# RFC 7503 : OSPFv3 Auto-Configuration

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 10 avril 2015

Date de publication du RFC : Avril 2015

https://www.bortzmeyer.org/7503.html

---

Le protocole de routage OSPF est traditionnellement configuré statiquement, et à la main par l'administrateur réseaux. Certains réseaux, comme par exemple des réseaux un peu complexes à la maison, ont besoin d'un protocole de routage, mais sans avoir d'administrateur réseaux disponible. Il faudrait un OSPF qui se configure tout seul, « "*plug and play*" ». Ce court RFC montre que c'est possible, avec très peu de modifications des mises en œuvre d'OSPF.

Ce RFC concerne OSPF v3, normalisé dans le RFC 5340 [1]. Les changements du protocole par rapport à cette norme sont minimes. Par exemple, deux routeurs OSPF sont désormais autorisés à devenir adjacents (à établir une sorte de session entre eux), même si leurs valeurs des paramètres annoncés dans le paquet `Hello`, comme `HelloInterval`, diffèrent (dans un réseau auto-configuré, on ne peut pas espérer que tous les routeurs aient la même valeur, malgré ce que demandait l'annexe A.3.2 du RFC 5340). Autre exemple, une hystérésis a été ajouté lors de l'envoi de certains LSA ("*Link State Advertisement*", les messages d'OSPF). Un routeur ayant les modifications permettant l'auto-configuration peut participer à un réseau avec des routeurs n'ayant pas ces modifications (l'inverse n'est pas vrai : un routeur OSPF classique aura du mal à s'insérer dans un réseau auto-configuré). Ces changements sont nécessaires pour s'adapter aux réseaux qui, tout en étant non-gérés, sont composés de plusieurs liens et plusieurs routeurs, commme ceux envisagés par le projet Homenet <https://tools.ietf.org/wg/homenet> (RFC 7368).

La section 2 de notre RFC liste les paramètres que doivent adopter les routeurs auto-configurés :

— La zone ("*area*") doit être 0.
— OSPF doit être activé sur toutes les interfaces IPv6 du routeur, sauf si on est sûr d'avoir une très bonne raison de ne pas le faire. Par exemple, pour un routeur CPE, genre "*box*", le RFC 7084 demande évidemment qu'on ne fasse pas tourner de protocole de routage dynamique sur l'interface qui mène au FAI.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5340.txt

— Le type de réseau OSPF ("*broadcast network*" ou point-à-point) doit être configuré en fonction du type de réseau physique (Ethernet et Wi-Fi seront tous les deux "*broadcast network*", cf. RFC 2328, section 1.2).
— Chaque routeur a le choix de paramètres comme `HelloInterval` (voir la section 3 du RFC pour les détails).
— Le choix de l'"*Instance ID*" (RFC 5838) doit être 0 pour IPv6 et 64 pour IPv4.

A priori, les réseaux auto-configurés n'auront aucune forme d'authentification, celle-ci nécessitant une certaine action de l'administrateur, par exemple entrer les mots de passe (section 4 de notre RFC). Si, toutefois, on veut authentifier, il est recommandé d'utiliser l'option du RFC 7166.

Dans OSPF, chaque routeur a un "*router ID*" (RFC 2328, section 1.2), qui fait 32 bits mais n'est pas une adresse IPv4. Il doit être unique dans la zone donc il faut que tous les routeurs auto-configurés se débrouillent pour ne pas prendre le même (autrefois, c'était une adresse IPv4, et celle du routeur - RFC 5340, annexe C.1, donc l'unicité était facilement garantie). Il faut donc désormais la générer aléatoirement, en utilisant comme graine du générateur aléatoire une information unique, comme le "*router hardware fingerprint*" décrit en section 7.2.2.

Même dans ce cas, des collisions de "*router ID*" sont possibles. Il faut donc une procédure de détection des duplicatas (section 7) qui consiste, pour les voisins immédiats, à se rendre compte qu'un LSA porte le même "*router ID*" que vous, avec une adresse IPv6 différente. Il faudra alors changer : c'est le routeur avec la plus petite adresse IP qui doit changer son "*router ID*". Cette procédure de détection et de correction a été le plus gros sujet de discussion au sein du groupe de travail à l'IETF.

Pour les routeurs non-voisins, on utilise un nouveau TLV placé dans le LSA d'auto-configuration, `Router-Hardware-Fingerprint`, déjà mentionné au paragraphe précédent (au passage, ce nouveau LSA, prévu pour l'auto-configuration, est le numéro 15 <`https://www.iana.org/assignments/ospfv3-parameters/ospfv3-parameters.xml#ospfv3-parameters-3`> et les valeurs qu'il contient font l'objet d'un nouveau registre <`https://www.iana.org/assignments/ospfv3-parameters/ospfv3-parameters.xml#ac-lsa`>). Sa valeur est un nombre qui a de très fortes chances d'être unique. Il est recommandé de le fabriquer en concaténant des valeurs probablement uniques, mais stables, comme l'adresse MAC, et numéro de série du routeur.

Comme vu plus haut au sujet de l'authentification, la sécurité ne s'entend pas bien avec l'auto-configuration (section 8 du RFC). L'auto-configuration fait que n'importe quelle nouvelle machine va être « adoptée » par le réseau et pourra y participer immédiatement. Une aubaine pour un attaquant. Si on n'est pas prêt à accepter cela, il faut recourir aux mécanismes d'authentification décrits dans la section 4 (RFC 7166 ou RFC 4552).

Tout le monde n'a pas forcément envie d'utiliser l'auto-configuration, surtout étant donné ses conséquences en termes de sécurité. Il faut donc un moyen de débrayer cette possibilité (section 9 de notre RFC). (Bien sûr, il faut aussi des moyens de configurer des paramètres comme le `HelloInterval` ou comme le mot de passe, si on veut faire de l'auto-configuration mais en choisissant certains paramètres.)

Voilà, il ne reste plus qu'à déployer ces nouveaux réseaux : d'après les auteurs, il y a déjà deux ou trois mises en œuvre d'OSPF qui incorporent les règles de ce RFC.