RFC 9099 : Operational Security Considerations for IPv6 Networks

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 7 septembre 2021

Date de publication du RFC : Août 2021

https://www.bortzmeyer.org/9099.html

Tous les gens qui gèrent des réseaux IPv4 savent comment les sécuriser (normalement...). Et pour IPv6 ? Si ce n'est pas un protocole radicalement différent, il a quand même quelques particularités de sécurité. Ce RFC donne des conseils pratiques et concrets sur la sécurisation de réseaux IPv6. (Je le répète, mais c'est juste une nouvelle version d'IP : l'essentiel du travail de sécurisation est le même en v4 et en v6.)

Les différences entre IPv4 et IPv6 sont subtiles (mais, en sécurité, la subtilité compte, des petits détails peuvent avoir de grandes conséquences). Ceci dit, le RFC a tendance à les exagérer. Par exemple, il explique que la résolution d'adresses de couche 3 en adresses de couche 2 ne se fait plus avec ARP (RFC 826 [1]) mais avec NDP (RFC 4861). C'est vrai, mais les deux protocoles fonctionnent de manière très proche et ont à peu près les mêmes propriétés de sécurité (en l'occurrence, aucune sécurité). Plus sérieusement, le remplacement d'un champ d'options de taille variable dans IPv4 par les en-têtes d'extension d'IPv6 a certainement des conséquences pour la sécurité. Le RFC cite aussi le cas du NAPT ("*Network Address and Port Translation*", RFC 2663). Souvent appelée à tort NAT (car elle ne traduit pas que l'adresse mais également le port), cette technique est très utilisée en IPv4. En IPv6, on ne fait pas de traduction ou bien on fait du vrai NAT, plus précisement du NPT ("*Network Prefix Translation*", RFC 6296) puisqu'on change le préfixe de l'adresse. La phrase souvent entendue « en IPv6, il n'y a pas de NAT » est doublement fausse : c'est en IPv4 qu'on n'utilise pas le NAT, mais le NAPT, et on peut faire de la traduction d'adresses en IPv6 si on veut. NAT, NAPT ou NPT ne sont évidemment pas des techniques de sécurité <https://www.bortzmeyer.org/nat-et-securite.html> mais elles peuvent avoir des conséquences pour la sécurité. Par exemple, toute traduction d'adresse va complexifier le réseau, ce qui introduit des risques. Autre facteur nouveau lié à IPv6 : la plupart des réseaux vont devoir faire de l'IPv4 **et** de l'IPv6 et les différentes techniques de coexistence de ces deux versions peuvent avoir leur propre impact sur la sécurité (RFC 4942).

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc826.txt

La section 2 du RFC est le gros morceau du RFC ; c'est une longue liste de points à garder en tête quand on s'occupe de la sécurité d'un réseau IPv6. Je ne vais pas tous les citer, mais en mentionner quelques-uns qui donnent une bonne idée du travail du ou de la responsable de la sécurité.

D'abord, l'adressage. Aux débuts d'IPv6, l'idée était que les spécificités d'IPv6 comme le SLAAC allaient rendre la renumérotation des réseaux tellement triviale qu'on pourrait changer les adresses souvent. En pratique, ce n'est pas tellement le cas (RFC 7010) et il faut donc prêter attention à la conception de son adressage : on aura du mal à en changer. Heureusement, c'est beaucoup plus facile qu'en IPv4 : l'abondance d'adresses dispense des astuces utilisées en IPv4 pour essayer d'économiser chaque adresse. Par exemple, on peut donner à tous ses sous-réseaux la même longueur de préfixe, quelle que soit leur taille, ce qui simplifie bien les choses (le RFC 6177 est une lecture instructive). Comme en IPv4, les adresses peuvent être liées au fournisseur d'accès (PA, "*Provider Allocated*") ou bien obtenues indépendamment de ce fournisseur (PI, "*Provider Independent*"). Le RFC 7381 discute ce cas. Cela peut avoir des conséquences de sécurité. Par exemple, les adresses PA sont en dernier ressort gérées par l'opérateur à qui il faudra peut-être demander certaines actions. Et ces adresses PA peuvent pousser à utiliser la traduction d'adresses, qui augmente la complexité. (D'un autre côté, les adresses PI sont plus difficiles à obtenir, surtout pour une petite organisation.) Ah, et puis, pour les machines terminales <https://www.bortzmeyer.org/terminal-host.html>, le RFC 7934 rappelle à juste titre qu'il faut autoriser ces machines à avoir plusieurs adresses (il n'y a pas de pénurie en IPv6). Une des raisons pour lesquelles une machine peut avoir besoin de plusieurs adresses est la protection de la vie privée (RFC 8981).

Les gens habitués à IPv4 demandent souvent quel est l'équivalent du RFC 1918 en IPv6. D'abord, de telles adresses privées ne sont pas nécessaires en IPv6, où on ne manque pas d'adresses. Mais si on veut, on peut utiliser les ULA ("*Unique Local Addresses*") du RFC 4193. Par rapport aux adresses privées du RFC 1918, elles ont le gros avantage d'être uniques, et donc d'éviter toute collision, par exemple quand deux organisations fusionnent leurs réseaux locaux. Le RFC 4864 décrit comment ces ULA peuvent être utilisés pour la sécurité.

Au moment de concevoir l'adressage, un choix important est celui de donner ou non des adresses IP stables aux machines. (Ces adresses stables peuvent leur être transmises par une configuration statique, ou bien en DHCP.) Les adresses stables facilitent la gestion du réseau mais peuvent faciliter le balayage effectué par un attaquant pendant une reconnaissance préalable. Contrairement à ce qu'on lit parfois encore, ce balayage est tout à fait possible en IPv6, malgré la taille de l'espace d'adressage, même s'il est plus difficile qu'en IPv4. Le RFC 7707 explique les techniques de balayage IPv6 possibles. Même chose dans l'article « "*Mapping the Great Void*" <http://www.caida.org/workshops/isma/1202/slides/aims1202_rbarnes.pdf> ». Bref, on ne peut pas compter sur la STO et donc, adresses stables ou pas, les machines connectées à l'Internet peuvent être détectées, et doivent donc être défendues.

Cela n'empêche pas de protéger la vie privée des utilisateurs en utilisant des adresses temporaires pour contacter l'extérieur. L'ancien système de configuration des adresses par SLAAC était mauvais pour la vie privée puisqu'il utilisait comme partie locale de l'adresse (l'IID, "*Interface IDentifier*") l'adresse MAC, ce qui permettait d'identifier une machine même après qu'elle ait changé de réseau. Ce système est abandonné depuis longtemps (RFC 8064) au profit d'adresses aléatoires (RFC 8981). Ceci dit, ces adresses aléatoires posent un autre problème : comme elles changent fréquemment, elles ne permettent pas à l'administrateur réseau de suivre les activités d'une machine (c'est bien leur but), et on ne peut plus utiliser de mécanismes comme les ACL. Une solution possible est d'utiliser des adresses qui sont stables pour un réseau donné mais qui ne permettent pas de suivre une machine quand elle change de réseau, les adresses du RFC 7217. C'est dans beaucoup de cas le meilleur compromis. (Le RFC 7721 contient des détails sur les questions de sécurité liées aux adresses IP.)

On peut aussi couper SLAAC (cela peut se faire à distance avec des annonces RA portant le bit M) et n'utiliser que DHCP mais toutes les machines terminales n'ont pas un client DHCP.

En parlant de DHCP, lui aussi pose des problèmes de vie privée (décrits dans le RFC 7824) et si on veut être discret, il est recommandé d'utiliser le profil restreint défini dans le RFC 7844.

Après les adresses, la question des en-têtes d'extension, un concept nouveau d'IPv6. En IPv4, les options sont placées dans l'en-tête, qui a une longueur variable, ce qui complique et ralentit son analyse. En IPv6, l'en-tête a une longueur fixe (40 octets) mais il peut être suivi d'un nombre quelconque d'en-têtes d'extension (RFC 8200, section 4). Si on veut accéder à l'information de couche 4, par exemple pour trouver le port TCP, il faut suivre toute la chaîne d'en-têtes. Ce système était conçu pour être plus facile et plus rapide à analyser que celui d'IPv4, mais à l'usage, ce n'est pas le cas `<https://www.bortzmeyer.org/analyse-pcap-ipv6.html>` (le RFC estime même que le système d'IPv6 est pire). En partie pour cette raison, certains nœuds intermédiaires jettent tous les paquets IPv6 contenant des en-têtes d'extension (RFC 7872, RFC 9288). D'autres croient que la couche Transport suit immédiatement l'en-tête, sans tenir compte de la possibilité qu'il y ait un en-tête d'extension, ce qui fausse leur analyse. L'en-tête d'extension "*Hop-by-hop options*" était particulièrement problématique, car devant être traité par tous les routeurs (le RFC 8200 a adouci cette règle).

Pour faciliter la tâche des pare-feux, plusieurs règles ont été ajoutées aux en-têtes d'extension depuis les débuts d'IPv6 : par exemple le premier fragment d'un datagramme doit contenir la totalité des en-têtes d'extension.

À l'interface d'IPv6 et de la couche 2, on trouve quelques problèmes supplémentaires. D'abord, concernant la résolution d'adresses IP en adresses MAC, pour laquelle IPv6 utilise le protocole NDP ("*Neighbor Discovery Protocol*", RFC 4861). NDP partage avec ARP un problème fondamental : n'importe quelle machine du réseau local peut répondre ce qu'elle veut. Par exemple, si une machine demande « qui est `2001:db8:1::23:42:61` ? », toutes les machines locales peuvent techniquement répondre « c'est moi » et donner leur adresse MAC. Ce problème et quelques autres analogues sont documentés dans les RFC 3756 et RFC 6583. DHCP pose le même genre de problèmes, toute machine peut se prétendre serveur DHCP et répondre aux requêtes DHCP à la place du serveur légitime. Pour se prémunir contre les attaques faites par des machines envoyant de faux RA, on peut aussi isoler les machines, par exemple en donnant un /64 à chacune, ou bien en configurant commutateurs ou points d'accès Wifi pour bloquer les communications de machine terminale à machine terminale (celles qui qui ne sont pas destinées au routeur). Le RFC recommande le "*RA guard*" du RFC 6105.

Et sur les mobiles ? Un lien 3GPP est un lien point-à-point, l'ordiphone qui est à un bout ne peut donc pas parler aux autres ordiphones, même utilisant la même base. On ne peut parler qu'au routeur (GGSN - "*GPRS Gateway Support Node*", ou bien PGW - "*Packet GateWay*"). Pour la même raison, il n'y a pas de résolution des adresses IP et donc pas de risque liés à cette résolution. Ce mécanisme empêche un grand nombre des attaques liées à NDP. Si vous voulez en apprendre plus à ce sujet, il faut lire le RFC 6459.

Le "*multicast*" peut être dangereux sur un réseau local, puisqu'il permet d'écrire à des machines qui n'ont rien demandé. Certains réseaux WiFi bloquent le "*multicast*". En IPv6, cela empêche des actions néfastes comme de pinguer `ff01::1` (l'adresse "*multicast*" qui désigne toutes les machines du réseau local), mais cela bloque aussi des protocoles légitimes comme mDNS (RFC 6762).

Compte-tenu de la vulnérabilité du réseau local, et des risques associés, il a souvent été proposé de sécuriser l'accès à celui-ci et IPv6 dispose d'un protocole pour cela, SEND, normalisé dans le RFC 3971, combiné avec les CGA du RFC 3972. Très difficile à configurer, SEND n'a connu aucun succès, à part dans quelques environnements ultra-sécurisés. On ne peut clairement pas compter dessus.

Voyons maintenant la sécurité du plan de contrôle : les routeurs et le routage (RFC 6192). Les problèmes de sécurité sont quasiment les mêmes en IPv4 et en IPv6, la principale différence étant le mécanisme d'authentification pour OSPF. Un routeur moderne typique sépare nettement le plan de contrôle (là où on fait tourner les protocoles comme OSPF, mais aussi les protocoles de gestion comme SSH qui sert à configurer le routeur) et le plan de transmission, là où se fait la transmission effective des paquets. Le second doit être très rapide, car il fonctionne en temps réel. Il utilise en général du matériel spécialisé, alors que le plan de contrôle est la plupart du temps mis en œuvre avec un processeur généraliste, et un système d'exploitation plus classique. Pas toujours très rapide, il peut être submergé par un envoi massif de paquets. Le plan de contrôle ne gère que les paquets, relativement peu nombreux, qui viennent du routeur ou bien qui y arrivent, le plan de transmission gérant les innombrables paquets que le routeur transmet, sans les garder pour lui. Chaque paquet entrant est reçu sur l'interface d'entrée, le routeur consulte une table qui lui dit quel est le routeur suivant pour ce préfixe IP, puis il envoie ce paquet sur l'interface de sortie. Et le tout très vite.

Notre RFC conseille donc de protéger le plan de contrôle en bloquant le plus tôt possible les paquets anormaux, comme des paquets OSPF qui ne viendraient pas d'une adresse locale au lien, ou les paquets BGP qui ne viennent pas d'un voisin connu. (Mais, bien sûr, il faut laisser passer l'ICMP, essentiel au débogage et à bien d'autres fonctions.) Pour les protocoles de gestion, il est prudent de jeter les paquets qui ne viennent pas du réseau d'administration. (Tout ceci est commun à IPv4 et IPv6.)

Protéger le plan de contrôle, c'est bien, mais il faut aussi protéger le protocole de routage. Pour BGP, c'est pareil qu'en IPv4 (lisez le RFC 7454). Mais OSPF est une autre histoire. La norme OSPFv3 (RFC 4552) comptait à l'origine exclusivement sur IPsec, dont on espérait qu'il serait largement mis en œuvre et déployé. Cela n'a pas été le cas (le RFC 8504 a d'ailleurs supprimé cette obligation d'IPsec dans IPv6, obligation qui était purement théorique). Le RFC 7166 a pris acte de l'échec d'IPsec en créant un mécanisme d'authentification pour OSPFv3. Notre RFC recommande évidemment de l'utiliser.

Sinon, les pratiques classiques de sécurité du routage tiennent toujours. Ne pas accepter les routes « *"bogons"* <https://team-cymru.com/community-services/bogon-reference/> » (conseil qui n'est plus valable en IPv4, où tout l'espace d'adressage a été alloué), celles pour des adresses réservées (RFC 8190), etc.

Pas de sécurité sans surveillance (c'est beau comme du Ciotti, ça) et journalisation. En IPv6 comme en IPv4, des techniques comme IPFIX (RFC 7011), SNMP (RFC 4293), etc sont indispensables. Comme en IPv4, on demande à son pare-feu, son serveur RADIUS (RFC 2866) et à d'autres équipements de journaliser les évènements intéressants. À juste titre, et même si ça va chagriner les partisans de la surveillance massive, le RFC rappelle que, bien que tout cela soit très utile pour la sécurité, c'est dangereux pour la vie privée, et que c'est souvent, et heureusement, encadré par des lois comme le RGPD. Administrateur réseaux, ne journalise pas tout, pense à tes responsabilités morales et légales !

Bon, mais cela, c'est commun à IPv4 et IPv6. Qu'est-ce qui est spécifique à IPv6 ? Il y a le format textuel canonique des adresses, normalisé dans le RFC 5952, qui permet de chercher une adresse sans ambiguité. Et la mémoire des correspondances adresses IP adresses MAC dans les routeurs ? Elle est très utile à enregistrer, elle existe aussi en IPv4, mais en IPv6 elle est plus dynamique, surtout si on utilise les adresses favorables à la vie privée du RFC 8981. Le RFC recommande de la récupérer sur le routeur au moins une fois toutes les 30 secondes. Et le journal du serveur DHCP ? Attention, en IPv6, du fait de l'existence de trois mécanismes d'allocation d'adresses (DHCP, SLAAC et statique) au lieu de deux en IPv4, le journal du serveur DHCP ne suffit pas. Et puis il ne contiendra pas l'adresse MAC mais un identificateur choisi par le client, qui peut ne rien vous dire. (Ceci dit, avec les machines qui changent leur adresse MAC, DHCPv4 a un problème du même genre.) En résumé, associer une adresse IP à une machine risque d'être plus difficile qu'en IPv4.

Une autre spécificité d'IPv6 est l'existence de nombreuses technologies de transition entre les deux protocoles, technologies qui apportent leurs propres problèmes de sécurité (RFC 4942). Normalement, elles n'auraient dû être que temporaires, le temps que tout le monde soit passé à IPv6 mais, comme vous le savez, la lenteur du déploiement fait qu'on va devoir les supporter longtemps, les réseaux purement IPv6 et qui ne communiquent qu'avec d'autres réseaux IPv6 étant une petite minorité. La technique de coexistence la plus fréquente est la double pile, où chaque machine a à la fois IPv4 et IPv6. C'est la plus simple et la plus propre, le trafic de chaque version du protocole IP étant natif (pas de tunnel). Avec la double pile, l'arrivée d'IPv6 n'affecte pas du tout IPv4. D'un autre côté, il faut donc gérer deux versions du protocole. (Anecdote personnelle : quand j'ai commencé dans le métier, IP était très loin de la domination mondiale, et il était normal, sur un réseau local, de devoir gérer cinq ou six protocoles très différents. Prétendre que ce serait une tâche insurmontable de gérer deux versions du même protocole, c'est considérer les administrateurs réseaux comme très paresseux ou très incompétents.) L'important est que les politiques soient cohérentes, afin d'éviter, par exemple, que le port 443 soit autorisé en IPv4 mais bloqué en IPv6, ou le contraire. (C'est parfois assez difficile à réaliser sans une stricte discipline : beaucoup de pare-feux n'ont pas de mécanisme simple pour indiquer une politique indépendante de la version du protocole IP.)

Notez que certains réseaux peuvent être « double-pile » sans que l'administrateur réseaux l'ait choisi, ou en soit conscient, si certaines machines ont IPv6 activé par défaut (ce qui est fréquent et justifié). Des attaques peuvent donc être menées via l'adresse locale au lien même si aucun routeur du réseau ne route IPv6.

Mais les plus gros problèmes de sécurité liés aux techniques de coexistence/transition viennent des tunnels. Le RFC 6169 détaille les conséquences des tunnels pour la sécurité. Sauf s'ils sont protégés par IPsec ou une technique équivalente, les tunnels permettent bien des choses qui facilitent le contournement des mesures de sécurité. Pendant longtemps, l'interconnexion entre réseaux IPv6 isolés se faisait via des tunnels, et cela a contribué aux légendes comme quoi IPv6 posait des problèmes de sécurité. Aujourd'hui, ces tunnels sont moins nécessaires (sauf si un réseau IPv6 n'est connecté que par des opérateurs archaïques qui n'ont qu'IPv4).

Les tunnels les plus dangereux (mais aussi les plus pratiques) sont les tunnels automatiques, montés sans configuration explicite. Le RFC suggère donc de les filtrer sur le pare-feu du réseau, en bloquant le protocole IP 41 (ISATAP - RFC 5214, 6to4 - RFC 3056, mais aussi 6rd - RFC 5969 - qui, lui, ne rentre pas vraiment dans la catégorie « automatique »), le protocole IP 47 (ce qui bloque GRE, qui n'est pas non plus un protocole « automatique ») et le port UDP 3544, pour neutraliser Teredo - RFC 4380. D'ailleurs, le RFC rappelle plus loin que les tunnels statiques (RFC 2529), utilisant par exemple GRE (RFC 2784), sont plus sûrs (mais IPsec ou équivalent reste recommandé). 6to4 et Teredo sont de toute façon très déconseillés aujourd'hui (RFC 7526 et RFC 3964).

Et les mécanismes de traduction d'adresses ? On peut en effet traduire des adresses IPv4 en IPv4 (le traditionnel NAT, qui est plutôt du NAPT en pratique, puisqu'il traduit aussi le port), ce qui est parfois présenté à tort comme une fonction de sécurité <https://www.bortzmeyer.org/nat-et-securite.html>, mais on peut aussi traduire de l'IPv4 en IPv6 ou bien de l'IPv6 en IPv6. Le partage d'adresses que permettent certains usages de la traduction (par exemple le CGNAT) ouvre des problèmes de sécurité bien connus <https://www.europol.europa.eu/newsroom/news/are-you-sharing-same-ip-address-cri
Les techniques de traduction d'IPv4 en IPv6 comme NAT64 - RFC 6146 ou 464XLAT - RFC 6877 apportent également quelques problèmes, décrits dans leurs RFC.

J'ai parlé plus haut du fait que les systèmes d'exploitation modernes ont IPv6 et l'activent par défaut. Cela implique de sécuriser les machines contre les accès non voulus faits avec IPv6. Du classique, rien de spécifique à IPv6 à part le fait que certains administrateurs système risqueraient de sécuriser les accès via

IPv4 (avec un pare-feu intégré au système d'exploitation, par exemple) en oubliant de le faire également en IPv6.

Tous les conseils donnés jusqu'à présent dans cette section 2 du RFC étaient communs à tous les réseaux IPv6. Les sections suivantes s'attaquent à des types de réseau spécifiques à certaines catégories d'utilisateurs. D'abord (section 3), les « entreprises » (en fait, toutes les organisations - RFC 7381, pas uniquement les entreprises capitalistes privées, comme le terme étatsunien "*enterprise*" pourrait le faire penser). Le RFC contient quelques conseils de sécurité, proches de ce qui se fait en IPv4, du genre « bloquer les services qu'on n'utilise pas ». (Et il y a aussi le conseil plus évident : bloquer les paquets entrants qui ont une adresses IP source interne et les paquets sortants qui ont une adresse IP source externe.)

Et pour les divers opérateurs (section 4 du RFC) ? C'est plus délicat car ils ne peuvent pas, contrairement aux organisations, bloquer ce qu'ils ne veulent pas (sauf à violer la neutralité <https://www.bortzmeyer.org/neutralite.html>, ce qui est mal). Le RFC donne des conseils de sécurisation BGP (identiques à ceux d'IPv4) et RTBH (RFC 5635). Il contient également une section sur l'« interception légale » (le terme politiquement correct pour les écoutes et la surveillance). Légalement, les exigences (et les problèmes qu'elles posent) sont les mêmes en IPv4 et en IPv6. En IPv4, le partage d'adresses, pratique très répandue, complique sérieusement la tâche des opérateurs quand ils reçoivent un ordre d'identifier le titulaire de telle ou telle adresse IP (RFC 6269). En IPv6, en théorie, la situation est meilleure pour la surveillance, une adresse IP n'étant pas partagée. Par contre, l'utilisateur peut souvent faire varier son adresse au sein d'un préfixe /64.

Quand au réseau de l'utilisateur final, il fait l'objet de la section 5. Il n'y a pas actuellement de RFC définitif sur la délicate question de la sécurité de la maison de M. Michu. Notamment, les RFC 6092 et RFC 7084 ne prennent pas position sur la question très sensible de savoir si les routeurs/pare-feux d'entrée de ce réseau devraient bloquer par défaut les connexions entrantes. La sécurité plaiderait en ce sens mais ça casserait le principe de bout en bout.

Voilà, nous avons terminé cette revue du long RFC. Je résumerai mon opinion personnelle en disant : pour la plupart des questions de sécurité, les ressemblances entre IPv4 et IPv6 l'emportent sur les différences. La sécurité n'est donc pas une bonne raison de retarder la migration si nécessaire vers IPv6. J'ai développé cette idée dans divers exposés et articles <https://www.bortzmeyer.org/ipv6-securite.html>.