RFC 6598 : IANA-Reserved IPv4 Prefix for Shared Address Space

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 23 avril 2012

Date de publication du RFC : Avril 2012

https://www.bortzmeyer.org/6598.html

Après beaucoup de discussions pas toujours sereines, l'IESG a finalement décidé de publier ce très controversé RFC. Il réserve un préfixe IPv4, 100.64.0.0/10, aux services de partage d'adresses IP entre utilisateurs, les CGN ("*Carrier-Grade NAT*"). Ce faisant, il légitime ce concept de CGN, ce qui a déclenché la colère de beaucoup.

Voyons d'abord le paysage : les adresses IPv4 sont à peu près épuisées <https://www.bortzmeyer.org/epuisement-adresses-ipv4.html>. Mais le déploiement d'IPv6 a pris beaucoup de retard et il n'est pas, à l'heure actuelle, prêt à prendre le relais. Plusieurs FAI, notamment en Asie, ont donc commencé à déployer des systèmes où l'abonné de base n'a aucune adresse IPv4 publique. Avant cela, M. Toutlemonde n'avait certes qu'une seule adresse publique et devait faire du NAT pour donner à toutes ses machines une connectivité Internet partielle. Mais, au moins, le partage d'adresses ne se faisait qu'entre habitants du même foyer, Aujourd'hui, par manque d'adresses IPv4, les déploiements en cours repoussent le NAT dans le réseau de l'opérateur (d'où le nom de CGN, "*Carrier-Grade NAT*", voir par exemple le RFC 6264 [1] ou bien le RFC 6888) et le partage d'adresses publiques se fait désormais entre abonnés n'ayant rien en commun. Désormais, si votre voisin télécharge illégalement, c'est peut-être sur vous que l'HADOPI tombera...

Le partage d'adresses (documenté dans le RFC 6269) n'est pas le seul inconvénient des CGN. Ces gros routeurs NAT, gardant en mémoire l'état des flux pour des centaines ou des milliers d'abonnés, diminuent la résistance aux pannes : si on redémarre l'un d'eux, tous les abonnés perdent leurs sessions en cours. Voilà pourquoi l'idée même de CGN (qui met de l'« intelligence » dans le réseau et non pas aux extrémités) hérisse tant de gens à l'IETF.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6264.txt

Si on fait quand même des CGN, se pose le problème de la numérotation des réseaux. Le réseau local de l'abonné (appelons-le M. Li car les CGN pour des accès Internet fixe sont aujourd'hui surtout répandus en Chine) est typiquement numéroté avec le RFC 1918. L'opérateur ne peut pas utiliser les adresses de ce même RFC pour son réseau, entre M. Li et le gros CGN, à cause du risque de conflit avec le réseau local de M. Li (sauf si l'opérateur contrôle ledit réseau, via ses "*boxes*"). Il ne peut pas utiliser des adresses IP publiques puisque, c'est le point de départ de toute l'histoire, celles-ci manquent. Il faut donc un « nouveau RFC 1918 ». C'est le rôle de ce RFC 6598, qui réserve un nouveau préfixe, `100.64.0.0/10`, à cet usage. Il s'ajoute aux autres préfixes « spéciaux » du RFC 6890. Il servira aux machines entre le CPE (la "*box*") et le routeur CGN et ne sera donc typiquement jamais vu sur l'Internet. À noter que ce préfixe n'a rien de particulier, à part son usage officiel : on pourrait parfaitement s'en servir pour autre chose que du CGN. Voici le nouveau préfixe, vu avec whois :

```
% whois 100.64.0.0
NetRange:       100.64.0.0 - 100.127.255.255
CIDR:           100.64.0.0/10
OriginAS:
NetName:        SHARED-ADDRESS-SPACE-RFCTBD-IANA-RESERVED
NetHandle:      NET-100-64-0-0-1
Parent:         NET-100-0-0-0-0
NetType:        IANA Special Use
RegDate:        2012-03-13
Updated:        2012-03-15
```

Ah, pourquoi une longueur de 10 à ce préfixe ? Un préfixe plus court (comme un /8) aurait été difficile à trouver de nos jours, et un plus long (par exemple un /12), offrant moins d'adresses, aurait obligé les FAI, dans certaines régions très peuplées, à déployer des CGN emboités... Un /10, par exemple, suffit à desservir toute l'agglomération de Tokyo (un FAI japonais ne peut donc pas avoir un seul routeur CGN pour tous le pays).

La section 4 du RFC précise l'usage attendu : chaque FAI utilisera librement `100.64.0.0/10` et ce préfixe n'aura donc de signification que locale. Les adresses `100.64.0.0/10` ne doivent **pas** sortir sur l'Internet public (le mieux est de les filtrer en sortie et, pour les autres FAI, en entrée, car il y aura toujours des négligents). Ces adresses ne doivent pas non plus apparaître dans le DNS public. Les requêtes DNS de type PTR pour ces adresses ne doivent **pas** être transmises aux serveurs DNS globaux, comme celles pour les adresses du RFC 1918, elles doivent être traitées par les serveurs du FAI (cf. le RFC 7793). Comme pour le RFC 1918, c'est sans doute un vœu pieux, et il faudra sans doute que l'AS112 (voir le RFC 7534) prenne en charge ces requêtes.

La section 3 décrit plus en détail les alternatives qui avaient été envisagées et les raisons de leur rejet. La solution la plus propre aurait évidemment été d'utiliser des adresses IPv4 globales, attribuées légitimement au FAI. Mais l'épuisement d'IPv4 rend cette solution irréaliste. Déjà, extraire un /10 des réserves n'a pas été facile.

La solution qui est probablement la plus utilisée à l'heure actuelle est celle d'utiliser un préfixe IPv4 usurpé, en se disant « de toute façon, ces adresses ne sortiront jamais sur l'Internet donc quel est le problème ? » Se servir sans demander est certainement plus rationnel, économiquement parlant, que de supplier la bureaucratie d'un RIR pour avoir des adresses. Autrefois, les FAI qui numérotaient ainsi leur réseau interne se servaient de préfixes non alloués (provoquant pas mal d'accidents au fur et à mesure de leur allocation ; même s'il n'y a pas de fuite de ces adresses, les abonnés du FAI peuvent être dans l'impossibilité de communiquer avec le détenteur légitime). Aujourd'hui, ils regardent quels sont les préfixes alloués mais non routés et les utilisent. Inutile de dire que le RFC condamne cette pratique incivique.

`https://www.bortzmeyer.org/6598.html`

Le RFC 1918 n'est, on l'a vu, possible que si le FAI contrôle complètement le réseau local de M. Li et sait donc quels préfixes sont utilisés sur celui-ci, et peut ainsi choisir des préfixes qui ne rentrent pas en collision. (Cela peut aussi marcher si la "*box*" sait bien se débrouiller lorsque le même préfixe est utilisé en interne et en externe, ce qui est le cas de certaines.)

Bref, l'allocation d'un nouveau préfixe semblait la seule solution raisonnable.

La section 5 du RFC est consacrée à une longue mise en garde sur les dangers associés aux CGN. Certaines applications peuvent avoir des mécanismes pour découvrir l'adresse externe de la machine sur laquelle l'application tourne (l'adresse qu'on verra sur l'Internet) et, ensuite, faire des choses comme de demander à un pair d'envoyer des données à cette adresse. Avec le CGN, cela a encore moins de chances de marcher que d'habitude car les applications actuelles ne connaissent pas encore `100.64.0.0/10` et considéreront que ces adresses sont globalement utilisables.

Parmi les applications qui ont de fortes chances de mal marcher dans le contexte du CGN, citons les jeux en ligne (si deux abonnés essaient de se connecter alors qu'ils sont derrière le même CGN et ont la même adresse publique), le pair-à-pair, et bien sûr les applications de téléphonie avec SIP, la géolocalisation (le CGN sera trouvé, pas la vraie machine), certaines applications Web qui restreignent les connexions simultanées en provenance de la même adresse IP, etc. Pour les applications de type pair-à-pair (échange de fichier, SIP), les techniques habituelles d'ouverture manuelle d'un port sur le routeur (« tout ce qui est envoyé au port 4554, transmets le à `10.4.135.21` ») ne marchent pas avec le CGN, l'utilisateur résidentiel n'ayant typiquement pas de moyen de configurer le routeur CGN.

Enfin, quelques bons conseils de sécurité forment la section 6 : ne pas accepter les annonces de route pour `100.64.0.0/10` à l'entrée d'un site, les paquets depuis ou vers ces adresses ne doivent pas franchir les frontières d'un opérateur, etc.

Voilà, comme indiqué, cela ne s'était pas passé tout seul et l'IESG avait même dû faire une longue note <`http://www.ietf.org/mail-archive/web/ietf-announce/current/msg09959.html`> détaillant le pourquoi de sa décision et expliquant que, certes, il n'y avait pas de consensus en faveur de ce projet mais qu'il n'y avait pas non plus de consensus contre. L'argument « pour » était :

— Les opérateurs vont déployer du CGN de toute façon. S'ils n'ont pas un préfixe dédié à cet usage, ils utiliseront des mauvaises méthodes, comme des préfixes squattés.

Les arguments contre étaient :

— Toute mesure qui prolonge au delà du raisonnable l'usage d'IPv4 ne fait que retarder le déploiement d'IPv6. Les efforts devraient se porter sur ce déploiement, pas sur l'acharnement thérapeuthique !

— Les opérateurs se serviront du nouveau préfixe pour étendre le RFC 1918, et pas pour l'usage attendu.

Pour d'autres articles sur ce sujet, voir celui sur le bon blog de Chris Grundemann <`http://chrisgrundemann.com/index.php/2012/100640010/`> (en anglais) ou bien celui de Jérôme Durand <`http://gblogs.cisco.com/fr-ipv6/2012/03/26/que-faire-du-prefixe-100-64-0-010/`> (en français).