RFC 7404 : Using Only Link-Local Addressing Inside an IPv6 Network

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 19 novembre 2014

Date de publication du RFC : Novembre 2014

https://www.bortzmeyer.org/7404.html

L'utilisation du protocole IPv6 fait que chaque machine a une adresse dite « locale au lien » ("*link-local*") qui n'est **pas** unique mondialement mais seulement unique sur le lien. Est-ce qu'on peut se contenter de ces adresses, et, par exemple, configurer ses routeurs pour les utiliser ? Ce RFC discute les avantages et les inconvénients. (Attention, le sujet est brûlant à l'IETF.)

Imaginons deux routeurs connectés et qui échangent des routes, via un protocole de routage. On les a configurés avec l'adresse du voisin. Cette adresse peut être une adresse « normale », mondialement unique. Mais elle peut aussi être locale au lien et cela présente quelques avantages. Par exemple, les adresses des routeurs ne sont pas présentes dans la table de routage (car elles n'ont de signification que locale), rendant ces tables plus petites. Et le routeur est plus dur à attaquer, puisqu'il faut être sur le lien pour lui parler. Par contre, cela peut rendre des outils de tests habituels comme ping ou traceroute difficiles ou impossibles à utiliser.

L'un dans l'autre, l'IETF ne tranche pas : cette possibilité marche, elle est documentée dans ce RFC mais chacun doit ensuite décider s'il va l'utiliser ou pas. Comme le dit le RFC avec un sens aigu du lavage de mains « "*The deployment of this technique is appropriate where it is found to be necessary*" ».

La section 2 forme le gros de ce RFC : exposer l'approche, ses avantages, et ses risques. Les adresses locales au lien sont désignées par le sigle LLA ("*link-local addresses*"). Voici un exemple sur une machine Linux (les LLA sont dans le préfixe `fe80::/10`) :

```
% ip -6 addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qlen 1000
    inet6 fe80::ba27:ebff:feba:9094/64 scope link
       valid_lft forever preferred_lft forever
```

Le principe de base de leur utilisation est que, lorsqu'une machine n'a pas besoin de parler au monde extérieur sur cette adresse (ce qui est typiquement le cas d'un routeur), on peut ne mettre qu'une LLA sur une interface.

Attention, ce n'est vrai que pour une interface. Pas question de n'avoir que des LLA sur l'ensemble du routeur car celui-ci doit pouvoir émettre des paquets ICMP du genre "*Message too big*" ou bien "*Time exceeded*". Il faut donc qu'au moins une interface du routeur ait une adresse globale, qui sera utilisée comme adresse source lors de l'émission de ces paquets ICMP (cf. RFC 6724 [1]). Cette adresse devra être routée, pour éviter tout filtrage en raison du RFC 3704. Dans le monde des routeurs, on appelle cela en général une "*loopback interface*" mais attention, c'est un sens différent de celui du mot "*loopback*" sur les machines Unix ordinaires. (Au fait, si quelqu'un sait comment modifier l[Caractère Unicode non montré [2]]interface source des erreurs ICMP sur IOS... Ça existe en NX-OS, mais c'est introuvable en IOS et IOS-XE.)

Les protocoles de routage (OSPF, BGP, RIPng) fonctionnent déjà avec des LLA naturellement, ou peuvent être configurés pour le faire (pour BGP, Francis Dupont me souffle qu'il faut faire attention au RFC 2545, qui n'est pas cité). La découverte des voisins par NDP se fait toujours avec des LLA donc n'est pas affectée. Pour les protocoles de gestion du routeur, comme SSH ou SNMP (le RFC s'amuse aussi à citer Telnet...) devront, eux, utiliser l'adresse globale mentionnée plus haut.

Ah, et, évidemment, le gros du trafic du routeur, ce ne sont pas les protocoles de routage ou de gestion du routeur, c'est le trafic des autres, qu'il transmet. Ce dernier a des adresses source et destination qui ne sont **pas** celles du routeur et, donc, l'utilisation par ce dernier de LLA ou pas ne change rien. Bref, ça devrait marcher. Mais quels sont les avantages à une configuration uniquement avec des LLA ?

D'abord, comme indiqué plus haut, les tables de routage sont plus petites, puisqu'on n'y met pas les LLA, seulement les adresses globales, moins nombreuses (une seule par routeur, dans le cas le plus économe). Ensuite, on simplifie le plan d'adressage : pas besoin d'attribuer des préfixes aux liens entre routeurs. On a également moins de complexité dans la configuration, les LLA étant attribuées automatiquement. Et on a moins de configuration DNS à maintenir, puisqu'on ne met pas les LLA dans le DNS (évidemment, on n'est pas forcé d'y mettre les adresses globales non plus).

Surtout, on réduit les possibilités d'attaque puisque l'envoi de paquets au routeur, depuis l'extérieur du lien, ne pourra se faire que via l'adresse globale (par exemple pour les attaques du RFC 4987). Il n'y aura donc que celle-ci à protéger (par exemple via des ACL).

Le monde où nous vivons n'étant pas un monde idéal, depuis l'expulsion hors du jardin d'Éden, il y a aussi des problèmes associés aux LLA. On peut encore pinguer une interface spécifique depuis le lien (`ping $lla%$if-name`) mais plus depuis un autre réseau. Le débogage peut donc devenir plus difficile. (Notez que, contrairement à ce qu'on lit souvent dans les articles sur TCP/IP, lorsqu'on pingue une adresse IP associée à une interface, une réponse positive ne garantit pas du tout qu'on est passé par cette interface.) Bien sûr, on peut toujours pinguer l'adresse globale du routeur depuis n'importe où, mais cela fournit moins d'informations. Pour déterminer si une interface marche ou pas, il faudra donc utiliser d'autres méthodes par exemple en se loguant sur le routeur et en examinant l'état des interfaces. (Notez que, là encore, en dépit des légendes, avec certains systèmes d'exploitation, on peut pinguer avec succès une adresse IP associée à cette interface même lorsque cette interface est débranchée.) Le

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc6724.txt`
2. Car trop difficile à faire afficher par LaTeX

RFC 5837, lorsqu'il est mis en œuvre, peut aider au débogage, en mettant de l'information sur l'interface dans la réponse ICMP.

Même problème, évidemment, avec traceroute. Non seulement on ne peut pas tracerouter vers une interface spécifique, mais le paquet ICMP de réponse viendra de l'adresse IP globale et ne nous renseignera donc pas sur l'interface précise qui l'a émis (sauf si le routeur utilise le RFC 5837 et si le traceroute utilisé exploite cette option). Notez que cela peut être vu comme un avantage : tous les traceroutes passant par ce routeur verront la même adresse de réponse, aidant à repérer le routeur (alors que, autrement, il aurait fallu corréler les différentes adresses, par exemple via les enregistrements PTR associés, ce qui dépend d'heuristiques peu fiables).

Et, bien sûr, cela concerne aussi les systèmes de gestion de réseau : si un gérant SNMP, par exemple, veut parler à un routeur, il devra probablement utiliser son adresse globale.

Autre problème, les adresses LLA automatiquement attribuées vont dépendre du matériel, puisqu'elles seront en général dérivées de l'adresse MAC (via EUI-64). Si on change une carte Ethernet du routeur, on change de LLA, ce qui peut nécessiter une reconfiguration manuelle si ces LLA étaient utilisées statiquement, par exemple dans une configuration BGP. (Matthieu Herrb me fait remarquer qu'on peut parfaitement créer des LLA statiques, genre `fe80::31`, ce que mentionne d'ailleurs le RFC.) Pendant qu'on est aux configurations statiques, il faut aussi rappeler que les LLA sont moins pratiques à manier puisqu'elles n'ont pas de signification globale. Il faut donc toujours indiquer le lien utilisé. Par exemple, une configuration BGP sera `bgp neighbor fe80::21e:8cff:fe76:29b6%eth2` (le `%eth2` indiquant l'interface réseau, cf. RFC 4007).

Un cas particulier est celui des points d'échange. Ils connectent beaucoup de monde et représentent une part significative du trafic Internet. Une attaque ou une panne peut sérieusement perturber le trafic. Le préfixe d'adresses IP qui est utilisé pour numéroter les routeurs sur le LAN du point d'échange est donc sensible. Pour réduire les risques, on peut soit ne pas le publier dans la table de routage globale, soit filtrer le trafic entrant vers ce préfixe. Dans le premier cas, les paquets émis depuis l'interface du routeur avec le point d'échange, ayant une adresse source non routée, seront jetés par les réseaux qui font des tests uRPF. Cela perturbe traceroute, mais, surtout la découverte de la MTU du chemin, ce qui est inacceptable. La deuxième méthode ne marche que si tous les opérateurs connectés au point d'échange la mettent en œuvre, ce qui est peu vraisemblable.

Une meilleure solution serait donc de numéroter les routeurs au point d'échange avec des LLA. Chaque routeur aurait toujours son adresse globale, prise dans l'espace d'adressage de l'opérateur propriétaire, mais une attaque globale contre tout le point d'échange serait plus difficile. Par contre, cela pourrait poser des problèmes avec certaines méthodes d'ingénierie du trafic, si l'opérateur veut transporter le préfixe du point d'échange dans son IGP. Ces opérateurs devront trouver une autre méthode.

En synthèse, la conclusion de notre RFC est que l'utilisation des LLA a des avantages et des inconvénients, et que chaque acteur doit faire son évaluation, le RFC ne recommandant spécialement aucune des deux méthodes. Cette conclusion a été chaudement discutée à l'IETF, ceux qui pensaient que les LLA étaient une mauvaise idée n'ayant pas envie que cette utilisation soit documentée, craignant que cela n'apparaisse comme une approbation.