Les “racines alternatives” : réalité et avenir

Stéphane Bortzmeyer
(AFNIC, mais s’exprimant en son nom personnel)
<bortzmeyer@nic.fr>

9 septembre 2003

Résumé

La question de racines du DNS, alternatives à celle existante, revient souvent dans les débats politiques sur Internet. Ce texte explique la notion de racine alternative, discute sa faisabilité et essaie surtout de séparer les questions techniques et politiques, et de bien distinguer ce qui est faisable à court terme et ce qui relève - au bon sens du terme - de l’utopie.

Ce texte propose ensuite une approche à la question de la gouvernance[1] de la racine du DNS en suggérant, non pas une juxtaposition de racines, ce qui ne peut pas marcher, mais la création d’une nouvelle racine, qui devra s’imposer par ses mérites.

1 Qu’est-ce qu’une racine du DNS ?

1.1 Le DNS tel qu’il est

1.1.1 Organisation des données

À la base de la conception du DNS ([Moc97]), se trouve la notion de hiérarchie[2]. Les domaines sont organisés en un arbre des domaines (voir figure 1). Chaque domaine est le sous-domaine d’un domaine parent, jusqu’aux TLD[3] qui sont sous-domaine de la racine, le point culminant[4] de l’espace de nommage hiérarchique. La racine est traditionnellement représentée par un point (.).

Chaque domaine peut déléguer des sous-domaines à d’autres organismes. Ceux-ci pourront alors les peupler à leur guise : le DNS est décentralisé. Mais le délégateur peut toujours accepter, refuser, ou bien changer une délégation. Il a donc un grand pouvoir, qui doit être encadré. La racine a le contrôle du contenu du DNS. D’autant plus que la “possession” d’un nom de domaine suscite des passions violentes (cf. [Kle03]).

[1] Le terme de gouvernance désigne l’ensemble des mécanismes politiques de gestion du système. Il est délibèrement assez flou car il doit pouvoir désigner des mécanismes politiques très divers. Les questions purement techniques n’appartiennent pas à ce domaine.

[2] Passer à un système non-hiérarchique - système non encore conçu et implémenté - nécessiterait donc de changer profondément l’Internet, avec d’énormes investissements.

[3] *Top Level Domains* comme `.fr` ou `.org`.

[4] Contrairement aux botanistes, les informaticiens placent les racines des arbres en haut.

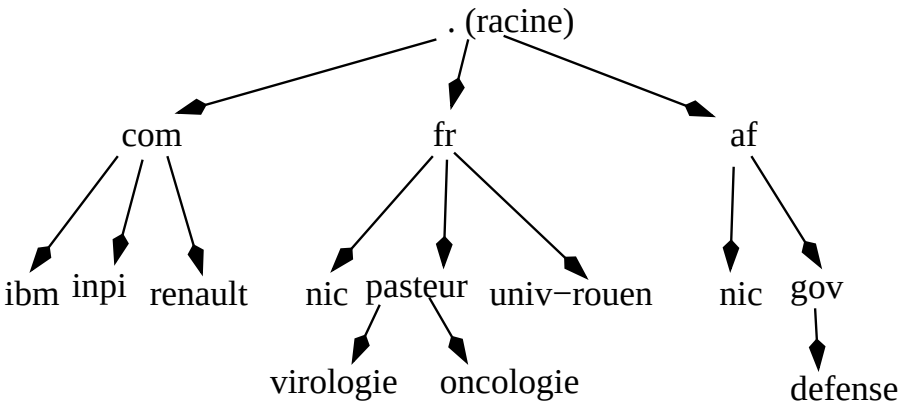

FIG. 1 – Hiérarchie des domaines

Des schémas de nommage non-hiérarchiques pourraient être envisagés mais aucun n'a encore fait l'objet d'une spécification complète, sans même parler d'un développement logiciel, a fortiori d'un déploiement sur le terrain. Le DNS est donc un élément hiérarchique dans un Internet qui en comporte peu[5].

1.1.2 La résolution de noms

Les humains se servent de noms (comme `www.debian.org`) et les machines d'adresses IP comme `192.134.4.20` ou bien `2001:660:3003:3::1:4`.

Pratiquement tout utilisation d'Internet, du Web au courrier en passant par des applications moins communes, nécessite de trouver l'adresse IP correspondant à un nom. Pour cela, les logiciels interrogent leur serveur de noms local (celui géré par leur Service Informatique ou bien par leur FAI[6]), le *cache/forwarder*. Celui-ci, s'il n'a pas de moyen plus direct de répondre, va contacter l'un des serveurs de noms de la racine, qui le redirigera vers les serveurs d'un TLD, et ainsi de suite (voir figure 2).

Les serveurs de la racine tirent cette information de leur fichier de zone (voir annexe B), un fichier géré par l'ICANN[7], The Internet Corporation for Assigned Names and Numbers (`http://www.icann.org/`), un prête-nom du gouvernement des États-Unis[8]. Le contrôle de ce fichier de zone, qui peut y faire des modifications, est l'objet de rudes luttes de pouvoir (cf. [Mue02]).

Ainsi, pour résoudre[9] `www.nic.fr`, le serveur local d'une Université brésilienne va demander à la racine, qui lui dira quels sont les serveurs de `.fr`. Il suffit donc à ce serveur local, à son démarrage, de connaitre les serveurs de la racine, le reste s'apprendra.

Comment les serveurs locaux trouvent-ils ceux de la racine ? Eh bien, nous sommes là au cœur du problème des racines alternatives. Ils trouvent l'adresse des serveurs de la racine dans un fichier

[5]Bien que l'égalité de tous dans l'Internet soit une notion assez idéalisée : Microsoft a un pouvoir considérable sur l'Internet, simplement en décidant du comportement de la prochaine version d'Internet Explorer.

[6]Fournisseur d'Accès Internet

[7]C'est ce qu'on appelle "la fonction IANA" dans le jargon de la gouvernance Internet, l'IANA (Internet Assigned Numbers Authority, `http://www.iana.org/`) étant un service de l'ICANN.

[8]C'est pourquoi on voit souvent des mentions de la "racine ICANN" ou bien la "racine NTIA/DoC" (le Doc, Department of Commerce, étant l'autorité de tutelle de l'ICANN et le NTIA `http://www.ntia.doc.gov/` son département des télécommunications) ou bien de "racine USG", pour United States Government.

[9]Traduire un nom en adresse IP.

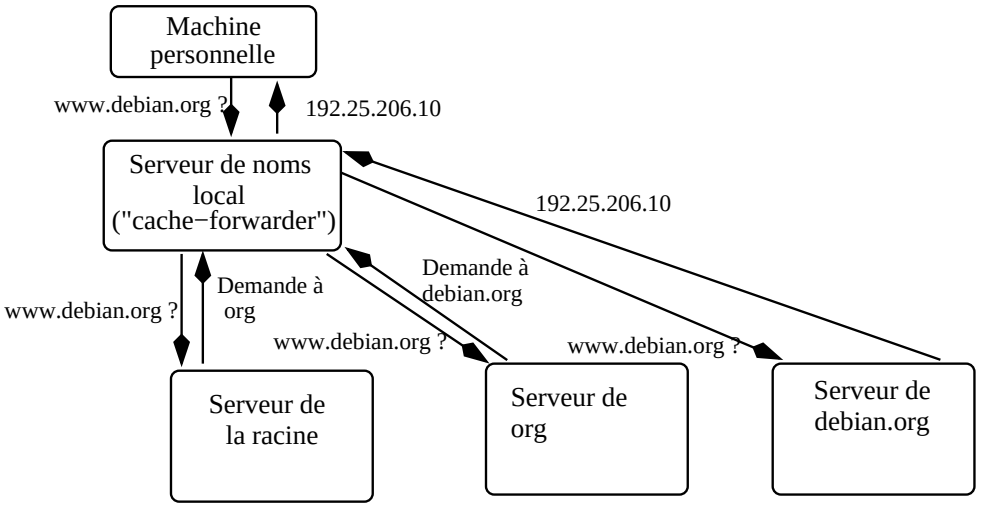

FIG. 2 – Résolution du nom www.debian.org en adresse IP

local (voir annexe A), configuré par le Service Informatique compétent. En général, ledit service se contente du fichier livré avec le logiciel utilisé. Dans la grande majorité des cas, ce logiciel est BIND (`http://www.isc.org/products/BIND/`). L'organisme qui gère BIND, l'ISC[10], a donc le pouvoir d'orienter fortement[11] le choix de la racine qu'on utilise. Le second serveur de noms, en terme d'utilisation, est probablement celui livré par Microsoft avec certaines versions de Windows.

1.2 Les racines alternatives

Alors, comment fonctionne une racine "alternative" ? Tout simplement, elle utilise le même système de nommage hiérarchique que la "vraie" mais elle a ses propres serveurs de noms, et son propre fichier de zone (qui peut utiliser tout ou partie du "vrai" fichier de zone).

1.2.1 Pourquoi créer une racine alternative ?

Il peut y avoir de nombreuses motivations pour se lancer dans cet exercice :
- C'est un exercice amusant et intéressant (beaucoup de techniciens créent une racine alternative pour cela),
- La gestion du contenu de la racine n'est pas satisfaisante, par exemple trop liée à un seul gouvernement (voir page 5),
- La gestion des serveurs de la racine n'est pas satisfaisante (pas assez de serveurs ou bien mal répartis),
- La racine alternative n'est qu'un moyen de créer de nouveaux TLD, par exemple pour vendre des enregistrements dans ces nouveaux TLD.

1.2.2 Créer sa racine ou "Le pape, c'est moi !"

Pour gérer son propre fichier de zone, la plupart des racines alternatives prennent celui de l'ICANN et ajoutent des domaines "bidon", c'est-à-dire reconnus uniquement par les utilisateurs

[10] Internet Software Consortium, `http://www.isc.org/`

[11] La plupart des administrateurs système ne changent pas les choix effectués par l'éditeur du logiciel.

de cette racine alternative particulière. C'est ainsi que l'on peut créer `.sex` ou `.law` sans formalités particulières.

Le processus est analogue à celui d'un schismatique qui prétend être le pape : tout le monde peut faire cela, et se mettre à émettre bulles et encycliques. Le plus dur est d'être reconnu par une communauté significative de fidèles.

On notera que, tant que la racine alternative demeure marginale, cela ne pose aucune difficulté technique. Trois PC connectés en ADSL et répartis chez des amis suffisent largement. Un tel exercice est souvent fait lors des formations DNS.

1.2.3 Utiliser une autre racine

Utiliser une racine alternative veut donc dire modifier le fichier de configuration de BIND (ou du logiciel équivalent) pour désigner ces serveurs au lieu des "vrais". Il faut donc une action délibérée de la part du Service Informatique ou bien du FAI[12].

Le déploiement significatif d'une racine alternative nécessite donc de convaincre beaucoup de décideurs. Ce qui nous amène aux questions sociales et politiques.

2 Quelles sont les racines alternatives actuelles ?

Cette section va malheureusement être courte : à l'heure actuelle, aucune des racines "alternatives" existantes n'offre la moindre garantie de sérieux, même en étant très indulgent. Il existe en gros trois catégories de racines alternatives :

- Les commerciaux sans scrupule, dont le seul but est de gagner de l'argent auprès de clients naïfs en leur vendant des domaines bidon. C'est l'équivalent *high tech* de l'escroc qui vous vend des propriétés sur la Lune.
  Ils prétendent en général qu'il existerait "un autre Internet" que l'on pourrait voir si l'ICANN ne les bloquait pas injustement. Ils menacent souvent l'ICANN de procès si elle ose créer un TLD correspondant au TLD bidon qu'ils ont "créé" deux ans auparavant (cf. [Gal01].
  Ils prétendent parfois avoir inventé une technologie révolutionnaire et brevetée, comme si la création d'une racine le nécessitait.
- Les individus isolés. Là encore, je ne citerai pas de noms pour ne faire de peine à personne, mais il s'agit typiquement d'individus qui viennent de découvrir que la création technique d'une racine ne demandait guère de compétences.
- Les organisations qui tentent d'explorer des voies politiques nouvelles et d'expérimenter une gouvernance vraiment démocratique de l'Internet. Elles sont peu nombreuses et les tentatives en ce sens ont toujours échoué. Aucune organisation de cette catégorie n'a une base d'utilisateurs significative. Aucune n'a vraiment produit (ou tenté de produire) de mécanisme de concertation et de décision nouveaux.
  On notera ORSC `http://www.open-rsc.org/`, ORSN `http://european.orsn.net/` ou bien OpenNIC `http://www.opennic.unrated.net/`.
  Certaines organisations appartenant à la première ou bien à la seconde catégorie avaient essayé de se faire admettre dans la troisième...

[12] Dans une certaine mesure, cette opération peut être faite par l'utilisateur final mais cela n'est pas réaliste si de nombreuses personnes le font : on perd en effet la fonction de *cache* effectuée par le serveur local, fonction sans laquelle les serveurs de la racine s'écrouleraient sous la charge.

Une liste de racines alternatives, apparement incomplète (et qui ne trie pas selon les catégories ci-dessus) est disponible en `http://root-dns.org/zones.htm`.

On notera que certaines des racines alternatives publient exactement le même fichier de zone que l'ICANN : elles ne cherchent qu'à tester la gestion des serveurs de la racine, pas la gestion des données de la racine. Comme le disent les administrateurs des serveurs racine : nous sommes des diffuseurs, pas des auteurs.

3 Doit-on et peut-on créer une nouvelle racine ?

3.1 Le problème d'une gouvernance vraiment internationale

Beaucoup de gens s'inquiètent de l'absence d'une gouvernance de l'Internet qui reflèterait son caractère international. Actuellement, on l'a vu, le gouvernement des États-Unis dispose d'un monopole sur la gestion de la racine. Il peut à sa guise redéléguer un domaine à ses amis, voire garder en otage un domaine ([Del03]).

Ce pouvoir n'est pas utilisé souvent, mais il est équivalent à l'arme nucléaire : on ne peut pas s'en servir à tout bout de champ mais c'est un monopole (un oligopole dans le cas des bombes nucléaires) qu'aucun gouvernement ne peut abandonner.

De même, l'ICANN exerce une pression permanente sur les gérants de ccTLD[13], exigeant qu'ils signent un contrat avec l'ICANN avant de faire la moindre modification au fichier de zone. Ainsi, des changements purement techniques, comme l'ajout d'un serveur de noms, prennent de six à dix-huit mois.

Pour renforcer ce pouvoir, l'ICANN garde la plupart des serveurs de noms sous son contrôle étroit. Dix de ces treize serveurs sont situés aux USA[14], ce qui limite le risque d'indépendance (le gestionnaire d'un serveur racine pourrait toujours décider d'aller chercher son fichier de zones ailleurs qu'à l'ICANN).

Si des techniques comme l'*anycast* ([Har02] ou [Kar03]) peuvent permettre de placer d'avantage de serveurs de noms, même sans autorisation de l'ICANN, elles ne réduisent pas le problème du contrôle de ces serveurs (toutes les répliques d'une même machine *anycastée* sont contrôlées par le même organisme).

De nombreux efforts ont été tentés pour changer cela : des demandes polies aux pressions modérées, les gestionnaires de domaines nationaux (ccTLD), l'ONU, les gouvernements non-états-uniens, des individus[15] ont essayé de faire évoluer les choses. Avec des résultats infimes. Le contrôle de l'Internet est devenu un enjeu majeur depuis que l'usage du réseau s'est répandu dans tous les domaines d'activité. Et le 11 septembre n'a pas amélioré les choses...

Il semble donc que le gouvernement des États-Unis n'acceptera d'évoluer que s'il a une raison sérieuse de penser que ses critiques sont prêts à mettre la main à la pâte et à démarrer une nouvelle racine. Je dis "nouvelle racine" et pas "racine alternative" car, on va le voir, il n'y a pas d'intérêt à faire marcher plusieurs racines.

[13] Country-Code Top Level Domains

[14] `http://www.root-servers.org/`

[15] `http://www.icannwatch.org` ou bien [Mue02]

3.2 L'Internet peut-il fonctionner avec plusieurs racines ?

En gros, non. Qui dit plusieurs racines dit fragmentation de l'Internet. Toute application utilisant le DNS (c'est-à-dire la grande majorité des applications) verra donc un résultat différent selon la racine utilisée. Un message envoyé à `nom@domaine.example` atterrirait dans des boites différentes selon la racine utilisée par votre fournisseur !

Ce problème, à mon avis bloquant, est bien décrit dans [ICA01] et [IAB00] même si le caractère *pro domo* du premier document le rend agaçant.

Pour résoudre ce problème de la coordination entre racines, certains ont développé le concept de racines inclusives ou exclusives. En gros, une racine exclusive ne sert sur le réseau que ses propres TLD (l'ICANN gère donc une racine exclusive) alors qu'une racine inclusive, comme son nom l'indique, inclus les TLD des autres racines inclusives.

Les racines inclusives sont souvent présentées comme un moyen de faire marcher en parallèle plusieurs racines. Mais cela oublie complètement la question des litiges : si deux racines différentes veulent `.sex`, qui l'aura ? Les litiges sont rares à l'heure actuelle, car les racines inclusives existantes ne sont que des petites expérimentations locales sans enjeu. Mais ce système ne pourrait pas fonctionner en vrai[16].

Et cela pose la question de leur légitimité : chaque individu peut créer une racine sur son PC en un quart d'heure, mais a t-il le droit de créer le TLD de son choix et d'obliger les racines inclusives à le servir ? Cette question est elle aussi laissée dans le flou : et pour cause, la définition de critéres de légitimité[17] reviendrait à créer une instance politique supérieure, justement ce qu'on prétendait éviter avec les racines multiples.

3.3 La période transitoire

On l'a vu dans la section précédente, la coexistence durable de plusieurs racines n'est pas une solution envisageable.

Le but est donc au contraire de faire une nouvelle racine, pendant une période transitoire, pour bien montrer au monde et au gérant actuel de la racine qu'une autre solution est possible et réaliste. Comme la confiance dans une telle racine ne se construit pas en quelques semaines, ni même en quelques mois, cette nouvelle racine coexistera avec l'ancienne pendant un temps assez long.

Pendant la coexistence, la nouvelle racine aura tout intérêt à suivre de près l'activité de l'ancienne : si un nouveau pays est créé, les responsables de son ccTLD ne préviendront pas forcément la nouvelle racine, il faudra donc noter son apparition dans le fichier de zone de l'ancienne racine et copier les données.

En revanche, il n'est pas utile de s'engager à copier aveuglément le fichier de zone de l'ancienne racine, le but étant de montrer la supériorité de la nouvelle. Les changements purement techniques, par exemple, comme l'ajout ou le retrait d'un serveur de noms, doivent se faire dans la journée, vue la faible taille du fichier de zone de la racine.

Cette période transitoire se terminera lorsque le gérant de l'ancienne racine sera persuadé que la nouvelle est une réalisation effective et qu'il acceptera de discuter d'égal à égal.

[16] C'est pour cela que les partisans des racines alternatives sont toujours très discrets sur ce sujet. Parfois, il y a une proposition concrète (dans une de celles que j'ai lu, il y avait une liste ordonnée de racines, les premières étant prioritaires), mais elle est vite oubliée car toutes reviennent à créer une super-racine, une nouvelle ICANN et pas forcément meilleure.

[17] "Au moins cinquante TLD et au moins trois mois de fonctionnement", ai-je lu dans un texte un peu plus précis que les autres. [ADN02] dit juste *"Those in the inclusive namespace work very hard to avoid and resolve collisions"*.

Ce projet est utopique, dans le bon sens du terme. Il est tout à fait inenvisageable à court terme[18]. Mais c'est un guide pour orienter les politiques futures, une "expérience de pensée" qui s'incarnera peut-être un jour, sous une forme qu'il est difficile de déterminer aujourd'hui.

4 Un petit numéro de politique-fiction

Un tel projet a t-il des chances de se réaliser un jour ? Il est possible de suggérer quelques prérequis pour que cette nouvelle racine ait quelques chances de succès. Il n'est pas possible ici de proposer un plan complet et détaillé, la situation n'est clairement pas assez mûre pour cela.

La partie technique est la plus facile, et de loin. Mais les parties sociales et politiques sont redoutables.

D'abord, la nouvelle racine doit être crédible, c'est-à-dire être soutenue par un certain nombre d'acteurs significatifs (un ensemble varié de gouvernements, d'opérateurs ou prestataires, d'utilisateurs).

La crédibilité implique aussi d'avoir, sinon des réponses toutes prêtes à toutes les questions, du moins d'avoir des propositions concrètes pour traiter un certain nombre de questions délicates. Le statut juridique des organismes de gouvernance est en effet très secondaire[19] par rapport à leur politique effective. Par exemple, *quid* des redélégations de ccTLD ? La nouvelle racine suivra t-elle [Pos94] ? Comment se fera l'attribution de nouveaux gTLD ? L'ICANN a un processus très ouvert pour cela[20]. Tout n'est pas forcément public mais il serait paradoxal que la nouvelle racine soit, par exemple, moins ouverte que l'ICANN sur ce point ! Cela donnerait raison à ceux qui présentent l'ICANN comme un moindre mal.

L'inconsistance des racines alternatives existantes ne se mesure nulle part mieux que dans leur silence complet sur ces questions délicates. Les réponses tournent la plupart du temps autour de "On se cordonnera". Comme si le fait de ne pas dépendre de l'ICANN allait suffire et que toutes les parties allaient devenir pleines de bonne volonté[21]. Parfois, la technique vient au secours du silence et on apprend qu'un protocole révolutionnaire (mais jamais décrit en détail) va permettre de synchroniser les racines entre elles sans douleur.

Ensuite, la nouvelle racine va devoir être humble : son succès dépendra du nombre d'acteurs qu'elle pourra convaincre[22] et aucune directive bureaucratique ne remplacera ce travail de conviction. Certaines organisations internationales, souvent présentées comme une alternative à l'ICANN, ont un passif particulièrement lourd sur ce point.

Cela suffira-t-il pour assurer le succès ? Je l'ignore mais il serait regrettable que la communauté Internet, qui a déjà remporté tant de victoires contre la résignation, ne puisse pas traiter avec succès la question d'une gouvernance vraiment internationale et démocratique.

[18] C'est l'argument favori de l'ICANN : "Que proposez-vous à la place ?".

[19] Surtout quant les statuts sont régulièrement violés, comme ce que fait l'ICANN.

[20] Voir tout le dossier de redélégation du `.org` en `http://www.icann.org/tlds/org/`.

[21] Certains gérants de TLD bidons sont très agressifs et n'hésitent pas à proférer des menaces ou à déclencher des procès à la moindre occasion, voir `http://www.dot-god.com/communications/TLD_Networks_Ltd/public_announcement.html`.

[22] FAI, pour modifier la configuration de leur serveur DNS local ; gérants de domaine, pour qu'ils s'adressent à la nouvelle racine et pas uniquement à l'ICANN ; auteurs de logiciels pour qu'ils livrent un fichier de serveurs de la nouvelle racine, etc.

A Annexe : la configuration du serveur local pour trouver la racine

Voici le fichier de configuration d'un serveur de noms local (celui de votre Université ou de votre FAI). C'est dans ce fichier qu'on trouve les adresses IP des serveurs de la racine. "Changer de racine" signifie donc simplement éditer ce fichier[23].

```
;       This file holds the information on root name servers needed to
;       initialize cache of Internet domain name servers
;       (e.g. reference this file in the "cache  .  <file>"
;       configuration file of BIND domain name servers).
;
;       This file is made available by InterNIC registration services
;       under anonymous FTP as
...
;
; formerly NS.INTERNIC.NET
;
.                        3600000  IN  NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.      3600000      A     198.41.0.4
;
; formerly NS1.ISI.EDU
;
.                        3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.      3600000      A     128.9.0.107
... (Autres serveurs, treize en tout)
```

B Annexe : le fichier de la racine

C'est ce fichier qu'utilisent les serveurs de noms de la racine. Il est disponible en `ftp://rs.internic.net/domain/root.zone.gz`. Vue sa taille, c'est une toute petite base de données, dont l'exploitation ne soulève aucune difficulté technique. En voici un extrait :

```
...
COM. NS A.GTLD-SERVERS.NET.
COM. NS G.GTLD-SERVERS.NET.
COM. NS H.GTLD-SERVERS.NET.
... (autres serveurs de .com)
EE. NS NS.EU.NET.
EE. NS SUNIC.SUNET.SE.
EE. NS NS.UU.NET.
EE. NS NS.KBFI.EE.
... (autres serveurs de l'Estonie)
FR. NS DNS.CS.WISC.EDU.
FR. NS NS1.NIC.FR.
FR. NS NS3.NIC.FR.
FR. NS DNS.INRIA.FR.
FR. NS NS2.NIC.FR.
FR. NS DNS.PRINCETON.EDU.
FR. NS NS-EXT.VIX.COM.
```

[23] On peut trouver la version officielle en `ftp://rs.internic.net/domain/named.root`.

```
FR. NS NS3.DOMAIN-REGISTRY.NL.
...
```

Références

[ADN02] ADNS, *About The Inclusive Namespace*. September 2002. http://www.adns.net/about_alternative_domains.html.

[Del03] Céline Delacourt, *Les noms de domaine, enjeu de la géopolitique américaine*. May 2003. http://news.zdnet.fr/story/0,,t235-s2134301,00.html.

[Gal01] Leah Gallegos, *ICANN governance*. February 2001. http://www.house.gov/commerce/hearings/gallegos.htm.

[Har02] T. Hardie, RFC 3258[24], *Distributing Authoritative Name Servers via Shared Unicast Addresses*. April 2002.

[IAB00] IAB, RFC 2826, *IAB Technical Comment on the Unique DNS Root*. May 2000.

[ICA01] ICANN, *A Unique, Authoritative Root for the DNS.* July 2001. http://www.icann.org/icp/icp-3.htm.

[Kar03] Daniel Karrenberg, *Distributing K-Root Service by Anycast Routing of 193.0.14.129*. February 2003. http://www.ripe.net/ripe/docs/ripe-268.html.

[Kle03] J. Klensin, RFC 3467, *Role of the Domain Name System (DNS)*. February 2003.

[Moc97] P. Mockapetris, RFC 1034, *Domain names - concepts and facilities*. November 1997.

[Mue02] Milton L. Mueller. *Ruling the root. Internet governance and the taming of cyberspace*. Number 0262134128 in ISBN. MIT press, 2002.

[Pos94] J. Postel, RFC 1591, *Domain Name System Structure and Delegation*. March 1994.

[24]Pour voir le RFC de numéro NNN, http://www.ietf.org/rfc/rfcNNN.txt, par exemple http://www.ietf.org/rfc/rfc3258.txt