DELEG, un changement radical de la délégation DNS (1/16)

Stéphane Bortzmeyer
stephane+jdll@bortzmeyer.org

JDLL, 24 mai 2025

Le résumé

Le résumé

- Un changement profond du mécanisme de délégation,

Le résumé

- Un changement profond du mécanisme de délégation,
- qui est au cœur du DNS,

Le résumé

- Un changement profond du mécanisme de délégation,
- qui est au cœur du DNS,
- qui devra coexister longtemps avec le système actuel,

Le résumé

- Un changement profond du mécanisme de délégation,
- qui est au cœur du DNS,
- qui devra coexister longtemps avec le système actuel,
- un projet proposé à l'IETF,

Le résumé

- Un changement profond du mécanisme de délégation,
- qui est au cœur du DNS,
- qui devra coexister longtemps avec le système actuel,
- un projet proposé à l'IETF,
- dont je pense que le succès n'est pas garanti.

Délégation

Délégation

- Les noms de domaine sont gérés de manière décentralisée.

Délégation

- Les noms de domaine sont gérés de manière décentralisée.
- Des noms peuvent être **délégués** et on change alors d'organisme responsable.

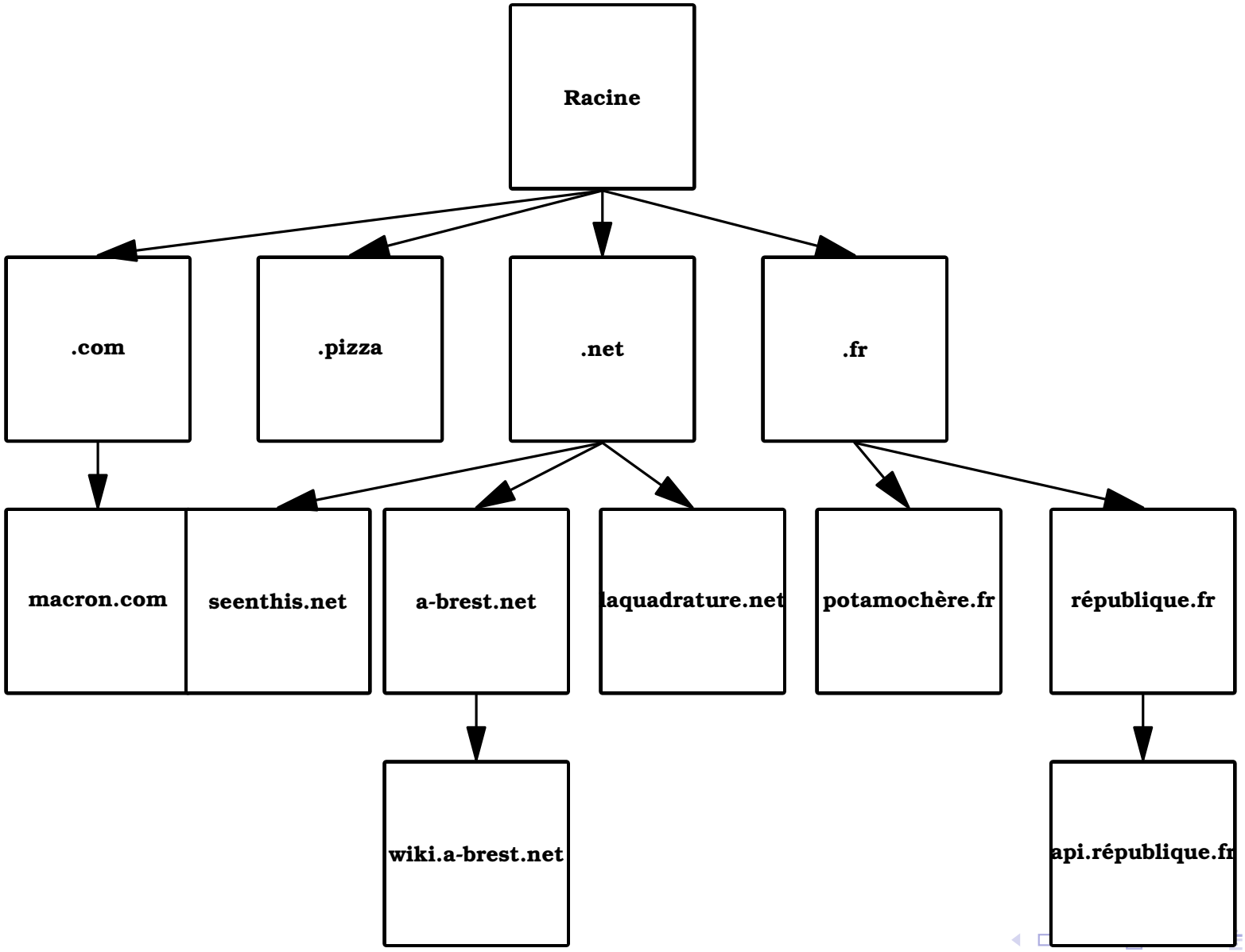
Délégation

- Les noms de domaine sont gérés de manière décentralisée.
- Des noms peuvent être **délégués** et on change alors d'organisme responsable.
- Par exemple `eu.org` est délégué depuis `.org` et délègue à son tour.

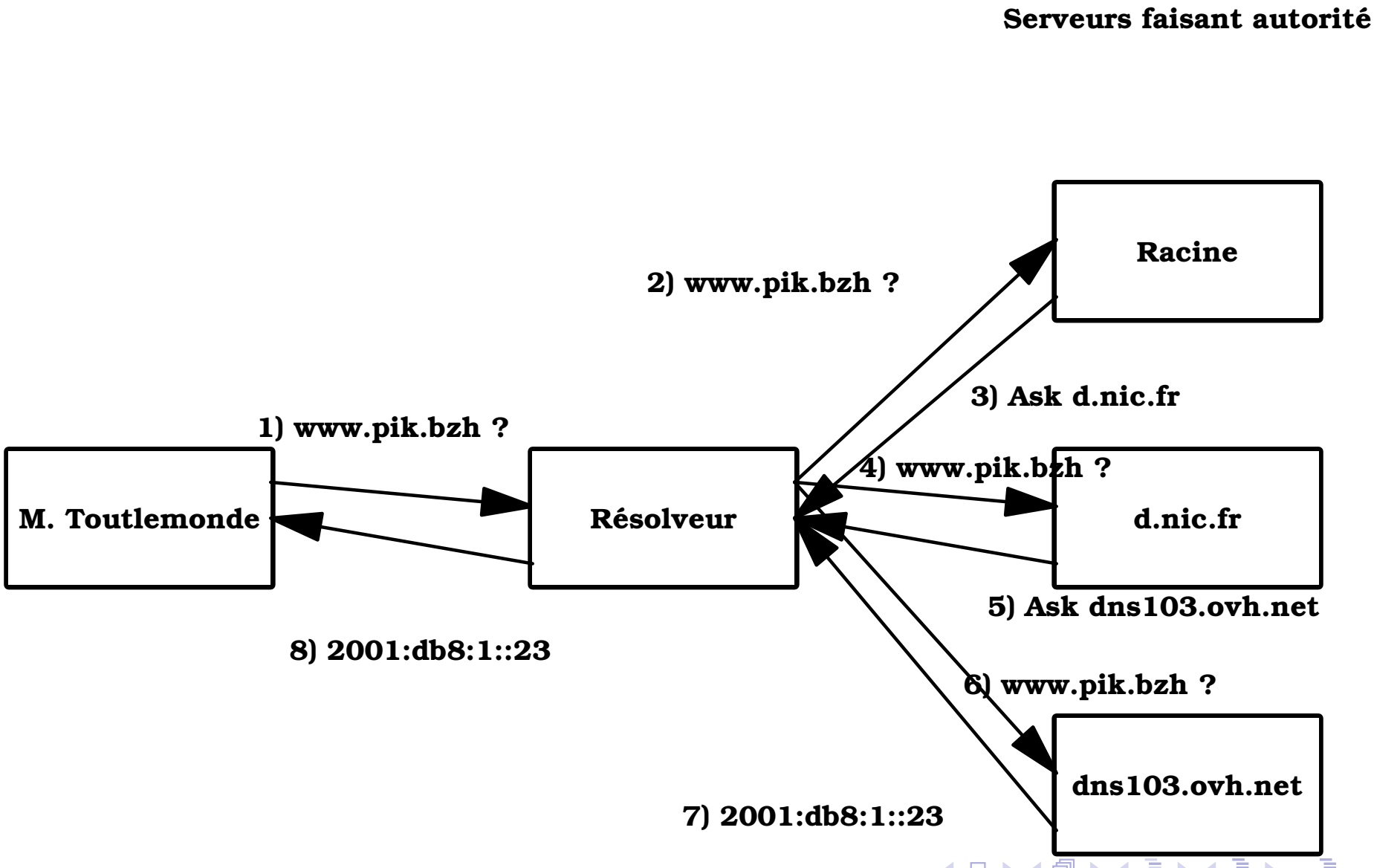
Délégation

- Les noms de domaine sont gérés de manière décentralisée.
- Des noms peuvent être **délégués** et on change alors d'organisme responsable.
- Par exemple `eu.org` est délégué depuis `.org` et délègue à son tour.
- Rien dans le nom n'indique où est la frontière de délégation : il faut utiliser le DNS.

L'arbre des noms de domaine



Résolution de noms, ou le protocole DNS en action



La délégation, vue avec dig

```
% dig @d.nic.fr www.pik.bzh
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1513
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 1
...
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 9a0da49400d664e901000000682b4aa5bb7c2c9710d3759e (good)
...
;; AUTHORITY SECTION:
pik.bzh.  3600 IN NS dns103.ovh.net.
pik.bzh.  3600 IN NS ns103.ovh.net.

;; Query time: 6 msec
;; SERVER: 2001:678:c::1#53(d.nic.fr) (UDP)
;; WHEN: Mon May 19 17:13:41 CEST 2025
;; MSG SIZE  rcvd: 116
```

Le système actuel

Le système actuel

- La délégation se fait en mettant dans la zone parente un ensemble d'enregistrements NS,

Le système actuel

- La délégation se fait en mettant dans la zone parente un ensemble d'enregistrements NS,
- ne faisant pas autorité et n'étant pas signé,

Le système actuel

- La délégation se fait en mettant dans la zone parente un ensemble d'enregistrements NS,
- ne faisant pas autorité et n'étant pas signé,
- qui doit être synchronisé avec le vrai ensemble NS,

Le système actuel

- La délégation se fait en mettant dans la zone parente un ensemble d'enregistrements NS,
- ne faisant pas autorité et n'étant pas signé,
- qui doit être synchronisé avec le vrai ensemble NS,
- ah, et il y a la colle, aussi.

Ses limites

Ses limites

- Dans le système RRR (*Registry Registrar Registrant)*, pas de place pour l'hébergeur DNS (*operator*).

Ses limites

- Dans le système RRR, pas de place pour l'hébergeur DNS.
- Exemple, si je suis titulaire et que mon hébergeur me dit d'annoncer `ns1.operator.example` et `ns2.operator.example`, et que l'hébergeur ajoute ensuite `ns3.operator.example`, tous ses clients vont devoir prévenir le registre, via le BE (Bureau d'Enregistrement).

Ses limites

- Dans le système RRR, pas de place pour l'hébergeur DNS.
- Exemple, si je suis titulaire et que mon hébergeur me dit d'annoncer `ns1.operator.example` et `ns2.operator.example`, et que l'hébergeur ajoute ensuite `ns3.operator.example`, tous ses clients vont devoir prévenir le registre, via le BE.
- Et pour le remplacement des clés DNSSEC ? L'hébergeur ne peut pas le faire directement.

Ses limites, suite

Ses limites, suite

- La délégation actuelle ne permet d'indiquer que noms et adresses IP.

Ses limites, suite

- La délégation actuelle ne permet d'indiquer que noms et adresses IP.
- Et le port ?

Ses limites, suite

- La délégation actuelle ne permet d'indiquer que noms et adresses IP.
- Et le port ?
- Et le protocole (DoT, DoH... Cf. RFC 9539) ?

Ses limites, suite

- La délégation actuelle ne permet d'indiquer que noms et adresses IP.
- Et le port ?
- Et le protocole ?
- Et d'autres trucs marrants ?

La proposition

La proposition

- Comme toujours en informatique, quand on a un problème, **on ajoute un niveau d'indirection**.

La proposition

- Comme toujours en informatique, quand on a un problème, **on ajoute un niveau d'indirection**.
- Le serveur faisant autorité, quand la réponse est sous une délégation, renverra un ensemble DELEG.

La proposition

- Comme toujours en informatique, quand on a un problème, **on ajoute un niveau d'indirection**.
- Le serveur faisant autorité, quand la réponse est sous une délégation, renverra un ensemble DELEG.
- Comme le DS, il est dans la zone parente, y fait autorité et est signé.

La proposition

- Comme toujours en informatique, quand on a un problème, **on ajoute un niveau d'indirection**.
- Le serveur faisant autorité, quand la réponse est sous une délégation, renverra un ensemble DELEG.
- Comme le DS, il est dans la zone parente, y fait autorité et est signé.
- Le bit DE : « je sais gérer DELEG ».

Exemple d'une délégation simple

(Exemple non définitif)

```
example.com.  86400  IN DELEG  1 ns1.example.com. (
                    ipv4hint=192.0.2.1 ipv6hint=2001:db8::1 proto=dot)
example.com.  86400  IN NS     ns1.example.com.

ns1.example.com.    86400   IN  A  192.0.2.1
ns1.example.com     86400   IN  AAAA    2001:db8::1
```

Exemple d'une délégation avec indirection

```
example.com.   86400   IN DELEG 0    config2.example.net.
example.com.   86400   IN NS      ns2.example.net.
```

La vraie information sera en `config2.example.net` et utilisera les SVCB du RFC 9460 :

```
config2.example.net. 3600     IN SVCB 1 . (
                    ipv4hint=192.0.2.54,192.0.2.56
                    ipv6hint=2001:db8:2423::3,2001:db8:2423::4 )
```

Les autres idées

Les autres idées

- Une proposition alternative utilise un sous-domaine `_deleg`.

La coexistence

La coexistence

- Il faut modifier les chaines d'avitaillement, les résolveurs, les serveurs faisant autorité, les logiciels de déboguage (DNSviz, Zonemaster).

La coexistence

- Il faut modifier les chaines d'avitaillement, les résolveurs, les serveurs faisant autorité, les logiciels de déboguage.
- 30 à 40 ans devraient suffire pour que l'ancien système soit remplacé par DELEG.

La coexistence

- Il faut modifier les chaines d'avitaillement, les résolveurs, les serveurs faisant autorité, les logiciels de déboguage.
- 30 à 40 ans devraient suffire pour que l'ancien système soit remplacé par DELEG.
- En attendant, côté publication, il faudra gérer les deux.

La coexistence

- Il faut modifier les chaines d'avitaillement, les résolveurs, les serveurs faisant autorité, les logiciels de déboguage.
- 30 à 40 ans devraient suffire pour que l'ancien système soit remplacé par DELEG.
- En attendant, côté publication, il faudra gérer les deux.
- Les vieux résolveurs ignoreront DELEG.

L'état actuel du projet

L'état actuel du projet

- Un groupe de travail à l'IETF.

L'état actuel du projet

- Un groupe de travail à l'IETF.
- Plusieurs *Internet-Drafts* dont certains adoptés par le groupe de travail.

L'état actuel du projet

- Un groupe de travail à l'IETF.
- Plusieurs *Internet-Drafts* dont certains adoptés par le groupe de travail.
- Prochaine étape, Madrid en juillet.

Déjà des idées d'extensions

Déjà des idées d'extensions

- DELEG pour indiquer les frontières administratives (en remplacement du défunt projet DBOUND).

Déjà des idées d'extensions

- DELEG pour indiquer les frontières administratives.
- L'idée d'ajouter des informations à la délégation excite beaucoup de monde.