- IDN TLD DNS servers' performance?
- The DNS administrators' knowledge of DNAME?

4.3.2.1. Apply DNAME to the second level names in the IDN TLD variants

If some of the following criterias are satisfied, we can consider to use the DNAME in the second level domain names.

- The names in the IDN TLD variants are seldom used or resolved by the internet users
- The DNS servers' performance is good enough to support a lot of resolution from the DNAME-unaware resolvers
- The DNS administrator has the knowledge of DNAME, and can configure it properly

There are two ways to apply DNAME to the second level names in the IDN TLD variants zone.

**Apply DNAME to all names

We can use the following configuration form in the zone apex of the IDN TLD variants:

<the IDN TLD variants> TTL IN DNAME <its original one>

**Apply DNAME to the name which the registrant wants to be DNAMEed

We can use the following configuration form in the zone of the IDN TLD variants:

<names in the IDN TLD variants> TTL IN DNAME <names in its original one>

If the second method is used, the other resource records except NS DNAME records under the IDN TLD variants SHOULD be same with the original IDN TLD in the DNS administration since the owner of DNAME does not redirect itself.

4.3.2.2. Apply NS to the second level names in the IDN TLD variants

If some of the following criterias are satisfied, we can consider to use the NS in the second level domain names.

- The IDN TLD variants are often used or resolved by the internet users
- The DNS servers' performance is not good enough to support a lot of resolution from the DNAME-unaware resolvers

- The DNS administrator has not the knowledge of DNAME, and can not configure it properly

The same name under the original IDN TLD and its variants should belong to the same registrant via some policy. In order to avoid the possible phishing or confusing, the configuration of names under the original IDN TLD and its variants SHOULD be same in the DNS administration. That is that any parameters or configuration applied to the names of the original IDN TLD SHOULD be available to the names of its variants. This can guarantee that the resolutions in the IDN TLD and its variants are identical.

5. IANA Considerations

There is no IANA consideration.

6. Security Considerations

If IDN TLD variants are implemented, this guideline is suggested to be used to avoid the possible phishing. If we apply NS to the second level names in the IDN TLD variants, we can not guarantee that every level of domain names under the IDN TLD and its variants are configured to be same. We can only specify some policy to make the same name under the IDN TLD and its variants to be owned by the same registrant. The registrant is unlikely to phishing itself via the name under the IDN TLD and its variants.

7. Acknowledgements

Some ideas are discussed in the ICANN IDN variant working group. Some nice comments are from Harald Alvestrand in this group. Thanks a lot to Sun Guonian for his helpful discussion with me about DNAME technology. The authors thanks the following experts for the kind comments and suggestions to this draft: Andrew Sullivan, Paul Hoffman, Alfred Hones and more.

8. Change History

[[anchor19: RFC Editor: Please remove this section.]]

8.1. draft-yao-dnsop-idntld-implementation: Version 00

- IDN TLD variants implementation guidelines

8.2. draft-yao-dnsop-idntld-implementation: Version 01

- o adjust the sections arrangement
- o change the category from BCP to INFO
- o refine some contents based on the comments from DNSOP and DNSEXT mailing list

9. References

9.1. Normative References

[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.

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

[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.

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

[RFC2870] Bush, R., Karrenberg, D., Kosters, M., and R. Plzak, "Root Name Server Operational Requirements", BCP 40, RFC 2870, June 2000.

[RFC3490] Faltstrom, P., Hoffman, P., and A. Costello, "Internationalizing Domain Names in Applications (IDNA)", RFC 3490, March 2003.

[RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", RFC 3629, November 2003.

[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.

[RFC4290] Klensin, J., "Suggested Practices for Registration of

Internationalized Domain Names (IDN)", RFC 4290, December 2005.

9.2. Informative References

[RFC2672bis]
Rose, S. and W. Wijngaards, "Update to DNAME Redirection in the DNS", Internet-Draft ietf-dnsext-rfc2672bis-dname-17.txt, 6 2009.

Authors' Addresses

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