RFC 6105 : IPv6 Router Advertisement Guard

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 24 février 2011

Date de publication du RFC : Février 2011

https://www.bortzmeyer.org/6105.html

Comme le décrit très bien le RFC 6104 [1], la situation de la sécurité des RA ("*Router Advertisement*", cf. RFC 4861) n'est pas satisfaisante. Les « faux RA », envoyés par un méchant ou par un maladroit, sont trop fréquents. Notre RFC 6105 propose donc une solution. Elle est bien plus légère que SEND et repose sur un filtrage au niveau deux.

Je vous renvoie à mon article sur le RFC 6104 pour davantage de détails sur le **problème**. Ici, je ne vais parler que de la **solution**. Elle fonctionne pour un réseau partagé où les participants doivent passer par un commutateur (on ne peut donc pas l'utiliser pour du WiFi ad hoc, cf. section 5) et elle nécessite que ledit commutateur mette en œuvre le système décrit dans ce RFC (cf. section 2 et sa figure 1).

Officiellement, SEND (RFC 3971), reste la solution de choix. Après l'obligatoire rappel que SEND résoudrait tous les problèmes, notre RFC rappelle qu'il n'est pas réaliste d'espérer un déploiement massif de SEND dans les années à venir. Pire, le RFC reconnait que certains équipements (on pense au célèbre grille-pain IPv6) n'auront jamais SEND. La solution proposé, "*RA Guard*", est donc un système de filtrage des RA par le commutateur, suivant plusieurs méthodes possibles. Le commutateur sert donc de centre de contrôle, autorisant ou bloquant les RA selon plusieurs possibilités.

Quelles sont ces possibilités ? Les sections suivantes les décrivent. D'abord, le "*RA guard*" sans état (section 3). Dans ce mode, le commutateur examine les RA entrants et les bloque ou pas en ne tenant compte que du contenu du RA et de sa propre configuration. Il n'a donc pas de mémoire, pas d'état. Sur quelle base décider ? L'adresse MAC source du RA, le port sur lequel le RA a été reçu, l'adresse IP source, le ou les préfixes annoncés dans le RA...Le commutateur a pu être configuré pour autoriser ou interdire sur la base de ces informations. Une fois le RA considéré comme légitime, il est transmis sur

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6104.txt

toutes les interfaces, comme n'importe quel paquet. Le RFC présente par exemple une solution ultra-simple où l'administrateur du commutateur indique juste un port comme étant celui du routeur officiel, et les RA arrivant sur les autres ports seront donc simplement ignorés. Cette méthode a l'inconvénient de nécessiter une configuration manuelle.

Plus sophistiquée, le "*RA guard*" avec état (section 4). Le principe est d'apprendre automatiquement à quoi ressemblent les RA légitimes, avant de se mettre à bloquer les autres. Dans sa version la plus simple, le commutateur écoute pendant un moment (défini par l'administrateur), notant qui envoie les RA, puis considère que, après ce laps de temps, tout autre RA est illégitime. Cela protège donc contre les RA anormaux survenant après cette période d'apprentissage. Si un nouveau routeur légitime arrive, on recommence l'apprentissage de zéro.

La section 4.1 décrit les détails. Au début, le commutateur est dans l'état `LEARNING` où il écoute les RA. Fait-il suivre tous les RA pendant cette phase, ou bien les bloque-t-il tous ? C'est configurable selon le degré de paranoïa de l'administrateur. Une fois cette phase terminée, les interfaces passent dans l'état `BLOCKING` ou `FORWARDING` selon qu'elles recevaient des RA acceptables ou non. (Le RFC ne mentionne donc que la possibilité d'apprendre les interfaces où se trouve un routeur légitime, pas celles d'apprendre son adresse MAC.) La section 7 suggère fortement que l'administrateur jette un coup d'œil à la liste des interfaces à RA légitimes, pour vérifier…Par contre, elle ne rappelle pas que le mécanisme est mis en danger si un routeur illégitime est présent dès la phase d'apprentissage. Normalement, ce cas est traité par le fait que cette technique est combinée avec des filtres manuels comme ceux de la section précédente.

Encore plus ambitieux, la possibilité pour le commutateur d'être un mandataire SEND (section 4.2). L'un des problèmes de SEND est que chaque machine du réseau, grille-pain et frigidaire inclus, doit faire de la cryptographie (parfois compliquée, par exemple s'il faut récupérer des certificats intermédiaires) et être configurée avec un certificat. Avec le mandataire SEND, seul le commutateur va valider les annonces signées par SEND. Il les fera suivre ou les bloquera en fonction du résultat de la validation.

Je ne connais pas de liste d'implémentations officielles de ce service. Apparemment, certains le déploieraient déjà, si on en croit des témoignages <`http://serverfault.com/questions/201547/router-advertisements-do-not-go-through-wired-wireless-bridge`>. Fin 2011, Juniper annonçait "*RA Guard*" pour les versions 12.x, Cisco a déjà cette fonction dans des engins comme le Cisco 3750g avec « "*advanced enterprise featureset*" » (voir un bon article sur le sujet <`http://ipv6blog.cisco.fr/tag/ra-guard/`> et un plus détaillé <`http://reseauxblog.cisco.fr/2012/11/19/jai-teste-pour-vous-ipv6-first-hop-security/`>, du même auteur). Brocade n'a rien communiqué. Une technique permettant de contourner le "*RA guard*" a déjà été décrite <`http://blog.si6networks.com/2011/09/router-advertisement-guard-ra-guard.html`>.