RFC 6269 : Issues with IP Address Sharing

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 29 juin 2011

Date de publication du RFC : Juin 2011

http://www.bortzmeyer.org/6269.html

Pour pas mal de raisons, il est fréquent aujourd'hui qu'une adresse IP soit partagée entre plusieurs machines. Le cas le plus typique est celui des N machines d'une petite entreprise, forcées d'utiliser une seule adresse IP publique, via un routeur NAT. Ce RFC est le premier document qui discute en détail de ce **partage d'adresses**, et de ses innombrables inconvénients.

Le RFC met surtout l'accent (section 1) sur une cause du partage d'adresses : l'épuisement de la réserve d'adresses IPv4 <http://www.bortzmeyer.org/epuisement-adresses-ipv4.html>, qui, n'étant pas compensée par un déploiement massif d'IPv6, mène à ce que le partage d'adresses soit très fréquent, et le sera sans doute davantage dans le futur (la plupart des solutions d'attente d'IPv6 utilisent intensivement ce partage). En fait, aujourd'hui, il est rare que M. Michu puisse bénéficier d'une vraie connexion Internet : il partage en général son adresse avec d'autres M. Michu ; par exemple, à la maison, M. Michu n'a aucune chance d'obtenir plus d'une adresse IPv4, même si plusieurs personnes vivent dans ce foyer et utilisent toutes des appareils connectés à l'Internet (ce qui est banal aujourd'hui dans les grandes villes du Nord). Le CPE fait office de routeur NAT et les machines de M. Michu et de sa petite famille sont contraintes de se contenter d'adresses IP privées (RFC 1918 [1]). Mais l'avenir (déjà réalisé en Europe sur les connexions ultra-civilisées de la 3G, et, en Asie, dès à présent sur toutes les connexions) nous réserve pire : le partage d'adresses IP, non pas au sein du foyer ou de la petite entreprise, mais entre abonnés, ce qu'on nomme parfois le CGN, pour "*Carrier-Grade NAT*" et qu'on pourrait qualifier de « partage d'adresses généralisé ». (L'annexe A résume les différents types de partage d'adresses.) Le « facteur multiplicatif » (annexe B) entre le nombre d'adresses privées et celui d'adresses publiques vaut typiquement entre 3 et 10 pour une maison européenne typique (une seule adresse publique mais plusieurs machines connectées, "*smartphones*", ordinateurs, consoles de jeu, etc). Il pourrait dépasser 1000 avec les CGN (plusieurs adresses IP publiques mais des milliers d'abonnés se partageant ce mince gâteau).

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

Le RFC insiste sur le fait que le déploiement d'IPv6 est la seule solution correcte aux problèmes engendrés par le partage d'adresses. C'est vrai mais il faut noter que le partage d'adresses a commencé bien avant la famine, qu'il est pratiqué par des entreprises qui disposent de suffisamment d'adresses IPv4 (en général au nom de pseudo-arguments de « sécurité ») et qu'on le trouve pratiqué massivement en Afrique et en Asie alors que le continent africain est celui qui a la plus grande réserve d'adresses IPv4 officielles disponibles. Donc, le non-déploiement d'IPv6 n'est pas la seule raison de l'utilisation du partage d'adresses.

J'ai mentionné le NAT tout à l'heure. Si le partage d'adresses se fait en général (mais pas toujours) via le NAT, l'inverse n'est pas forcément vrai. On peut avoir du NAT sans partage d'adresses, si chaque adresse interne est mise en correspondance avec une et une seule adresse externe. Évidemment, en IPv4, c'est rare, vu le manque d'adresses, mais cela sera peut-être plus fréquent avec IPv6 <http://www.bortzmeyer.org/nats.html>.

À noter que ce RFC ne discute que du problème : il ne propose pas de solution, celles-ci étant renvoyées à des documents ultérieurs (qui ne seront peut-être pas nécessaire si le déploiement d'IPv6 rend inutile ces solutions). Il ne se penche pas non plus sur les problèmes qui sont spécifiques à une technique utilisant le partage d'adresses, essayant au contraire de voir les questions communes à toutes ces techniques. Ainsi, qu'on utilise, pour gérer le passé en attendant le déploiement d'IPv6, NAT64, DS-Lite ou encore d'autres importe peu : toutes ont en commun les même défauts liés au partage d'adresses.

Des problèmes, notamment de sécurité, liés au partage d'adresses avaient déjà été discutés dans les RFC sur le NAT comme les RFC 2663 et RFC 2993 (section 2 de notre RFC). Mais le partage généralisé, entre utilisateurs n'ayant rien en commun, va aggraver ces problèmes. Cette situation se rencontre souvent aujourd'hui en Asie, et dans les "*hotspots WiFi publics*". Mais elle sera hélas sans doute demain le lot de beaucoup d'utilisateurs.

Bien, arrivé à ce stade, vous avez le droit de penser que j'ai beaucoup répété qu'il y avait des problèmes, sans dire lesquels. Patientez encore un peu. L'analyse des problèmes qui commence en section 3 est faite en cherchant d'abord si le problème affecte l'organisation qui déploie le partage d'adresses (et donc ses abonnés ou employés), ou bien des tiers (comme la police par exemple ou bien comme un CDN qui essaie de distribuer du contenu en fonction de l'adresse). Le tout est stocké dans un grand tableau synthétique (figure n° 1) et détaillé dans les sections suivantes. Pour ne prendre que trois exemples de ce tableau, le fait que les requêtes DNS traduisant une adresse en nom perdent de leur signification affecte aussi bien l'utilisateur que les tiers (ceux qui traduisent une adresse IP entrante en nom). Par contre, la perte de traçabilité qui résulte du partage (si on détecte un comportement illégal lié à une adresse IP, on ne retrouve plus facilement la machine en cause) n'affecte que les tiers (les organisations répressives comme la HADOPI). Au contraire, la perte de fiabilité de la connexion (car l'engin qui fait les traductions d'adresses est un nouveau composant dans la connexion, qui peut avoir des bogues ou des pannes, cf. section 18) ne concerne que l'utilisateur, les tiers ne seront pas touchés.

Les sections suivantes du RFC détaillent successivement chacun de ces problèmes (je ne les présente pas dans l'ordre, j'essaie de mettre les plus importantes en premier). La section 5 s'attaque aux problèmes liés à l'allocation de port. Avec le partage d'adresses, plusieurs adresses « internes » sont mises en correspondance avec une seule adresse « externe ». Comment, dans ces conditions, différencier les paquets IP qui arrivent, à destination de cette adresse IP externe ? On utilise le numéro de port TCP ou UDP pour cela et c'est donc le couple {adresse, port} qui identifie la machine et non plus l'adresse seule. Ce numéro de port n'étant stocké que sur 16 bits, cela met une limite stricte à l'ampleur du partage. Si 500 machines partagent une adresse (facteur multiplicatif de 500), cela ne fait qu'un peu plus de 131 ports chacune (et même moins car certains doivent être réservés, cf. RFC 4787), ce qui est vite épuisé sur une machine un tant soit peu active, qui ouvre de nombreuses connexions (une seule page Web peut se traduire par l'ouverture de dizaines de connexions). D'autant plus que ce n'est pas le nombre de

connexions actives qui compte, mais celui des connexions TCP dans l'état `TIME-WAIT`, celui dans lequel les connexions fermées restent pendant quatre minutes (RFC 1337).

Voyons les ports « sortants », ceux alloués pour les connexions initiées de l'intérieur (section 5.1). Les études (Alcock, S., « "*Research into the Viability of Service-Provider NAT*" `<http://www.wand.net.nz/~salcock/someisp/flow_counting/result_page.html>` ») semblent indiquer que la distribution de la consommation est très inégale : une minorité d'utilisateurs consomme beaucoup de ports. Cela encourage à répartir les numéros de port à partir d'un "*pool*" central, et pas à attribuer de manière fixe des plages de ports à chaque client (cf. annexe A). Mais la seconde solution serait bien plus simple et moins coûteuse. Et la première est vulnérable à une attaque DoS : une seule machine infectée par du "*malware*" et qui ouvre des connexions le plus vite possible peut épuiser le "*pool*". Ceci dit, l'allocation statique de plages de ports a aussi ses risques (cf. RFC 6056). Tous ces problèmes existaient avec le partage limité à un foyer ou une entreprise mais sont évidemment plus graves en cas de partage généralisé puisqu'un utilisateur peut être bloqué par un autre utilisateur qu'il ne connait pas.

Et pour les ports des connexions entrantes (section 5.2) ? L'étude citée ci-dessus montre qu'elles sont fréquentes (la majorité des utilisateurs) mais consomment moins de ports. Comment négocier entre la machine de l'utilisateur et le routeur NAT l'allocation d'un port « entrant » ? Aujourd'hui, les méthodes les plus courantes sont l'allocation manuelle (la plupart des CPE permettent de configurer des ports entrants, du genre « toute connexion arrivant pour le port 80 de l'adresse publique doit être traduite vers `192.168.1.13:8080` ») ou bien un protocole comme UPnP. Le CGN complique sérieusement les choses puisqu'il n'est pas dédié à un utilisateur et qu'on doit donc sérieusement étudier sa sécurité avant de permettre à un utilisateur de se réserver les ports 22 ou 80 ! C'est encore pire si le CPE et le CGN doivent coopérer pour rendre le service, puisqu'il n'existe aucun protocole standard pour cela. Actuellement, sur l'abonnement 3G typique en Europe, on n'a pas accès à l'allocation de ports entrants et le "*smartphone*" ne peut donc pas héberger de serveur. Cet engin bien plus puissant que les ordinateurs des débuts de l'Internet est donc limité à un rôle de Minitel plus perfectionné.

Il existe des solutions potentielles à ces problèmes mais aucune n'est vraiment satisfaisante. À titre d'exemple, le RFC cite les enregistrements SRV qui pourraient permettre de faire savoir que tel service réside sur tel port de la machine coincée derrière le partage d'adresses. Parmi les limites de cette solution, notons qu'elle ne s'applique pas au protocole le plus demandé, HTTP, qui n'utilise pas les SRV...

Jusqu'à présent, j'ai surtout parlé du problème des applications « serveur », celles qui écoutent des connexions inattendues sur un port bien connu, un serveur SSH, par exemple. On peut se dire que de tel cas sont rares sur la machine de M. Michu, qui n'installe en général pas de serveur SSH, ni même HTTP. Mais il y a toute une catégorie d'applications qui a besoin d'écouter des connexions entrantes sans être pour autant un « serveur » à proprement parler. La section 6 est une bonne occasion de les mentionner. En effet, cette section examine tous les cas où le partage d'adresses gène les applications. Cela concerne bien sûr les serveurs traditionnels, vus en section 5.2, mais aussi, entre autres :

— Les applications qui indiquent des adresses et des ports dans leur trafic, ce qui concerne typiquement FTP et SIP. Un ALG sera nécessaire pour les gérer.
— Les applications qui n'utilisent pas du tout de port (ping...) et pour qui il faut donc trouver d'autres moyens de démultiplexage. Une section entière, la 9, détaille les problèmes posés à ICMP, puisque ce protocole n'a pas de notion de port. Outre ping, ce protocole est utilisé, par exemple par les applications pair-à-pair pour mesurer la « distance » avec un pair, ce qui ne marche plus dans le cas d'un partage généralisé.
— Un cas analogue est celui des applications qui n'utilisent pas TCP ou UDP, mais, par exemple, SCTP ou encore le protocole 41 (encapsulation IPv6 dans IPv4, pour gérer le cas des réseaux qui n'ont toujours pas IPv6). Très rares sont les techniques de partage d'adresses qui gèrent d'autres protocoles que TCP et UDP. Ces techniques contribuent donc à l'ossification de l'Internet (la grande difficulté à déployer de nouveaux protocoles).

— Les applications qui tiennent pour acquise l'unicité des adresses IP (voir aussi le RFC 6250). Par exemple, une application Web qui lie les "*cookies*" à une adresse IP, pour augmenter la sécurité, n'a pas de sens si cette adresse est partagée entre des dizaines d'utilisateurs qui ne se font pas forcément confiance.

Résultat, les applications passent aujourd'hui beaucoup de temps à mettre en œuvre des techniques de contournement, cherchant à récupérer leur connectivité que le NAT contrarie. Il suffit de regarder le code source de n'importe quelle application de téléphonie sur l'Internet pour voir le résultat : le code est plus complexe, et dépend de systèmes difficiles comme ICE (RFC 5245). Avis personnel : il est donc faux de dire que le NAT fait faire des économies. Le NAT est un **déplacement de coûts**, depuis les administrateurs réseaux vers les développeurs d'applications, contraints à des prodiges d'astuces pour assurer la connectivité.

Un des principaux problèmes que pose fondamentalement le partage d'adresses est la traçabilité (notez que ce n'est pas un problème pour tout le monde). Il est fréquent de suivre les actions d'une machine et de son propriétaire via l'adresse IP. `192.0.2.66` s'est connecté à `www.anonymous.org`. `203.0.113.13` a envoyé du spam. `198.51.100.254` a participé à une attaque DoS. Évidemment, si les adresses IP sont partagées, cette traçabilité n'existe plus. Aujourd'hui, avec le NAT local classique, on peut au moins relier une adresse IP à un foyer ou une entreprise. Avec du partage d'adresses généralisé, cela ne sera plus le cas (section 12). Actuellement, une requête de la police auprès d'un FAI pour obtenir l'identité d'un abonné dont la machine s'est fait repérer inclus l'adresse IP et l'heure (pour les cas d'adresses IP dynamiques, changeant régulièrement). Le partage généralisé oblige à inclure d'autres informations dans la requête, comme le numéro de port <`http://www.bortzmeyer.org/loguer-adresse-et-port.html`>, que peu de serveurs enregistrent aujourd'hui. Attention, identifier un abonné à partir du couple {adresse IP, port} est délicat, car la table de correspondance change bien plus vite que les baux DHCP typiques. La requête doit donc inclure une heure très précise et, pour cela, s'appuyer sur une horloge bien synchronisée. Comme cela risque de ne pas suffire (et cette solution implique que le serveur enregistre le numéro de port source, ce qui est inhabituel aujourd'hui), faudra t-il que le routeur NAT enregistre également l'adresse IP de destination ? Cela étendrait le domaine du flicage très loin...

Et le FAI doit garder des journaux de taille colossale pour pouvoir répondre aux questions comme « Qui utilisait le couple {`198.51.100.254`, 23152} le 23 mai à 11 :28 :05 ? », les obligations légales de surveillance imposant en général de conserver ces données pendant six à douze mois. Cela ne sera probablement pas réaliste pour tous les FAI, sauf à créer des obligations légales qui acculeraient bien des opérateurs à la faillite. Noter l'adresse IP de destination aggraverait évidemment le problème.

Comment cela va t-il se passer alors ? Une solution est de baisser les bras et de ne pas divulguer l'identité de l'abonné. Cela peut poser des problèmes légaux au FAI, des lois comme la LCEN en France leur faisant obligation de surveiller leurs abonnés, comme un hôtelier des vieux films policiers surveillait les entrées et sorties de ses clients. Une autre solution est de divulguer les coordonnées de tous les abonnés qui avaient une session active à ce moment là et de laisser la police trier. On imagine le nombre d'innocents qui seront alors harcelés.

À noter que la situation décrite par cette section 12 ne sera pas forcément perçue comme un problème par tout le monde. Ainsi, certains utilisateurs pourraient trouver des avantages à un système qui rend plus compliquée la tâche des surveillants. Si, à cause du partage d'adresses, une société privée de surveillance comme TMG, qui collecte les adresses IP de partageurs de fichiers, a des problèmes, tant mieux, se diront-ils. Le partage d'adresses pourrait alors fournir, sinon l'anonymat, au moins un certain brouillage de pistes. Ce n'est pas faux mais c'est à mettre en rapport avec les inconvénients de ce partage d'adresses.

Le partage d'adresses perturbe une mesure importante pour le bon fonctionnement de l'Internet, celle de la MTU du chemin (section 10). Bien des systèmes mesurent cette MTU du chemin (RFC 1191)

pour optimiser le transfert de données. Mais cette PMTU est en général stockée par adresse IP et le partage généralisé peut donc fausser les mesures : deux machines derrière la même adresse IP peuvent ne pas avoir la même PMTU. Cela peut permettre des attaques par déni de service où une des machines derrière l'adresse publique générerait des paquets ICMP `packet too big` (type 3 et code 4 d'ICMP) indiquant une taille ridiculement basse... qui sera utilisée pour tous les malheureux situés derrière la même adresse.

Il y a d'autres questions de sécurité liées au partage d'adresses. La section 13 les expose successivement. Par exemple, bien des mesures de sécurité sont prises sur la base de l'adresse IP. Un exemple est le logiciel fail2ban qui met automatiquement en liste noire (et donc filtre) les adresses IP qui sont à l'origine de comportements agressifs (comme des connexions SSH répétées). Si cette adresse IP est partagée, des innocents vont aussi se voir bloquer l'accès. Même chose pour les listes noires des expéditeurs de spam.

Des problèmes peuvent également survenir avec des logiciels qui estiment qu'une adresse IP identifie une machine (section 14). Un des exemples est l'optimisation TCP du RFC 2140, qui consiste à partager l'information entre toutes les connexions TCP vers la même machine. Cette optimisation ne fonctionnera plus si la même adresse IP sert à des machines connectées de manière très différente (avec le NAT résidentiel d'aujourd'hui, ce n'est pas trop un problème car toutes les machines de la même maison ont à peu près la même connectivité).

Autre conséquence négative du partage d'adresses : la géolocalisation (section 7). Les adresses IP sont souvent utilisées pour donner une idée (fort imparfaite) de la localisation d'une machine. C'est un système très contestable, déjà aujourd'hui, comme le note le RFC. Mais le partage généralisé d'adresses le rendra encore moins utile, puisque c'est l'adresse du routeur CGN qui sera vue par le serveur, et qu'elle peut n'avoir qu'un très lointain rapport avec le client. Bon, personnellement, je trouve qu'on en arrive à un fort niveau de pinaillage ici : les problèmes posés par le partage d'adresses sont assez graves pour qu'on ne charge pas la barque en mentionnant des conséquences négatives sur un système qui était déjà mal fichu, comme la géolocalisation. Même remarque pour la section 8, qui fait remarquer que le partage généralisé empêchera de compter le nombre d'utilisateurs uniques en comptant le nombre d'adresses IP - ce qui est déjà largement le cas, ou la 11 qui note que le fait d'utiliser le numéro de port pour démultiplexer les paquets arrivant dans le routeur NAT pose un problème avec la fragmentation, puisque seul le premier fragment contient le numéro de port.