A Method for Identifying the Administrative Boundaries of DNS Names

draft-yao-dbound-identify-dns-boundary-01

Jiankang Yao
CNNIC
IETF 124 in Montreal

Motivation

Two or more DNS names belonging to the same registrants may share the same DNS administrative boundaries.

- V-label.TLD (IDN issues)
  - different labels ending with the same TLD
    - 清华大学 .cn == 清華大学 .cn

- LABEL.V-tld (New gTLD issues)
  - same label ending with different TLDs
    - example. 中国 == example. 中國
    - . 中国 == . 中國

Currently, there are no good methods to identify such shared administrative boundaries in DNS.

History

- The main idea of this draft was discussed in the IETF dbound WG in 2015.
- ✓ The WG which focused on developing a specification to represent differing administrative control between "related" DNS names (such as example.com and foo.example.com).
- ✓ https://datatracker.ietf.org/wg/dbound/about/
- ✓ This WG closed without producing any RFCs.

- Domain Boundaries (dbound2) BoF in IETF 116 in 2023
- ✓ The BoF concluded with creating a WG

Problems

- Two or more DNS names may have the same administrative boundaries. If they share the same DNS administrative boundaries, we regard that they have a relationship. Otherwise they have not a relationship.
- This document describes a method for using dbound resource record for judging domain name administrative boundaries.
- DNS currently lacks a standardized method to identify administrative boundaries between domain names owned by the same entity.
- While multiple domains may belong to the same registrant, DNS does not natively express these relationships.

New gTLD Variants

- As the ICANN new gTLD program has expanded, registrants frequently obtain multiple domain names serving a common purpose. Consequently, there is a need to develop a mechanism for determining when two or more domain names share administrative boundaries.

✓ variant1 and varant2 share the same administrative boundaries.

Framework

- A mechanism to lookup of the administrative boundary between two domains. The mechanism defines a new resource record type (RRTYPE) called as Dbound to satisfy the requirements specified in the previous section. The RDATA for an Dbound RR consists of a 1 octet Flag field, a 1 octet Reserved 1 field, a 1 octet Reserved 2 field, and a Anchor Name / Name Collection field.

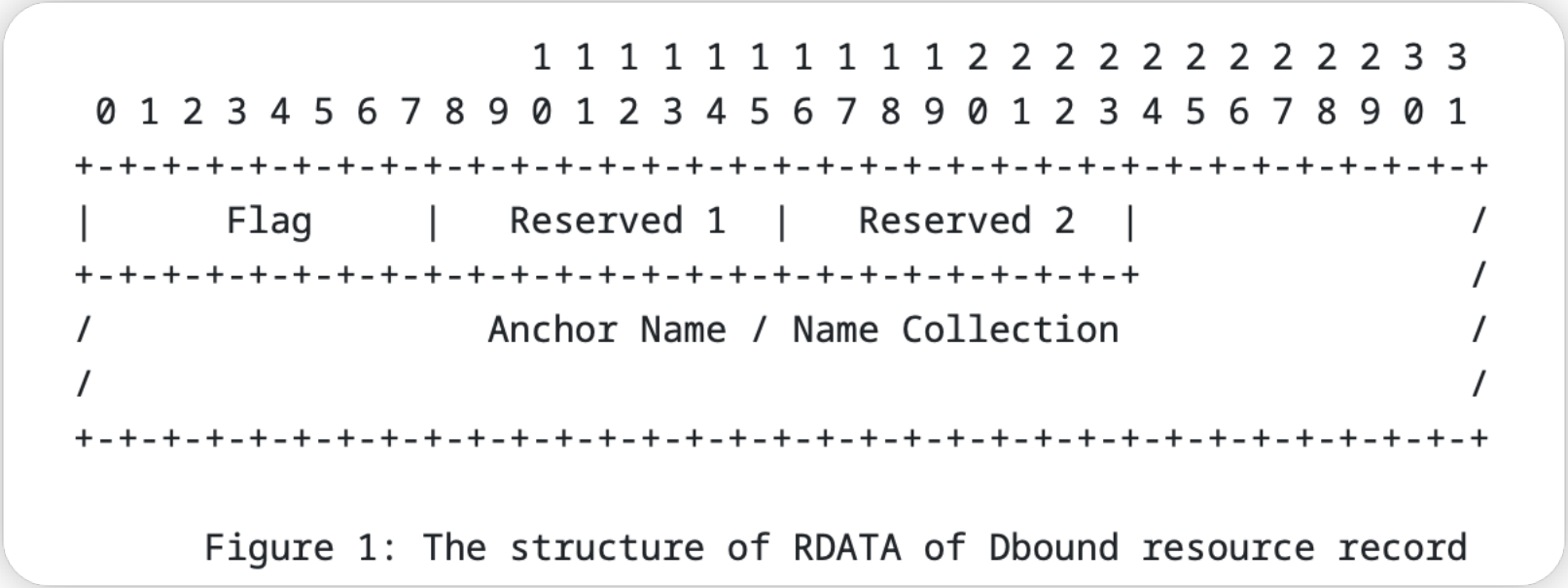


Figure 1: The structure of RDATA of Dbound resource record

Flag: The Flag field identifies the usage of Anchor Name / Name Collection field.

• If flag=0, the Anchor Name / Name Collection is the anchor name, and the anchor name will be the string of PSL.

•If flag=1, the Anchor Name / Name Collection is the anchor name, and it means that dbound record is to try to build a connection between the owner name and the anchor name which is a FQDN.

• If flag=2, the Anchor Name / Name Collection is the name collection, and the Name Collection will be a collection of names which are supposed to share the same DNS boundaries under the same anchor name and will be separated by comma(,). The owner name is some names' anchor name in other dbound RR.

Application Algorithm for Dbound Query

- Given two domain names A and B , there are two cases where application can determine whether domain names A and B share the same administrative boundaries.
- Case 1: If A and B's flag value in the dbound record are 0, application should confirm that the Anchor Name / Name Collection fields of both names have the value of PSL.
- Case 2: If A and B's flag value in the dbound record are 1, application should check whether the names point to the same anchor

Algorithm :
1)When the application needs to know whether two names A and B share the same administrative boundary, it needs to do the following steps to confirm it.

Step 1, the application sends the query of A for dbound record to the DNS servers, and analyzes the response. If the application gets the dbound RR for A, it checks whether there is a dbound record with the flag value of 0 or 1. If the value of flag of A's dbound records is 0, go to step 2; If the value of flag of A's dbound records is 1, go to step 3; Otherwise, go to step 4;

Step 2, the application sends the query of B for dbound record to the DNS servers, and analyzes the response. If the application gets the dbound RR, it checks this RR. If the value of flag of B's dbound records is 0, check whether the value of anchor name of A and B's dbound records are PSL. If yes, it means that A and B tend to enjoy the same administrative boundaries under the PSL. Then check the PSL to confirm whether A and B enjoy the same administrative boundaries. If yes, return the response and exit. Otherwise go to step 4

Step 3, the application sends the query of B for dbound record to the DNS servers, and analyzes the response. If the application gets the dbound RR, it checks this RR. If the value of flag of B's dbound records is 1, check whether the value of anchor name of A and B's dbound records are same. If yes, it means that A and B tend to enjoy the same administrative boundaries under the same anchor name. Then check the anchor name to confirm whether A and B enjoy the same administrative boundaries. That means If yes, the application should send the query of the anchor name for dbound record to the DNS servers, and analyzes the response. If the application gets the dbound RR, it checks this RR. If the value of flag of anchor's dbound records is 2, check whether the dbound record's value include A and B in its name collection. If yes, ten return the response and exit. Otherwise go to step 4

step 4, Exit and display some error information

- 2)Given name A, the application queries the DNS servers for the dbound record of name A and processes the response. If a dbound RR for A is retrieved, and if the flag value of A's dbound record is 1, the application checks for the presence of a dbound record with flag value 2 associated with A's anchor name. Upon such a record being found, the application extracts the name collection from this dbound record to obtain the list of names. For each name in this list, the application uses the procedure specified in Algorithm 1) (for the case of two domain names A and B) to verify whether it shares the same administrative boundary as A.
- 3） Given more than two names, check whether they share the same administrative boundaries. The application selects one of the names as A and check whether every other name shares the same administrative boundaries with A via the the method 1) which describes the case of two domain names A and B.

EXAMPLE 1,
Configuration: if a.example and b.exmaple want to share the same DNS administrative boundaries, it can configure the following RRs:

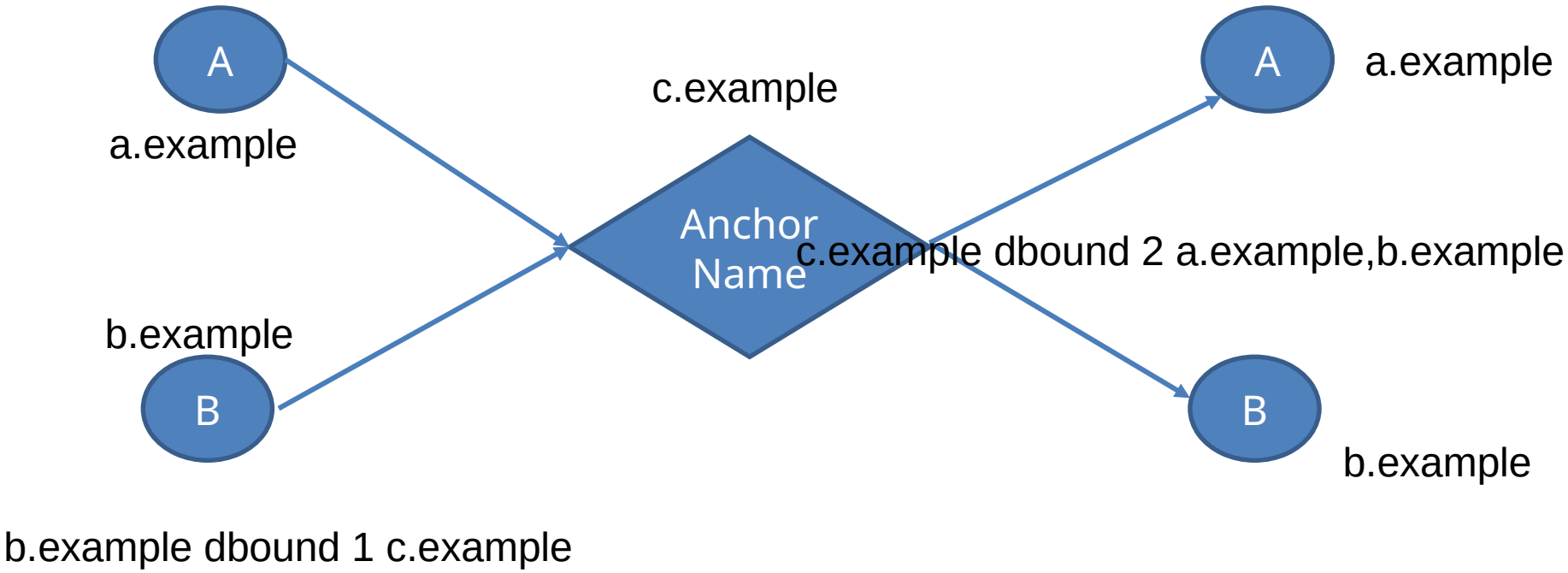
a.example dbound 1 c.example
b.example dbound 1 c.example
c.example dbound 2 a.example,b.example

or the anchor name can also be one of the names who share the same DNS administrative boundaries:
a.example dbound 1 b.exmaple
b.example dbound 1 b.example
b.example dbound 2 a.example,b.example

USAGE: if the application wants to check whether a.example and b.example share the same DNS boundaries, it finds a.example and b.example share the same anchor under the flag's value of 1 under the RRs above, and verify that a.example and b.example share the same DNS boundaries.

if the application wants to check which domain names share the same DNS boundaries with a.example, it finds a.example and b.example are supposed to have the same DNS boundaries under the flag's value of 2, and verify that a.example and b.example share the same DNS boundaries through checking a.example and b.example sharing the same anchor under the flag's value of 1 .

a.example dbound 1 c.example



EXAMPLE 2,
Configuration: if a.example and b.exmaple want to share the same DNS administrative boundaries under PSL, it can configure the following RRs:
a.example dbound 0 http://mxr.mozilla.org/mozilla-central/source/netwerk/dns/ effective_tld_names.dat?raw=1
b.example dbound 0 http://mxr.mozilla.org/mozilla-central/source/netwerk/dns/ effective_tld_names.dat?raw=1

USAGE: if the application wants to check whether a.example and b.example share the same dns boundaries, it finds a.example and b.example share the same anchor under the flag's value of 0, and verify that a.example and b.example share the same dns boundaries via the PSL link.

This new mechanism builds a relationship through the anchor name (middleman) to avoid to construct too many pairwise relationship. It will help to reduce the RRs configuration and checking when there are many domain names which are supposed to share the administrative boundaries.

Question

- New RRTYPE is expensive. Instead of applying to use dbound RRTYPE, Use “_dbound_ “ as the prefix for txt record?

- Continue the current Stream?