RFC 6744 : IPv6 Nonce Destination Option for ILNPv6

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 10 novembre 2012

Date de publication du RFC : Novembre 2012

http://www.bortzmeyer.org/6744.html

Une grande partie de la sécurité d'ILNP, architecture de séparation de l'identificateur et du localisateur <http://www.bortzmeyer.org/separation-identificateur-localisateur.html>, dépend d'un **numnique <http://www.bortzmeyer.org/nonce.html>**, nombre imprévisible choisi par une machine et transmis à son correspondant au début d'une session. En renvoyant ce nombre, le pair prouve qu'il est bien le même correspondant. Ce RFC décrit les détails de l'option IPv6 "*Nonce*" <http://www.bortzmeyer.org/nonce.html> (numnique), utilisée pour ILNP sur IPv6.

ILNP est décrit dans le RFC 6740[1], avec certains détails pratiques dans le RFC 6741. Comme tous les systèmes à séparation de l'identificateur et du localisateur, son talon d'Achille est le lien ("*binding*") entre l'identificateur d'une machine et son localisateur. Si on reçoit un paquet disant « pour joindre la machine d'identificateur 3a59:f9ff:fe7d:b647, envoie désormais les paquets au localisateur 2001:db8:43a:c19 », faut-il le croire ? Évidemment, non, pas sur l'Internet public en tout cas. La solution adoptée par ILNP est d'avoir un **numnique**. C'est un nombre généré de manière imprévisible par un tiers (idéalement, ce devrait être un nombre aléatoire), que chaque machine envoie au début de la session ILNP. Lorsqu'un correspondant veut s'authentifier (par exemple lorsqu'il envoie le message de changement de localisateur cité plus haut, cf. RFC 6743), il inclura ce numnique.

Ce numnique sera transporté, aussi bien pour le début de la session que pour les mises à jour de localisateur, dans une option Destination IPv6 (ces options sont décrites dans le RFC 2460, section 4.6). Cette option sert donc à la sécurité d'ILNP. Mais elle a aussi une autre fonction, signaler, lors du débat d'une conversation, qu'on connait ILNP et que le correspondant peut l'utiliser (la coexistence pacifique d'ILNPv6 et d'IPv6 Classic en dépend). Elle ne doit donc apparaître que dans les paquets ILNP.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6740.txt

L'en-tête « options pour la Destination » peut contenir plusieurs options (en pratique, à l'heure actuelle, comme le note notre RFC, il n'est quasiment jamais utilisé), mais il ne doit y avoir qu'une seule option "*Nonce*". Si d'autres options sont quand même présentes (comme celle du RFC 5570), le RFC recommande que "*Nonce*" soit la première dans l'en-tête.

La section 2 décrit la syntaxe de cette option. Elle comporte les champs obligatoires, "*Option Type*" (0x8b dans le registre IANA <https://www.iana.org/assignments/ipv6-parameters/ipv6-parameters.xml#ipv6-parameters-2>), "*Option length*" (en octets ; le numnique n'a pas de longueur fixe mais au moins les valeurs de 4 et 12 octets doivent être acceptées par les mises en œuvre de ce RFC) et "*Nonce*" (la valeur du numnique, de préférence générée selon les bons principes du RFC 4086).

En l'absence de l'option "*Nonce*" dans un paquet entrant, ILNP jettera le paquet si le localisateur source n'est pas dans la liste actuellement connue et stockée dans l'ILCC ("*Identifier-Locator Communication Cache*", cf. RFC 6741). Lorsqu'une machine ILNP change sa liste de localisateurs (section 4), elle envoie un paquet avec la nouvelle liste et ce paquet doit inclure l'option "*Nonce*" (avec un numnique correct) pour être accepté. Le RFC recommande également d'inclure cette option dans les paquets suivants, pour une durée d'au moins trois RTT, afin de se prémunir contre un éventuel réordonnancement des paquets. (Notez que cela ne règle que le cas d'un retard du "*Locator Update*", pas le cas de sa perte. Recevoir le paquet avec le numnique correct ne suffit pas à changer les localisateurs mémorisés, ne serait que parce que ce paquet ne contient qu'un seul localisateur et pas la liste actuelle.)

Si vous êtes en train de programmer une mise en œuvre d'ILNP, lisez aussi la section 5, qui donne d'utiles conseils, notamment sur l'ILCC (qui garde en mémoire le numnique actuel de la session, c'est une des informations les plus importantes qu'il stocke).

L'Internet à l'heure actuelle ne contient que des machines IP Classic. Comment cela va t-il se passer pour les premières machines ILNP ? La section 6 décrit la compatibilité. L'option "*Nonce*" sert à deux choses, indiquer le numnique, bien sûr, mais aussi signaler qu'ILNP est utilisé. Cette nouvelle option ne doit donc **pas** être présente dans des paquets IP Classic. Dans les paquets ILNP, elle doit être présente dans les premiers paquets (pour signaler qu'on connait ILNP) et dans tous les messages ICMP générés par les machines ILNP (comme le "*Locator Update*" du RFC 6743). Elle peut aussi être mise dans tous les paquets mais ce n'est pas indispensable. Le RFC recommande quand même de le faire si le taux de pertes de paquets de la session est particulièrement élevé (car les paquets portant l'option pourraient être perdus).

Donc, la machine recevant le premier paquet ILNP sait que son correspondent connait ILNP grâce à l'option "*Nonce*". Et la machine qui émet le premier paquet ? Comment sait-elle que le pair connait ILNP ? La principale méthode est, comme toujours dans ILNP, via le DNS. Comme décrit en détail dans le RFC 6742, la présence d'enregistrements `NID` dans le DNS indique que la machine distante connait ILNP. Et si l'information dans le DNS est fausse ou dépassée ? Dans ce cas, vu le type de l'option "*Nonce*" (avec les deux bits de plus fort poids à 10, ce qui indique que le paquet doit être rejeté si cette option n'est pas comprise, RFC 2460, section 4.2). L'émetteur, en recevant le message ICMP de rejet ("*Parameter Problem*"), saura qu'il ne faut plus essayer en ILNP.

Dans un monde idéal, cela s'arrêterait là. Mais les options de destination comme celle décrite ici sont rares dans l'Internet actuel <http://www.bortzmeyer.org/destination-options-ipv6.html> et il serait bien imprudent de promettre que celle d'ILNP passera sans problème. Comme l'a montré l'expérience d'IPv4 <http://www.bortzmeyer.org/options-interdites.html>, ce qui n'est pas utilisé finit par ne plus être géré correctement, notamment par les équipements intermédiaires. Le RFC ne mentionne pas ce problème mais évoque un problème proche, se contentant de dire que les routeurs IPv6 correctement programmés devraient ignorer tout l'en-tête "*Destination Options*" (dans un monde idéal, là encore).

La section 7 revient sur les exigences de sécurité. Le numnique ne doit pas être prévisible par un attaquant extérieur, il est donc recommandé qu'il soit généré selon les règles du RFC 4086. Notez bien que cela ne sert à rien si l'attaquant est situé sur le chemin des paquets et peut les "*sniffer*". C'est également le cas en IP Classic et le seul mécanisme vraiment sûr dans ce cas est IPsec, si on veut protéger jusqu'à la couche 3.

Si vous aimez regarder les paquets qui passent sur le réseau avec wireshark ou tcpdump, désolé, mais ces logiciels ne gèrent pas encore les options spécifiques à ILNP et ne les analyseront pas.