RFC 6866 : Problem Statement for Renumbering IPv6 Hosts with Static Addresses in Enterprise Networks

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 28 février 2013

Date de publication du RFC : Février 2013

https://www.bortzmeyer.org/6866.html

Comment renuméroter (changer les adresses IP) le réseau d'une organisation ? Quels sont les obstacles techniques qui font que cette renumérotation est parfois difficile ? Ce RFC décrit le problème du renumérotage en IPv6 pour le cas des adresses statiques, le RFC 6879 [1] fournissant des solutions pour les autres cas (le RFC 4192 fournissait déjà certaines pistes).

Le problème avait été posé par le RFC 5887 : changer les adresses IP sur un réseau local nécessite du travail, trop de travail. Peut-on faciliter la vie des administrateurs réseaux sur ce point ? C'est le travail du groupe 6renum <http://tools.ietf.org/wg/6renum> de l'IETF dont voici le premier RFC. 6renum se focalise sur les réseaux IPv6 (en IPv4, la pénurie d'adresses <https://www.bortzmeyer.org/epuisement-adresses-ipv4.html> rend le problème bien pire). Et ce RFC de description du problème se lmite au cas où les machines ont des adresses **statiques**, c'est-à-dire stables sur une longue période. Autrement, pour les adresses dynamiques, renuméroter est bien plus simple (en général, on redémarre les machines et c'est tout). Les "*Enterprise Networks*" dont parle le titre du RFC sont les réseaux assez grands et complexes pour avoir pas mal d'adresses statiques (le petit réseau de la maison ou du SOHO est en général 100 % en adresses dynamiques).

Notons qu'avec une autre architecture de réseau, par exemple une séparation de l'identificateur et du localisateur <https://www.bortzmeyer.org/separation-identificateur-localisateur.html>, le problème n'existerait pas. Mais, comme le note la section 3.2 du RFC 6250, l'Internet a commencé avec uniquement des adresses statiques (DHCP n'existait pas) et les programmeurs ont supposé certaines propriétés des adresses IP qui étaient vraies à l'époque mais ne le sont plus forcément aujourd'hui. C'est à cause de cela qu'il est parfois plus simple aujourd'hui d'avoir des adresses statiques, bien que les raisons de ce choix ne soient pas toujours incontestables :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6879.txt

— Certains serveurs doivent être connus par une adresse IP, pas par un nom (c'est typiquement le cas des serveurs DNS),
— Certains serveurs **pourraient** être identifiés par un nom, résolu via le DNS, mais l'administrateur ne maitrise pas assez le DNS et ne l'utilise pas (de mon expérience, c'était très fréquent encore au début des années 1990 mais aujourd'hui, cela me semble rare),
— Une adresse statique facilite la gestion du parc des machines, et leur localisation, par exemple en cas d'incident de sécurité,
— Certains mécanismes de licence logicielle sont fondés sur l'adresse IP (très mauvaise idée mais qu'on rencontre dans la nature),
— Les équipements du réseau (par exemple les routeurs) ont souvent des adresses statiques, par exemple pour faciliter la supervision,
— Les ACL et autres mécanismes de sécurité sont souvent basés sur des adresses IP fixes.

Attention, on parle bien d'adresses statiques, pas d'adresses manuellement affectées. Les adresses manuelles sont toujours statiques mais l'inverse n'est pas vrai : on peut attribuer des adresses statiques par DHCP, pour centraliser la configuration et éviter de modifier chaque machine.

La section 3 résume le problème à résoudre et l'approche proposée pour l'instant :
— Éviter de désigner des machines par des adresses IP, utiliser les noms pour leur stabilité <https://www.bortzmeyer.org/pourquoi-le-dns.html>,
— Avoir une gestion de configuration centralisée où, à partir d'une base de données centrale, les informations de configuration sont automatiquement calculées et poussées vers toutes les machines,
— Utiliser les ULA du RFC 4193 pour le trafic purement interne,
— Lorsqu'on renumérote, suivre les procédures du RFC 4192.

La section 2 analyse en détail chacun des points délicats. D'abord, pour avoir des adresses statiques, il faut aussi des préfixes IP statiques. Cela facilite certains diagnostics (≪ tous les gens qui se plaignent sont dans 2001:db8:199:ac:: donc il doit y avoir un problème de ce côté-là ≫) mais, en IPv6, ce n'est nullement obligatoire, les préfixes, comme les adresses, peuvent être entièrement dynamiques (d'autant plus que, contrairement aux préfixes IPv4, ceux d'IPv6 sont difficiles à mémoriser). Pour les petits réseaux, c'est certainement la meilleure solution.

Et les machines qui sont référencées par une adresse IP ? Pourquoi des gens font cela alors qu'ils pourraient utiliser le DNS, le SLP du RFC 2608 ou mDNS (combiné avec "*Service Discovery*") ? C'est parce qu'utiliser des adresses IP peut représenter moins de travail pour les petites organisations que d'installer et de configurer un serveur DNS. Et SLP, comme mDNS, est largement implémenté mais très rarement déployé dans les réseaux d'≪ entreprise ≫. Bref, pas mal de gens numérotent l'imprimante 10.1.1.2 et communiquent cette adresse aux utilisateurs pour qu'ils l'entrent dans leur configuration. Cela empêche une renumérotation facile. Il n'est pas évident que cette pratique continue en IPv6, où les adresses sont nettement plus difficiles à communiquer (≪ Non, j'ai dit 2001 comme le film, deux points, non l'un au dessus de l'autre, pas un point suivi d'un autre, db8, oui, D comme Denise et B comme Béatrice... ≫).

Naturellement, il n'y a pas que les imprimantes : les serveurs ont souvent des adresses IP fixes. Il serait mieux que les serveurs soient accédés par leurs noms, pas par leurs adresses. Mais cela suppose de mettre à jour le DNS en cas de renumérotation, ce que certains ont du mal à faire. Du DNS mis à jour dynamiquement et de manière sécurisée (RFC 3007) serait peut-être une solution. Cela laisserait toutefois la question du TTL (RFC 4192).

Je le répète, adresse statique ne signifie pas forcément adresse manuellement configurée quelque part sur le serveur. On peut parfaitement distribuer des adresses statiques avec DHCP. Si la zone DNS et la configuration DHCP sont dérivées automatiquement de la même base de données, la cohérence est assurée. C'est une bonne pratique, comme indiqué plus haut : nul besoin d'usines à gaz, un fichier plat

et un script Python de quelques lignes suffisent. Sans cette pratique, il faut se connecter à chaque serveur pour changer sa configuration (ou bien utiliser des systèmes comme Ansible ou peut-être Chef).

Les routeurs et autres composants du réseau (comme les commutateurs) sont également souvent numérotés de manière fixe. Comme ils sont essentiels au bon fonctionnement du réseau, ils sont en général sous supervision. Cela rend difficile la renumérotation car il faut alors changer la configuration de Nagios ou de son équivalent. Il y a une école qui défend l'idée d'adresses ULA (RFC 4193) pour tous ces éléments de l'infrastructure, de manière à les préserver contre la renumérotation.

On l'a vu, une autre raison importante pour laquelle les administrateurs réseaux utilisent des adresses IP statiques est la gestion de parc. L'adresse IP sert alors d'identificateur pour la machine, simplifiant certaines procédures. L'IDS dit que `2001:db8:21:1::1:134` fait plein de connexions vers le port 25 ? On retrouve facilement de quelle machine il s'agit. Notons toutefois qu'aujourd'hui, même dans les réseaux qui ont une telle pratique, les machines connectées en WiFi y échappent, et ont des adresses dynamiques.

À noter que les bons conseils de la section 3 laissent ouverts quelques problèmes :

— Même en suivant tous ces conseils, les sessions de très longue durée (SSH, par exemple) seront coupées. Est-ce acceptable ?
— Est-ce que la rénumérotation des éléments du réseau (comme les routeurs) sans couper les sessions utilisateur est possible ?