RFC 5227 : IPv4 Address Conflict Detection

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 4 juillet 2008

Date de publication du RFC : Juillet 2008

https://www.bortzmeyer.org/5227.html

Ce RFC est entièrement consacré à un problème qui a causé des cheveux blancs à beaucoup d'administrateurs de réseaux informatiques : la détection d'une duplication d'adresses IP.

Que la duplication soit un phénomène normal (cas des réseaux non gérés, ceux dont personne ne s'occupe, où il n'y a pas de liste des adresses allouées), le résultat d'une erreur humaine, ou une incivilité (« Je prends une adresse IP au hasard, on verra bien »), elle est quasiment impossible à empêcher. Une machine peut toujours émettre avec l'adresse qu'elle veut, le protocole ARP (RFC 826 [1]) ne peut fournir aucune sécurité (section 6 du RFC). Peut-on au moins la détecter ? C'est ce que propose notre RFC, après avoir expliqué (section 1) pourquoi le mécanisme proposé par le RFC 2131 n'est pas suffisant (cette section 1, comme souvent avec Stuart Cheshire, tourne d'ailleurs souvent au réglement de comptes, comme lorsque l'auteur souligne que Mac OS avait déjà résolu le problème en 1998).

Le nouveau protocole, ACD, repose sur ARP. La section 1.2 commence en listant les nouveautés. Le principe d'ACD est d'utiliser ARP, non pas pour poser sincèrement la question « Qui utilise telle adresse IP ? » mais pour détecter ceux qui répondraient à une requête pour l'adresse IP de la machine émettrice. Comme le note la section 1.2, de telles questions « orientées » sont courantes dans la vie. Si on demande au café « Est-ce que cette table est libre ? » c'est en général avec l'intention de s'y asseoir si elle l'est. De même, avec ACD, la machine qui veut vérifier l'unicité de son adresse IP, mettons `192.0.2.48` va demander à tout le monde « Qui utilise `192.0.2.48` ? » et confirmer cette adresse si personne ne réagit. ACD est utilisable sur tout réseau où ARP fonctionne.

La section 2 est la description détaillée du protocole. Lors du démarrage ou redémarrage d'une interface réseau, la machine ACD envoie une requête ARP pour sa propre adresse, avec sa propre adresse

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

MAC comme adresse MAC source et `0.0.0.0` comme adresse IP source (section 2.1.1 : cette surprenante précaution est nécessaire pour éviter de polluer les caches ARP si quelqu'un utilise déjà cette adresse).

Après une attente suffisante (les détails se trouvent dans le RFC), si personne n'a répondu, la machine considère qu'il n'y a pas de duplication d'adresse et envoie une deuxième requête ARP, cette fois-ci avec son adresse IP en source, pour prévenir qu'elle va désormais utiliser cette adresse.

La réponse ARP est normalement acheminée en "*unicast*" mais la section 2.6 explique qu'ACD peut aussi utiliser la diffusion générale.

Et si ça va mal ? Si quelqu'un utilise cette adresse ? La section 2.4 couvre ce cas, en notant également que la détection de conflit doit être continue, puisqu'une autre machine peut arriver à tout moment en voulant utiliser la même adresse. La section détaille donc le concept de « défendre son adresse », comment et dans quelles conditions.

La section 3 contient l'explication d'un choix de conception qui fut très discuté, l'utilisation, pour tester la duplication, de **requêtes** ARP au lieu de **réponses** ARP, a priori plus adaptées. La principale raison est la crainte que certaines implémentations ne gèrent pas correctement des réponses qui n'ont été précédées d'aucune requête. Notons aussi qu'il est malheureusement rare dans les RFC de voir une discussion des choix alternatifs : la spécification est en général annoncée telle quelle, sans justification des choix, contrairement à ce que fait ce RFC.

La section 4, historique, rappelle l'ancienne technique des « ARP gratuits » (au sens de « meurtres gratuits »), qui avait été proposée par Stevens dans son "*TCP/IP illustrated*" et explique en quoi ACD est préférable (l'ARP gratuit est l'équivalent de crier « Je vais prendre cette table » sans vérifier si elle est déjà occupée).