RFC 7343 : An IPv6 Prefix for Overlay Routable Cryptographic Hash Identifiers Version 2 (ORCHIDv2)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 21 septembre 2014

Date de publication du RFC : Septembre 2014

https://www.bortzmeyer.org/7343.html

Une nouvelle pierre dans la construction d'une éventuelle future architecture Internet séparant identificateur et localisateur <https://www.bortzmeyer.org/separation-identificateur-localisateur.html>, les ORCHID sont des identificateurs dont la forme est celle d'une adresse IPv6 (afin de pouvoir être utilisés dans les API qui attendent des adresses IP). Ils sont typiquement utilisés dans le cadre de protocoles comme HIP (RFC 9063 [1]). Pour les distinguer, notre RFC réserve le préfixe `2001:20::/28`. Si vous voyez une telle « adresse IP », ne vous attendez pas à pouvoir forcément la « pinguer », elle n'a pas vocation à être routable, c'est un pur identificateur.

ORCHID signifie "*Overlay Routable Cryptographic Hash Identifiers*". L'adresse IP traditionnelle joue un rôle double, **localisateur** d'une machine dans le réseau et **identificateur** d'une machine. ORCHID est prévu pour les protocoles qui séparent identificateur et localisateur (comme HIP <https://www.bortzmeyer.org/hip-resume.html>) et sert d'identificateur. Leur forme physique est celle d'une adresse IPv6, afin de ne pas changer les API et les applications qui les utilisent (on peut publier des ORCHID dans le DNS, faire un `ssh 2001:20::1:42` si on est sur une machine HIP, etc). Bien sûr, il serait plus propre de tout refaire de zéro, avec de nouvelles API, plus adaptées à cette séparation identificateur/localisateur, mais c'est irréaliste. (Dommage, cela aurait permis d'utiliser tout le `::/0` pour ORCHID au lieu de les limiter à un préfixe. Voir la section 4 à ce sujet.)

Voilà pourquoi vous ne trouverez pas des adresses de ce préfixe dans les paquets IPv6 ordinaires (l'identificateur est traduit en localisateur par HIP avant que le paquet soit mis sur le câble). Les paquets ayant ces adresses sont routables dans le réseau virtuel HIP, pas dans l'Internet actuel. Les ORCHID sont donc utilisés « entre machines consentantes », dit le RFC. Un préfixe spécial, le `2001:20::/28`, est

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc9063.txt`

réservé par l'IANA pour éviter les confusions avec les « vraies » adresses IP. Il figure dans le registre des adresses spéciales <https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-s
xml> (RFC 6890). Cela permet aussi des choses comme une mise en œuvre de HIP sous forme d'un programme extérieur au noyau du système, utilisant le préfixe pour distinguer facilement les ORCHID, et permettre au noyau de transmettre les paquets utilisant des ORCHID à ce programme extérieur. Dans tous les cas, l'utilisation des ORCHID nécessitera un programme (dans le noyau ou extérieur) qui fera la correspondance entre les identificateurs maniés par les applications (les ORCHID) et les localisateurs mis dans l'en-tête des paquets IPv6 envoyés sur le réseau.

Les ORCHID ont été normalisés pour la première fois dans le RFC 4843. Ce nouveau RFC est la version 2, très différente (nouveau préfixe, nouvel algorithme de construction, voir l'annexe B pour toutes les différences entre ORCHID v1 et ORCHID v2).

Les ORCHID ont les propriétés suivantes :

— Quasi-unicité (sauf malchance, voir l'annexe A),
— Sécurité, via une chaîne de bits utilisée pour leur construction (la plupart du temps, une clé cryptographique, qui servira à authentifier l'ORCHID),
— Limitation au préfixe `2001:20::/28`,
— Routabilité dans l'"*overlay*", pas dans le réseau sous-jacent (l'Internet d'aujourd'hui).

Comme les adresses CGA (RFC 3972), les ORCHID sont en général utilisés avec de la cryptographie, la section 2 de notre RFC détaillant le mécanisme de construction d'un ORCHID. On part d'un certain nombre de paramètres, un OGA ID ("*ORCHID Generation Algorithm IDentifier*") qui identifie la fonction de hachage utilisée, un contexte qui identifie le protocole qui utilise ORCHID (la liste possible est à l'IANA <https://www.iana.org/assignments/cga-message-types>), une chaîne de bits et quelques autres. La chaîne de bits est censée être unique. En pratique, ce sera souvent une clé publique. Il y aura un contexte pour HIP, et un pour les futurs autres protocoles qui utiliseront ORCHID. On concatène chaîne de bits et contexte, on les condense et on a un identificateur de 96 bits de long. Il n'y a plus ensuite qu'à ajouter le préfixe `2001:20::/28` et l'identificateur OGA (4 bits) pour avoir l'ORCHID complet de 128 bits.

Maintenant qu'on a construit des ORCHID, comment s'en sert-on ? La section 3 décrit les questions de routage et de transmission. Les routeurs ne doivent pas traiter les ORCHID différemment des autres adresses IP par défaut (afin d'éviter de gêner le déploiement ultérieur de nouveaux usages des ORCHID). Par contre, ils peuvent être configurés pour les rejeter (on peut changer la configuration plus tard, mais c'est plus difficile pour le code), par exemple par une ACL.

La section 4 revient sur les décisions qui ont été prises pour la conception des ORCHID. La principale était la longueur du préfixe. Un préfixe plus court aurait laissé davantage de place pour le résultat de la fonction de condensation, résultat qu'on doit tronquer à 96 bits, au détriment de la sécurité. Mais cela aurait avalé une plus grande partie de l'espace d'adressage d'IPv6. Pour gagner des bits, le contexte (le protocole utilisé) n'est pas dans l'ORCHID lui-même mais dans les paramètres d'entrée qui seront condensés. On ne peut donc pas, en regardant un ORCHID, connaître le contexte (on peut connaitre la fonction de hachage utilisée, via l'OGA ID qui, lui, est dans l'ORCHID final). On ne peut que vérifier a posteriori que le contexte supposé était le bon. Cela comble un des principaux défauts d'ORCHID v1 (dans le RFC 4843), l'absence d'agilité cryptographique (la possibilité de changer d'algorithme suite aux progrès de la cryptanalyse). Par exemple, dans l'ancienne norme ORCHID, HIP était restreint à utiliser SHA-1.

Si vous vous lancez dans l'analyse sécurité d'ORCHID, regardez aussi la section 5. ORCHID dépend de la sécurité des fonctions de condensation (RFC 4270) pour garantir la liaison sécurisée entre une clé publique et l'ORCHID. La nécessité de tronquer leur résultat, pour tenir dans les 128 bits d'une adresse

IPv6 (moins le préfixe et le OGA ID) a affaibli ces fonctions (le RFC 6920, quoique parlant d'un sujet très différent, discutait déjà des conséquences de cette troncation).

L'annexe A du RFC, elle, se penche sur les risques de collision. Après tout, chaque ORCHID est censé être unique. Or, il n'y a pas de registre central des ORCHID : chacun les génère de son côté. Il n'y a donc qu'une unicité statistique : il est très improbable que deux machines génèrent le même ORCHID.

Et l'annexe B résume les différences entre les ORCHID v1 du RFC 4843 et les v2 de ce RFC 7343 :

— Mécanisme d'agilité cryptographique en mettant l'identificateur de l'algorithme (OGA ID) dans l'ORCHID,
— Suppression de plusieurs discussions intéressantes mais pas indispensables pour créer des ORCHID (voir le RFC 4843 si vous êtes curieux),
— Nouveau préfixe IPv6, `2001:20::/28`, remplaçant l'ancien `2001:10::/28`, désormais restitué à l'IANA et à nouveau libre. Les ORCHID v2 sont donc totalement incompatibles avec les v1.

Les programmeurs de HIP for Linux `<http://hipl.hiit.fi/>` et OpenHIP `<http://www.openhip.org/>` ont déjà promis de modifier leur code pour s'adapter à ces nouveaux ORCHID (qui sont désrmais dans la v2 de la norme HIP, RFC 7401).

Merci aux deux auteurs du RFC pour leur relecture de cet article.