

RFC 5684 : Unintended Consequence of NAT deployments with Overlapping Address Space

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 4 Février 2010

Date de publication du RFC : Février 2010

<http://www.bortzmeyer.org/5684.html>

Le NAT est depuis longtemps une des plaies de l'Internet. Justifié au début par le manque d'adresses IPv4, il est désormais de plus en plus utilisé en raison de l'épuisement des adresses v4 <<http://www.bortzmeyer.org/epuisement-adresses-ipv4.html>>, mais aussi sur des sites qui croient qu'il leur simplifie la vie, voire qu'il améliore leur sécurité. Une des conséquences du NAT tel qu'il est déployé pour IPv4 est que les adresses privées sont prises dans une réserve d'assez petite taille et qu'on voit désormais des cas de recouvrement d'adresses IP entre deux réseaux utilisant cette technique. Ce RFC décrit deux cas de cette catégorie.

L'utilisation « canonique » du NAT est avec un réseau local qui utilise des adresses privées du RFC 1918¹ et une seule adresse IP publique, attribuée par le FAI et affectée au routeur qui connecte le réseau local à l'Internet. Dans cette configuration (section 3.2.1), les limites et les problèmes du NAT sont bien connus. (Voir les RFC 2993, RFC 3424, RFC 5218, etc.) Mais, en raison du succès du NAT, on voit de plus en plus apparaître des configurations moins classiques, qui apportent de nouveaux problèmes.

L'Internet avait été prévu pour un espace d'adressage unique (section 1 du RFC), où chaque machine avait une adresse unique au monde. Le déploiement souvent irréfléchi du NAT a mené à une séparation Identificateur/Localisateur <<http://www.bortzmeyer.org/separation-identificateur-localisateur.html>> de fait (et mal faite) : désormais, il existe plusieurs machines sur l'Internet qui ont l'adresse 192.168.1.1.

Parmi les causes de ce déploiement du NAT :

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

pas un individu mais un FAI "low cost" qui fournit un service dégradé à ses clients (dont on espère qu'ils n'ont pas payé cher). Il ne leur donne pas une adresse IP publique, mais une privée dans 10.1.1.0/24 (notez que c'est le même préfixe que Bob : comme il n'y a pas d'allocation centrale des adresses privées, et que l'espace du RFC 1918 est très étroit, ce genre de collisions est fréquent). Des fournisseurs comme CheapoISP sont fréquents dans les pays du Sud, où il est très difficile d'obtenir des adresses IPv4 publiques (la fracture numérique passe aussi par là). Derrière CheapoISP, trois clients, Ann, Mary et Lex. Mary n'a qu'une machine mais Ann et Lex ont configuré, comme Bob, un petit routeur NAT qui alloue encore des adresses dans le préfixe 10.1.1.0/24. Aussi surprenant que cela puisse apparaître (après tout, les routeurs de Ann et Lex ont le même préfixe sur deux pattes), une telle configuration semble marcher à première vue : tout le monde peut regarder <http://www.cnn.com/> (section 3.1.1, sur le fonctionnement du client/serveur).

Les ennuis commencent avec le pair à pair (section 3.1.2). Comme plusieurs machines ont la même « identité », la même adresse IP, les communications pair-à-pair sont difficiles. D'abord, pour se trouver, les machines vont avoir besoin d'un serveur extérieur, qui va organiser les rendez-vous. Ensuite, même si les machines apprennent l'adresse IP d'une autre via ce serveur, elles ne pourront pas forcément la contacter, en raison de l'absence d'adresse unique. Par exemple, une machine pourra contacter, à la place du pair convoité, une autre machine de son réseau local, qui aura la même adresse IP que le pair qu'on veut joindre.

Ann et Lex ont même un problème supplémentaire, qui fait l'objet de la section 3.2.2 : il y a duplication des adresses IP. Plusieurs machines ont la même adresse, car l'allocation n'est pas coordonnée et l'espace du RFC 1918 étant très petit, les collisions sont inévitables. Si les routeurs d'Ann et de Lex tentent d'utiliser le classique ARP sur toutes leurs interfaces, ils peuvent obtenir des réponses différentes selon l'interface. Une telle configuration, qui marchera a priori (« Je peux voir YouTube », en raison du NAT) produira des phénomènes bizarres et difficilement explicables à première vue.

Le fait qu'il y ait plusieurs niveaux de NAT dans ces cas cause également d'autres surprises (section 3.2.3), comme le fait que les machines aux adresses privées peuvent communiquer avec l'Internet mais pas entre elles, même lorsqu'elles sont clientes du même FAI. Parfois, une communication est possible via le routeur NAT, si celui-ci permet les connexions « en épingle à cheveux » (où le paquet va au routeur de sortie puis tourne en épingle à cheveux pour revenir vers le réseau privé). Les RFC 4787 et RFC 5382 demandent qu'un tel routage soit possible.

Mais, même lorsque « ça marche », la configuration reste bancale. Ainsi, on ne peut plus utiliser l'adresse IP d'une machine, normalement unique <<http://www.bortzmeyer.org/loguer-adresse-et-port.html>>, comme **identité** (section 3.2.4). Cela fait que les paquets peuvent être transmis à la mauvaise machine. Le RFC donne l'exemple d'un résolveur DNS. S'il utilise des adresses privées et qu'un des réseaux locaux connectés utilise des adresses de la même plage, les machines de ce réseau ne pourront pas joindre leur résolveur. Le RFC recommande donc que les serveurs vitaux, comme le résolveur DNS, reçoivent toujours des adresses globales.

Un autre cas où des recouvrements des plages d'adresses IP peut se produire est celui des VPN, dans la section 4. Quelle que soit la technologie utilisée pour les réaliser (IPsec, L2TP, etc), le VPN donne accès à un réseau dont les adresses sont souvent privées. Si, sur son réseau d'attachement physique, le client VPN utilise également des adresses privées, le risque de collision est important. Un exemple que cite le RFC en section 4.2.1 est celui où le serveur DHCP du réseau local de la machine cliente a la même adresse (privée...) qu'une machine du réseau distant. Au moment de renouveler le bail DHCP, les paquets iront sur le site distant et pas sur le réseau local... Le RFC recommande donc que les paquets à destination des adresses IP du serveur DHCP et du premier routeur ne soient jamais envoyées à travers le VPN, même dans le cas où celui-ci est configuré pour faire passer la totalité du trafic, ce qu'on nomme le "non-split VPN", et qui est souvent préféré pour des raisons de sécurité. Le RFC conseille aussi de

garder la possibilité du *"split VPN"* (où seul les paquets à destination du réseau de l'entreprise sont routés via le VPN), qui limite les risques de collision.

La section 5 reprend et résume les recommandations de notre RFC 5684. Elles viennent en sus de celles des RFC 4787, RFC 5382 et RFC 5508. Si elles sont suivies, les conséquences de l'adressage privé seront minimisées.

Si elles ne le sont pas, plusieurs accidents auront lieu, parfois avec des conséquences néfastes pour la sécurité (section 7), comme l'envoi de paquets à une machine autre que celle à qui ils étaient normalement destinés. Le RFC conseille de toute façon d'avoir également une authentification forte et de ne pas se fier uniquement à l'adresse IP source.

Ah, un dernier conseil, personnel : pour limiter le risque de collisions lorsque vous utilisez des adresses RFC 1918, n'utilisez pas le début des plages. Pour vous éloigner des autres, numérotez avec un numéro « haut », choisi au hasard, par exemple avec 10.198.200.0/22 ou 10.243.24.0/22 plutôt qu'avec le banal 10.1.0.0/24 que tout le monde utilise...