draft-yao-dbound-dns-solution-01

yaojk@cnnic.cn

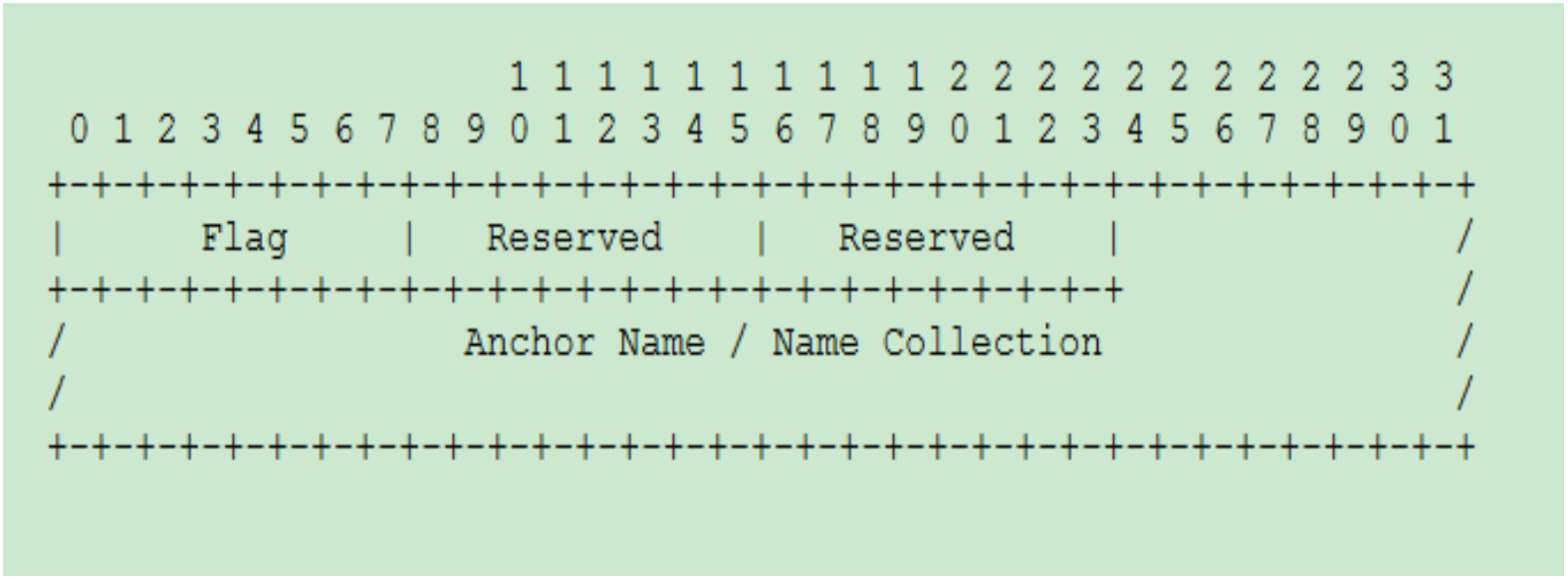
IETF 94

Requirements or Use cases

- Given 2 domain names: A and B, the application can check whether A and B enjoy the same administrative boundaries
- Given multiple domain names A, B, C, D…, the application can check whether these domain names enjoy the same administrative boundaries
- Given a single domain name A, the application can find out what domain names share the same administrative boundaries with this single domain name A. (Application do not know B, C, D beforehand)
- Also try to satisfy the use cases in problem statements documents of the WG

- After discussing in the WG list, I propose the following solution (see more in section 6.1 of draft-yao-dbound-dns-solution-01)

The structure of RDATA of Dbound resource record



- The main idea is to add an anchor name (middleman or middle domain name). Those domain names which are supposed to share the same dns administrative boundaries will point to the same anchor name (FQDN) with the flag's value of 1; Those domain names which are supposed to share the same dns administrative boundaries through PSL will point to the PSL link with the flag's value of 0; The anchor name can point to name collections which are supposed to share the same DNS administrative boundaries with the flag's value of 2.

Mechanism

- If flag=0, the Anchor Name / Name Collection is the anchor name, the anchor name will be the string of PSL. Through it, the DNS administrators can configure the relationship between the owner name and PSL. Those which point to the PSL will share the same DNS administrative boundaries;

  A--→PSL

  B--→PSL

- If flag=1, the Anchor Name / Name Collection is the anchor name, it means that dbound record is to try to build a connection between the owner name and the anchor name which is a FQDN. Through it, the DNS administrators can configure the relationship between the owner name and the anchor name. Those which share the same anchor name will share the same DNS administrative boundaries;

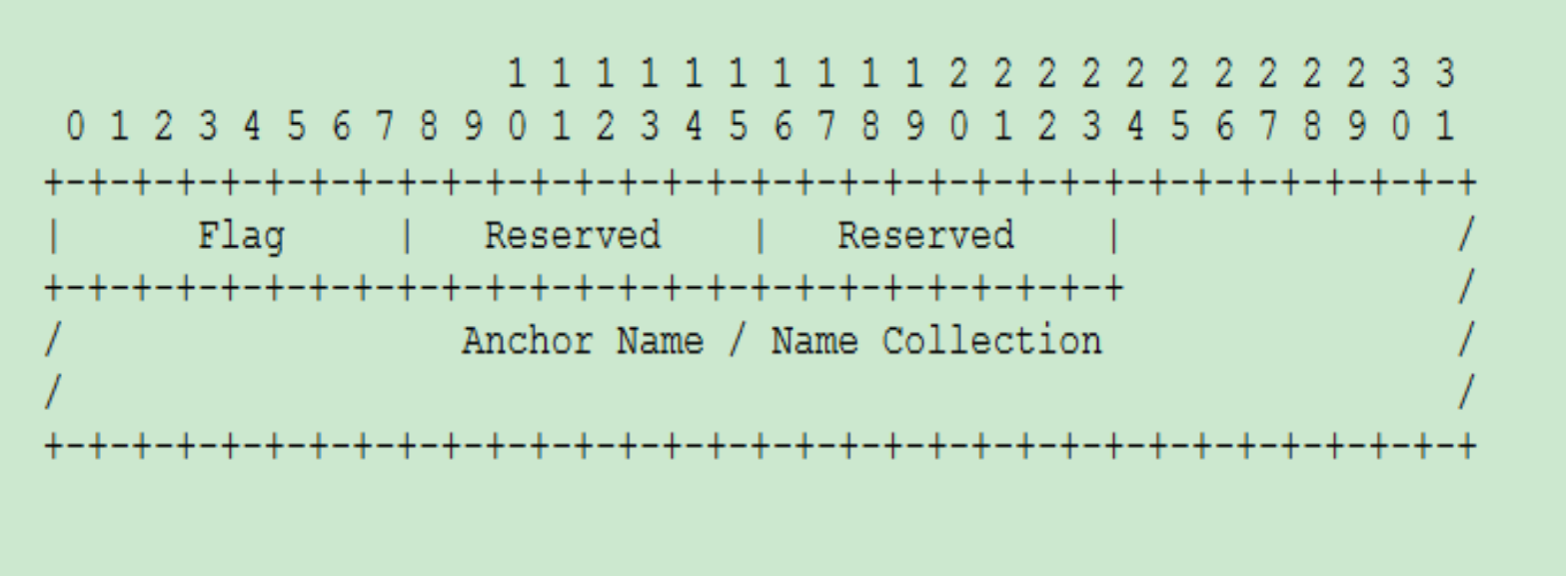
  A--→Anchor Name

  B--→Anchor Name

Mechanism

- If flag=2, the Anchor Name / Name Collection is the name collection, 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. Through it, the application can learn how many names share the same DNS boundaries under the owner name (some names' anchor name in other dbound RRs)

Anchor Name--→ Name Collection (for example, A , B)



EXAMPLE 1

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 find 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 find 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

EXAMPLE 2

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 find 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.

- Is this solution suitable for problems raised by John Levin? (My answer is yes)
  * the browser cookie problem
  * the CA name/wildcard problem
  * the DMARC organizational domain problem

EXAMPLE 3 (wildcard)

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

- a.example dbound 1 a.example
- *.a.example dbound 1 a.example
- a.example dbound 2 a.example, *.a.example

b.b.a.example VS a.example

*.b.c.a.example VS c.a.example

……

- Any comments to this proposed solution?
- Is this proposed solution suitable for all the main use cases?

Q&A