RFC 7084 : Basic Requirements for IPv6 Customer Edge Routers

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 23 novembre 2013

Date de publication du RFC : Novembre 2013

https://www.bortzmeyer.org/7084.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 dans la 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 succède, avec quelques changements, au RFC 6204 [1], qui était le premier de cette série.

Ce RFC se focalise (section 1) 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 ».

Ce RFC utilise un vocabulaire normatif, celui du RFC 2119, mais pas pour spécifier un protocole mais pour indiquer quel est le minimum qu'on peut attendre d'un CPE IPv6 aujourd'hui.

D'abord (section 3), 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 2012. 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

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6204.txt

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 7084 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. Pour les communications entre machines du réseau interne, il faudra utiliser les mécanismes du RFC 4191.

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 et, pour s'y retrouver, elles portent chacune un identificateur formel, indiquant la catégorie et un numéro. Par exemple, la première, G-1, rappelle qu'un routeur est aussi un nœud du réseau et doit donc suivre le protocole IPv6, tel qu'il s'applique à tous les nœuds IPv6, routeur ou machine terminale (RFC 8504). Parmi les autres exigences (je vous rassure, je ne vais pas les citer toutes), G-4 et G-5 précisent que, si le CPE n'a pas pu obtenir une connectivité IPv6 avec l'extérieur, il ne doit **pas** publier d'adresses IPv6 sur le réseau local (car beaucoup d'applications réagissent mal lorsque la machine a une adresse IPv6 mais pas de connectivité, cf. RFC 6555). Si le CPE n'a pas de connectivité globale, il doit émettre des annonces RA ("*Router Advertisement*", RFC 4861) avec une durée de vie nulle.

Le CPE se connecte avec le reste de l'Internet en suivant les protocoles standard d'encapsulation pour IPv6 par exemple le RFC 2464 pour Ethernet et le RFC 5072 pour PPP (exigences WLL-1 et WLL-2).

Le CPE doit donc obtenir une adresse et une connectivité depuis l'amont, depuis le FAI. Cela peut se faire avec NDP ou avec DHCP (tous les deux fonctionnent sur tout type de lien, pas seulement sur Ethernet). C'est pour cela que, sur PPP, il n'y a pas de mécanisme en IPv6 pour allouer des adresses globales (RFC 5072). Donc, exigence W-1, le CPE doit utiliser NDP (RFC 4862) ou DHCP (RFC 8415) pour récupérer une adressse IPv6 globale. Avoir une adresse pour le CPE, c'est très joli, mais il faut aussi qu'il ait un préfixe à déléguer aux clients du réseau local, et il doit l'obtenir avec la technique DHCP du RFC 8415 (exigences W-4 et WPD-1).

Nouveauté de ce RFC par rapport au RFC 6204, W-6, le CPE doit aussi inclure un client PCP ("*Port Control Protocol*", RFC 6887) pour son propre usage (il n'est pas obligé de fournir ce service à ces clients du LAN).

À côté d'autre exigences évidentes, portant sur des fonctions de base d'IPv6, le RFC demande aussi que le client DHCP dans le CPE utilise les options du RFC 3646 permettant de récupérer la liste des serveurs de noms (exigences WAA-3 et WAA-4).

Il devrait aussi avoir un serveur NTP (RFC 5905), mais pour son usage, pas forcément pour distribuer l'heure sur le réseau local (exigence WAA-5). La liste des serveurs NTP devrait également être récupérée dynamiquement et de manière standard avec les options DHCP du RFC 5908.

Justement, côté LAN, maintenant, que doit faire le bon CPE IPv6 ? Là encore, on trouve beaucoup d'exigences qui sont juste un rappel des fonctions de base d'IPv6. Mais d'autres sont moins évidentes comme la capacité à gérer des ULA (exigence ULA-1 et RFC 4193) ou le serveur DHCP pour les clients du réseau local (exigence L-8, en pratique, très rare sur les CPE d'aujourd'hui). Ce serveur DHCP peut servir à l'affectation des adresses IP (RFC 8415) ou bien uniquement à distribuer des paramètres statiques, comme le permet le RFC 8415. Aussi bien en DHCP (RFC 3646) qu'en RA (RFC 8106), le CPE doit fournir aux machines du réseau local les adresses des serveurs de noms, ainsi que quelques paramètres DNS.

Également côté LAN, le CPE 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 (RFC 4193) 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 (exigences ULA-1, ULA-2 et ULA-3).

Une autre nouveauté de ce RFC 7084 par rapport à son prédécesseur, le RFC 6204, est l'exigence que le CPE IPv6 gère certaines des techniques de coexistence et de transition <https://www.bortzmeyer.org/transition-ipv6-guilde.html> IPv4-IPv6. Ainsi, le RFC recommande fortement 6rd (RFC 5969) et DS-Lite (RFC 6333).

La securité est la dernière sous-section de cette section 4. C'est un sujet très délicat, car il opposait, à l'IETF, ceux qui voulaient interdire par défaut les connexions entrantes, au nom de la sécurité (« Minitel 2.0 <http://www.fdn.fr/internet-libre-ou-minitel-2.html> ») à ceux qui voulaient profiter du fait qu'IPv6, avec son abondance d'adresses globalement uniques, permettait de rétablit le modèle de bout en bout de l'Internet, qui permet à deux machines consentantes d'échanger les paquets qu'elles veulent. Le compromis entre les deux camps a finalement été que le CPE devait mettre en œuvre, dans son logiciel, cette capacité de bloquage, mais pas forcément l'activer par défaut. Un autre RFC, le RFC 6092, discute plus en détail des fonctions de pare-feu d'un CPE. Dans notre RFC 7084, on a juste la recommandation que, **par défaut**, le CPE filtre les adresses IP usurpées (RFC 2827) et les paquets clairement invalides ("*bogons*", par exemple).

Quels sont les changements depuis le RFC 6204, qui avait été le premier à s'attaquer à cette difficile question de la spécification d'un CPE idéal ? Ils sont assez importants (surtout que le RFC 6204 est assez récent, vieux de seulement deux ans et demi), et décrits en annexe A. Les principaux :

— L'ajout des techniques de transition comme 6rd et DS-Lite.
— La normalisation de PCP dans le RFC 6887, qui permet désormais de l'indiquer comme obligatoire (mais seulement pour le CPE lui-même, pas forcément pour les machines du réseau local).
— Des obligations en plus, comme les paramètres DNS, qui passent de "*SHOULD*" à "*MUST*".
— Plus de précision dans certaines demandes, par exemple sur le fait que le CPE doive cesser d'annoncer des routes IPv6 si lui-même n'a plus de connectivité vers le FAI.

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.