IDN TLD Variants Implementation Guideline

draft-yao-dnsop-idntld-implementation-01.txt

Yao Jiankang

中国互联网络信息中心
CHINA INTERNET NETWORK INFORMATION CENTER

IDN TLD Variants Problem

- ICANN is pushing the IDN TLD into the root server.
- ICANN Seoul meeting has approved the IDN ccTLD fast track.
- In 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'.
- Many non-ASCII languages or scripts have some variant characters. (国 VS 國)

- If Internationalized Domain Label" or "IDL" 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”中国(U+4E2D U+56FD) and its IDL variant中國(U+4E2D U+570B) are put into the root, the first one中国is called as the original IDN TLD and the second one中國 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.

The Security Concern of IDN TLD Variants

usabank.com VS usabank.COM

.中国 VS .中國

bank.中国 VS bank.中國

bank.中国 A 192.168.1.1

bank.中國 A 192.168.252.252

- GOOD: bank.中国 and bank.中國 belongs to the same registrant and gets the same DNS resolution
- Not bad: bank.中国 VS bank.中國 belongs to the same registrants and gets the different DNS resolution
- Danger: bank.中国 VS bank.中國 belongs to the different registrants and gets the different DNS resolution

The principle of IDN TLD variants implementation

- Same or identical 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.

The requirement of the root server operation

- [RFC2870] points out that the root domain name servers are seen as a crucial part of the correct, safe, reliable, and secure operation of the internet infrastructure.
- The root server should run as stable as possible.
- Any change or update to the root servers should be done in caution.

IDN TLD Variants Implementation Guideline

- 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.
- Some relative policy should also be used to manage the IDN TLD and its variants.

Apply DNAME to IDN TLD variants in the root

- Configuration form:

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

- Advantages:
  - ✓ Redirection the whole sub-tree of the domain name tree to another one
  - ✓ DNAME does not direct itself (the owner name).
- There are also some other issues related to the IDN TLD

中国互联网络信息中心
CHINA INTERNET NETWORK INFORMATION CENTER

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.
- There are a lot of legacy DNS applications which are unaware of DNAME.

Zero TTL

- [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 the DNAME 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.

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.

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.
- 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

Apply NS to IDN TLD variants in the root

- 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 delegations.
- In registration policy, the original IDN TLD and its IDN TLD variants SHOULD be allocated to the same registry.

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

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?

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

- **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 this 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.

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.
  - ✓ The DNS administrator is supposed to have 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.

Security Considerations

- If IDN TLD variants are implemented, this guideline is suggested to be used to avoid the possible phishing.
- If we apply NS both to IDN TLD variants in the root and 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.

中国互联网络信息中心
CHINA INTERNET NETWORK INFORMATION CENTER

Q&A

yaojk@cnnic.cn
Jiankang YAO

中国和谐信息社会重要的基础设施建设者、运行者和管理者

北京市海淀区中关村南四街四号中科院软件园　　邮编: 100190

www.cnnic.cn