

V0.2a

Dr.Francis Muguet: francis.muguet@unige.ch

[KNIS, Research Group](#)

[Département des Systèmes d'Information](#)

[Université de Genève](#)



La différence entre les « Classes » de nommage et les serveurs racines alternatifs

Un petit dialogue entre Ludovic et Fabien

Pour donner un peu de vie à un sujet qui pourrait paraître aride aux non-spécialistes, cet exposé est mis sous la forme d'un dialogue entre deux personnages fictifs : Ludovic, partisan des serveurs racines alternatifs et Fabien partisan des classes.

Rappelons qu'une *classe* est le paramètre qui définit un réseau dans lequel on peut installer un espace de nommage. Les *classes* sont déterminées par la [RFC 2929](#) que les logiciels de serveurs et clients devraient normalement mettre en oeuvre. L'internet dont nous faisons tous usage, utilise la *classe* « IN » dont le nommage est géré par l'ICANN. A l'heure actuelle, en pratique, le champ *classe* ne prends que la valeur « IN », mais il existe jusqu'à 65,000 classes disponibles et non utilisées.

Ludovic : Pour avoir plusieurs espaces de nommage indépendants de l'ICANN, il suffit d'installer des DNS indépendants de l'ICANN. Il n'y a nullement besoin de *classes*, il suffit d'utiliser BIND standard, et c'est immédiatement disponible. Pour indiquer l'espace, on peut indiquer sur son ordinateur les adresses IP du DNS associé. Ce n'est rien d'autre que des racines dites alternatives, que je préfère appeler des racines "ouvertes". Il y en a des dizaines en service.

Fabien : C'est tout à fait exact.

D'abord notons que le nombre d'[opérateurs DNS alternatifs](#) ne fait que diminuer et leur activité décroître : [Public Root](#) - [Open Nic](#) - [New.net](#) - [UnifiedRoot](#) - [NameSpace](#) (546 gTLDs).

Ensuite, le premier point évident qui vient à l'esprit que la majorité écrasante des internautes ne savent même pas ce qu'est un serveur DNS, et savent encore moins comment le modifier. C'est pourquoi [New.net](#), un parmi les cinq survivants des [opérateurs DNS alternatifs](#), n'indiquent même plus la liste de leurs serveurs DNS, [New.net](#) préconise l'usage d'un plugin propriétaire d'Internet Explorer, que [Wikipedia](#) caractérise comme un [espioniciel](#), qui est souvent installé à l'insu de l'internaute : *Il collecte les informations sur l'utilisation du PC et les revend, Il crée une grande base de données. Il ralentit la vitesse de surf sur internet, des téléchargements, et provoque de nombreuses déconnexions.*

En dehors de l'usage non-éthique concernant la collecte des informations, il est clair que ne disposant pas du cache du serveur DNS du FAI, le plugin doit aller l'information sur le serveur racine DNS alternatifs, puis doit probablement se constituer son proche cache (la base de données) dont l'intégrité n'est pas garantie(déconnexions). Tout cela n'est pas très performant et ralentit la résolution des noms de domaines.

Un point pratique important que les serveurs DNS alternatifs sont inadaptés à la mobilité, et en tout cas à la procédure manuelle (comme chez [namespace](#)) que vous suggérez. Très souvent, les internautes utilisent des adresses IP dynamiques déterminées automatiquement (DHCP), les serveurs DNS sont alors déterminés par le DHCP, et seul une infime minorité d'internautes savent modifier les IPs des serveurs DNS dans ce cas. Ensuite, il faudrait remettre les IPs des serveurs DNS alternatifs, à chaque fois que le DHCP renouvelle les IP dynamiques et écrase les anciennes IPs des serveurs DNS, c'est totalement impraticable sauf à installer un script ou plugin, avec les problèmes sus mentionnés.

De plus, bien souvent les FAIs n'autorisent que l'usage de leurs serveurs DNS pour éviter le [phishing](#). Au niveau sécurité, d'une certaine manière, les serveurs DNS alternatifs ne sont qu'un vaste [phishing](#) .

Votre appellation de racines "ouvertes" induit une confusion avec le défunt [Open Root Server Network](#) (initiative européenne fermée fin 2008) qui comprenait 13 racines synchronisées une fois par jour sur les racines de l'ICANN.

Un autre point important à expliquer, est les serveurs racines ne sont pas consultés à chaque requête de résolution d'un nom de domaine, car les serveurs DNS des FAIs gardent en cache les réponses qu'ils ont donné récemment, et donc donne une réponse immédiatement. S'ils n'ont pas la réponse, il la demandent à des serveurs DNS régionaux, qui peuvent la donner s'ils ont la réponse en cache, et ainsi de suite, récursivement, avec des

serveurs DNS de niveau supérieur. Les serveurs racines ne consultés que s'il n'y a pas eu de réponse dans les caches successives . Il est assez remarquable de souligner que ce réseau de serveurs DNS s'est construit d'une manière informelle, au cours du temps, sans aucun cadre contractuel. Avec l'approche des *classes*, on utilise le même réseau de serveur DNS, dont cependant le logiciel doit supporter pleinement la [RFC 2929](#). Dans une phase d'expérimentation dans une région donnée, on s'assurera précisément que les FAIs et autres intervenants techniques participants utilisent bien un logiciel DNS supportant les *classes*.

Les serveurs DNS alternatifs obéissent à une autre logique, comme on utilise dès le départ un serveur DNS différent, on ne peut pas utiliser la hiérarchie existante des millions de serveurs DNS existants, avec leurs caches. Par conséquent, à moins de reconstruire un réseau équivalent, on aura des temps de réponse dégradée dès que l'on mettra le système en charge.

Maintenant votre espace de nommage, si je comprend bien, est complètement distinct de celui de l'ICANN, comment faites-vous pour répondre à la demande des internautes d'accéder au noms de domaines de l'ICANN. ?

Ludovic : Très facile, mes serveurs racines « ouverts » peuvent contenir une copie de tout ou partie de la racine de l'ICANN auquel je rajoute mes TLDs !

Fabien : D'abord ce n'est pas une mince affaire technique que de copier les gros serveurs racines de l'ICANN avec fiabilité et synchronisation. Ensuite, est-ce vous copiez aussi les serveurs racines de vos concurrents alternatifs ?

Ludovic : Non, il ne me semble pas....

Fabien : Donc vous avez une double fragmentation (avec des collisions possibles) non seulement avec l'ICANN; mais entre opérateurs alternatifs !; ce n'est pas un système très cohérent, ni vraiment ouvert à la compétition ! . Il y a des collisions entre opérateurs alternatifs, par exemple le *.free* à la fois chez OpenNic et New.net !

Au contraire le système des *classes*; lui permet d'avoir 65,000 concurrents avec des espaces de nommages qui sont adressables entre eux, et sans collision possible !.

Concernant les collisions, par exemple [New.net](#) vendaient les extensions *.biz* et *.travel* qui ne figuraient pas alors dans les extensions ICANN et ensuite, quand l'ICANN a introduit les *.biz* et *.travel*, les propriétaires de noms de domaines *.biz* et *.travel* ont tout perdu en pratique, sans aucun recours possible.

Ludovic : Ils se sont fait escroqués par l'ICANN ! Ils étaient les premiers arrivants !

Fabien : Oui, mais ces malheureux détiennent des droits par rapport à une entité [New.net](#) qui elle ne possède aucun droit !, ni selon une norme ou un accord spécifique. L'ICANN lui possède des droits en vertu d'accords avec le département du Commerce des États-Unis. D'ailleurs ce serait plutôt l'ICANN

et Verisign qui pourraient poursuivre [New.net](#) !

Ludovic : A quel titre ? Et devant quelle juridiction ?

Fabien : La juridiction de pratiquement n'importe quel pays. Quand j'ai dit, que les opérateurs DNS alternatifs n'ont aucun droit, en fait c'est encore pire. Ils contreviennent aux RFCs qui stipulent que chaque classe possède un serveur racine unique (avec un système technique de sauvegarde sur plusieurs sites), car ils opèrent dans la *classe* IN. Vis à vis de leurs clients qui achètent des noms de domaines en contradiction avec les RFCs, ils se pose un problème de responsabilité, sauf à dire que les RFCs n'ont pas de valeur légale... ce qui est un autre problème que nous ne discuterons pas....

Vis à vis de l'ICANN et de Verisign, au niveau civil, il y a des problèmes juridiques, sur le fondement de dommages (responsabilité civile) et au niveau commercial sur le fondement de la concurrence déloyale ou du parasitisme : Suivant l'étude [Les nouveaux comportements de parasitisme/concurrence déloyale en matière de noms de domaines](#) par Hélène Thomopoulos et Didier Le Goff (cabinet Selafa), d'une manière générale : *Selon M. Saint-Gal, qui a introduit en France le concept de parasitisme, « la concurrence parasitaire [...] consiste pour un tiers à vivre en « parasite » dans le sillage d'un autre en profitant des efforts qu'il a réalisés et de la réputation de son nom et de ses produits ».* La spécificité de la notion de parasitisme réside en la possibilité de qualifier comme fautive la reproduction ou l'imitation d'un signe sans référence nécessaire au risque de confusion et sans que le fautif soit un concurrent. Le fait de profiter indûment des investissements de recherche et des efforts commerciaux du titulaire du signe est considéré comme répréhensible en soi. Si on copie la base de donnée d'un tiers, sans contrepartie, ni autorisation, pour y rajouter quelque chose pour le revendre, il y a de fortes chances que l'on soit dans une situation de parasitisme. Comme les serveurs alternatifs sont des échecs, l'ICANN et Verisign ne sont sans doute pas donné la peine de faire des procès.

Quant on utilise les *classes*, on n'a pas besoin de copier les bases de données des autres *classes*. C'est techniquement moins cher et juridiquement plus approprié.

Ludovic : il n'en reste pas moins que l'attribution des *classes* est administrée par l'IETF! Quelle chance pour eux, cela va leur permettre de les vendre ou de les interdire !

Fabien : A l'inverse de l'ICANN, je ne connais pas d'exemple où l'IETF ait vendu quelque chose, mais je peux me tromper... Concernant les *classes*, les précédents sont très forts, ni Hesiod, ni ChaosNet, ni l'Internet n'ont du payer leurs *classes* !, et je doute qu'il y ait un consensus IETF pour modifier cette approche, ne serait-ce que parce que les partisans des *classes* s'y opposeraient. Avec un système consensuel, il est très difficile de modifier une RFC existante. Si malgré tout, la coordination de l'IETF, outrepassant le manque de consensus, décidait que l'attribution d'une classe se faisait par une vente, l'IETF serait dans une position juridique délicate, susceptible d'une action judiciaire.

Cette attitude ouvrirait la voie à une remise en cause du rôle de l'IETF dans la l'attribution des *classes* car celle-ci concerne la gouvernance entre des réseaux différents, et car par construction l'IETF n'a pas une autorité sur d'autre réseau que l'Internet. Selon le droit international public, ce serait plutôt l'UIT qui serait légitime dans une gouvernance inter-réseau.... Une action judiciaire pourrait aboutir à un dessaisissement de l'autorité de l'IETF quant à l'affectation des classes.

Donc au niveau juridique, la situation avec les classes, est totalement différente que celle avec les DNS alternatifs. Le rapport des forces est complètement inversé.

Pour l'utilisation de l'une des 255 *classes* privées, l'IETF n'a pas à être consultée. Une expérimentation de *classes* peut donc commencer sans aucun obstacle juridique.

Conclusion.

Ce dialogue fictif illustre bien que la problématique technique, et le contexte juridique des serveurs DNS alternatifs et des *classes* sont totalement différents.