# RFC 3879 : Deprecating Site Local Addresses

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 14 octobre 2008

Date de publication du RFC : Septembre 2004

https://www.bortzmeyer.org/3879.html

---

L'IETF n'a jamais apprécié les identificateurs à portée purement locale, comme le TLD `.local` ou comme les adresses IP privées du RFC 1918[1]. Ces identificateurs locaux, dont la signification est spécifique à un site donné, soulèvent plusieurs problèmes, par exemple une question pratique : que faire si deux organisations fusionnent et qu'elles utilisent toutes les deux de tels identificateurs, qui sont en collision ?

Les RFC successifs sur l'adressage IPv6 prévoyaient des identificateurs « "*site-local*" », spécifiques à un site, dans le préfixe `FEC0::/10` (RFC 3513, section 2.5.6, ce RFC ayant depuis été remplacé par le RFC 4291). Toute organisation pouvait piocher librement dans ces adresses, tout en faisant attention à ne pas les laisser sortir de son site. Cela a permis à beaucoup d'organisations de commencer à expérimenter avec IPv6.

Mais ces identificateurs posaient des problèmes, en général communs avec tous les problèmes des identificateurs locaux. La section 2 du RFC les détaille :

- Si des applications se passent des adresses IP, comme le font FTP ou SIP, elles doivent connaitre les frontières de site pour savoir si elles peuvent passer des adresses privées (section 2.2).
- Commes les domaines privées, les adresses IP privées tendent à « fuir », à être transmises en dehors du site (par exemple dans les en-têtes `Received:` du courrier électronique ou via des requêtes DNS comme celles qu'absorbe l'AS112). Comme elles perdent toute signification en dehors du site d'origine, cela sème la confusion (section 2.3).
- Elles nécessitent un traitement spécial par les routeurs (section 2.4).
- Selon le RFC 3879, le concept de « site » lui-même n'est pas clairement défini (section 2.5). Est-ce une entité administrative unique ? Un site géographique unique ? Un AS ? Je dois avouer que cette section est la moins convaincante de tous et qu'elle donne l'impression que les auteurs ont voulu charger la barque. Puisque les adresses « "*site-local*" » sont spécifiques à un site, rien n'empêchait chaque site d'avoir sa propre définition.

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc1918.txt`

Du point de vue pratique, pour l'opérateur d'un réseau, ces inconvénients pouvaient sembler légers et, de toute façon, un mécanisme de remplacement était nécessaire. C'est au développement de ce mécanisme que s'attaque la section 3 qui réclame un mécanisme alternatif assurant l'unicité des adresses « locales ». Cela ne supprimera pas, par exemple, les fuites, mais cela les rendra plus facile à déboguer. Ce mécanisme, les **ULA** ("*Unique Local Addresses*") a finalement été créé par le RFC 4193.

Un détail important : la section 5, consacrée à la sécurité, rappelle que, contrairement à ce que croient beaucoup d'administrateurs réseaux débutants, le fait d'avoir des adresses privées n'offre à peu près aucune protection (par exemple parce que des techniques comme le changement DNS <https://www.bortzmeyer.org/dns-rebinding-pinning.html> permettent d'attaquer de l'intérieur). La bonne technique est l'emploi de filtres et elle s'applique aux adresses privées comme aux publiques.

Il ne faut cependant pas considérer que les identificateurs locaux sont systématiquement une mauvaise idée. Ils sont nécessaires lorsque l'obtention d'identificateurs globaux, valables partout, est difficile ou coûteuse. C'est le cas des adresses IPv4 privées du RFC 1918 : vue la pénurie d'adresses IPv4 et les obstacles financiers et bureaucratiques à franchir pour en obtenir, il est logique d'utiliser ces adresses privées. C'était également le cas à l'époque pour les adresses IPv6 privées. Pendant longtemps, il était complètement impossible d'en obtenir (par diplomatie, pour éviter de vexer les RIR, le RFC 3879 évite de rappeler cet épisode). Il est donc déplorable que ce RFC aie été publié avant que son successeur, le RFC 4193, soit prêt. Désormais, les ULA de ce RFC fournissent une meilleure solution, qui évite notamment les collisions entre deux sites qui fusionneraient. On peut donc enterrer `FEC0::/10` sans remords.