RFC 6204 : Basic Requirements for IPv6 Customer Edge Routers

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 28 avril 2011

Date de publication du RFC : Avril 2011

https://www.bortzmeyer.org/6204.html

Ce RFC du groupe de travail v6ops <http://tools.ietf.org/wg/v6ops>, qui se consacre aux problèmes pratiques du fonctionnement d'IPv6 (sans modification des protocoles, donc), porte sur les CPE ("*Customer Premises Equipment*"), alias CER ("*Customer Edge Routers*"), alias "*home gateway*", qui sont les boîtiers installés chez l'utilisateur domestique ou petite entreprise. Par exemple, en France, la Freebox ou la DartyBox sont des CPE. Certains d'entre eux gèrent le protocole IPv6 et ce RFC résume tout ce que doivent savoir les concepteurs de ces « "*boxes*" » pour faire de l'IPv6 proprement. Il a depuis été remplacé par le RFC 7084 [1].

Le gros débat qui avait eu lieu à l'IETF lors de la conception de ce RFC portait sur une règle exprimée dans les premières versions de l'"*Internet-Draft*" qui avait précédé le RFC : cette règle disait qu'un CPE IPv6 devait, par défaut, bloquer les connexions entrantes. L'argument principal était que les CPE IPv4 font tous cela. Mais ils le font parce qu'en IPv4, la pénurie d'adresses <https://www.bortzmeyer.org/epuisement-adresses-ipv4.html> oblige à des bricolages comme le NAT, et empêchent de toute façon les connexions entrantes. IPv6 permettant enfin de récupérer une adresse IP unique mondialement, et donc d'avoir à nouveau une connectivité de bout en bout, cette règle évoquait plus un « Minitel 2.0 <http://www.fdn.fr/internet-libre-ou-minitel-2.html> » que l'Internet du futur.

Elle a donc été retirée de ce RFC, qui laisse ouverte la question de la sécurité, la déléguant à un autre document, le RFC 6092. En coupant les connexions entrantes, on bloque certaines attaques (par forcément les plus fréquentes : aujourd'hui, la plupart des attaques se font par le contenu des données transférées - importation de "*malware*" - et pas directement sur IP) mais on empêche les utilisateurs de profiter des services comme la téléphonie sur IP ou le pair-à-pair, qui dépendent souvent de cette possibilité de connexions entrantes.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc7084.txt

Donc, en dehors de ce point, que contient ce RFC ? La section 1 résume les points importants : le RFC se focalise sur le cas où IPv6 est natif (pas de traduction d'adresses entre v4 et v6), et sur le cas simple où il n'y a qu'un seul CPE, qui récupère sa configuration sur le WAN, puis la distribue aux machines IPv6 locales, puis route leurs paquets. Le déploiement de l'IPv6 dans le réseau de l'opérateur n'est pas discuté (cf. RFC 4779). Ce RFC concerne uniquement le « foyer, doux foyer ».

D'abord, un rappel du fonctionnement d'un CPE IPv4 aujourd'hui. Ce fonctionnement n'est spécifié nulle part, il résulte d'une accumulation de choix par les auteurs anonymes des CPE existants. Ces choix sont souvent erronés <https://www.bortzmeyer.org/home-gateway.html>. En l'absence de norme formelle, la section 3.1 décrit le CPE « typique » de 2010. Ce CPE typique a une (et une seule) connexion avec l'Internet, une seule adresse IP publique (et encore, parfois, il y a même du NAT dans le réseau de l'opérateur) et il sert de routeur NAT aux machines IPv4 situées sur le réseau local. Par défaut, en raison du NAT, il bloque toutes les connexions entrantes (c'est la seule allusion à cette question qui soit restée dans la version finale du RFC). Ouvrir des ports entrants ("*port forwarding*") se fait par une configuration manuelle du CPE, via une interface Web (cas de la Freebox) ou bien par UPnP. C'est donc un vrai Minitel 2.0 <http://www.fdn.fr/internet-libre-ou-minitel-2.html>. Un avantage de ces adresses privées est toutefois d'assurer la stabilité des adresses internes : elles ne changent pas si on quitte son FAI.

L'architecture ci-dessus est largement déployée et correspond au cas de la plupart des abonnés à l'Internet à la maison. À quoi ressemblera t-elle en IPv6 ? On ne peut évidemment pas encore être sûr. mais la section 3.2, qui la décrit en termes très généraux, suppose qu'elle ne sera pas très différente, à part que la présence de plusieurs réseaux (et donc plusieurs préfixes IP) sera peut-être un cas plus fréquent qu'aujourd'hui. Quelles adresses IP seront utilisées à l'intérieur ? On pense immédiatement au RFC 5902, qui n'est toutefois pas cité. Le RFC 6204 présente la possibilité que des adresse locales, les ULA (RFC 4193) soient utilisées pour le réseau local. Le CPE devra bien alors fournir un mécanisme de traduction.

Alors, maintenant, quelles sont les exigences auxquelles devront se plier les futurs CPE IPv6 ? La section 4 est la liste de ces demandes. Elles sont nombreuses. Citons, parmi elles, l'obligation de d'abord se comporter en bon routeur, ce qui implique par exemple de mettre en œuvre ICMP (RFC 4443) correctement. Du côté du WAN, le CPE devra lui-même utiliser les protocoles standard de découverte d'un routeur (RFC 4861) pour trouver où envoyer les paquets, devra demander son préfixe avec DHCP (RFC 8415), devra bien sûr encapsuler IPv6 correctement (RFC 2464 pour Ethernet), etc. Du côté du LAN, il devra fournir des adresses globales ou des ULA (les adresses locales au lien ne suffisent pas et, de toute façon, pas besoin d'un routeur pour en acquérir). La gestion des ULA est désormais obligatoire, et le CPE doit pouvoir mémoriser le préfixe ULA, même en cas de redémarrage, de façon à fournir un préfixe stable (et, idéalement, configurable) au réseau dont il a la charge. Il doit évidemment pouvoir distribuer ce préfixe sur le réseau local avec SLAAC ("*Stateless Address Autoconfiguration*", RFC 4862) ou avec DHCP (RFC 3315, ce protocole devient donc désormais obligatoire). Il doit fournir des options comme l'annonce des serveurs DNS (RFC 3646).

La sécurité, on l'a vu, est l'aspect délicat de ces machines, puisque le M. Michu qui les utilise pour connecter sa maison, ne connait pas le problème et n'a pas envie d'apprendre. Sur ce point controversé, la section 4.4 se contente de renvoyer à un autre RFC, le RFC 6092 en disant que ce serait bien de mettre en œuvre ses recommandations. Délibérement, la question de la configuration par défaut souhaitable (permettre les connexions entrantes ou pas) est laissée de côté.

Les CPE d'aujourd'hui mettent-ils en œuvre ces recommandations ? Difficile à dire, je ne connais pas d'étude systématique ayant été faite sur les capacités de ces engins (un projet est en cours <http://www.ipv6ready.org/?page=public-review-cpe>), mais ce serait certainement très instructif. Des tests chez Free sur une Freebox v5 semblent indiquer que tout est correct (pas de filtrage bizarre, et merci à Ludovic Martin pour ses essais.)