Groupe de travail Réseau
Request for Comments : 4193
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

R. Hinden, Nokia
B. Haberman, JHU-APL

octobre 2005

Adresses IPv6 d'envoi individuel local uniques

Résumé
Le présent document définit un format d'adresse IPv6 en envoi individuel qui est unique au monde et est destiné aux communications locales, généralement à l'intérieur d'un site. Ces adresses ne sont pas supposées être acheminables sur l'Internet mondial.

Table des Matières

1. Introduction

Le présent document définit un format d'adresse IPv6 en envoi individuel qui est unique au monde et est destiné aux communications locales [RFC2460]. Ces adresses sont appelées adresses IPv6 d'envoi individuel local univoques et sont abrégées dans le présent document en adresses IPv6 locales. Elles ne sont pas supposées être acheminables sur l'Internet mondial. Elles sont acheminables à l'intérieur d'une zone plus limitée comme un site. Elles peuvent aussi être acheminées entre un ensemble limité de sites.

Les adresses IPv6 locales en envoi individuel ont les caractéristiques suivantes :
- Un préfixe unique au monde (avec une forte probabilité d'unicité).
- Un préfixe bien connu pour permettre un filtrage facile aux frontières du site.
- Elles permettent que les sites soient combinés ou interconnectés de façon privée sans créer de conflit d'adresses ou exiger de dénumérotage des interfaces qui utilisent ces préfixes.
- Indépendantes du fournisseur d'accès Internet et peuvent être utilisées pour les communications à l'intérieur d'un site sans avoir aucune connexité Internet permanente ou intermittente.
- Si une fuite accidentelle se produit à l'extérieur d'un site via l'acheminement ou le DNS, il n'y a pas de conflit avec une autre adresse.
- En pratique, les applications peuvent traiter ces adresses comme des adresses de portée mondiale.

Le présent document définit le format des adresses IPv6 locales, comment les allouer, et des considérations d'utilisation incluant l'acheminement, les routeurs de frontière de site, le DNS, la prise en charge d'application, l'usage de VPN, et des lignes directrices sur comment les utiliser pour une communication locale à l'intérieur d'un site.

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

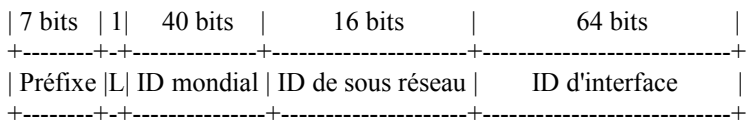
2. Remerciements

L'idée sous-jacente à la création des adresses IPv6 locales décrite dans le présent document a été proposée un certain nombre de fois par diverses personnes. Les auteurs du présent document ne revendiquent pas son exclusivité. Le mérite en revient à Brian Carpenter, Christian Huitema, Aidan Williams, Andrew White, Charlie Perkins, et de nombreux autres. Les auteurs tiennent aussi à remercier Brian Carpenter, Charlie Perkins, Harald Alvestrand, Keith Moore, Margaret Wasserman, Shannon Behrens, Alan Beard, Hans Kruse, Geoff Huston, Pekka Savola, Christian Huitema, Tim Chown, Steve Bellovin, Alex Zinin, Tony Hain, Bill Fenner, Sam Hartman, et Elwyn Davies de leurs commentaires et suggestions sur le présent document.

3. Adresses IPv6 d'envoi individuel local

3.1 Format

Les adresses IPv6 locales sont créées en utilisant un identifiant mondial alloué de façon pseudo aléatoire. Elles ont le format suivant :



Où :

Préfixe : préfixe FC00::/7 pour identifier les adresses IPv6 locales en envoi individuel.

L : réglé à 1 si le préfixe est alloué en local. Réglé à 0 pourra être défini à l'avenir. Voir au paragraphe 3.2 des informations supplémentaires.

ID mondial : identifiant mondial de 40 bits utilisé pour créer un préfixe unique au monde. Voir au paragraphe 3.2 des informations supplémentaires.

ID de sous réseau : identifiant de sous réseau de 16 bits pour identifier un sous réseau au sein du site.

ID d'interface : identifiant d'interface de 64 bits comme défini dans la [RFC3513].

3.1.1 Fondements

Il y a une gamme de choix disponibles pour la taille du préfixe et du champ Longueur d'identifiant mondial. Il y a un

compromis à faire entre avoir un champ Identifiant mondial assez grand pour prendre en charge la croissance future prévisible et ne pas utiliser trop d'espace d'adresses IPv6 sans nécessité. Une façon raisonnable d'évaluer la longueur d'un champ spécifique est de le comparer à une population mondiale projetée en 2050 de 9,3 milliards [POPUL] et le nombre de préfixes /48 résultants par personne. Une gamme de choix de préfixes est montrée dans le tableau suivant :

Préfixe	Longueur d'ID mondial	Nombre de préfixes /48	Préfixes par personne	% d'espace d'adresse IPv6
/11	37	137 438 953 472	15	0,049 %
/10	38	274 877 906 944	30	0,098 %
/9	39	549 755 813 888	59	0,195 %
/8	40	1 099 511 627 776	118	0,391 %
/7	41	2 199 023 255 552	236	0,781 %
/6	42	4 398 046 511 104	473	1,563 %

On peut supposer un très fort taux d'utilisation de ces allocations parce que le champ Identifiant mondial n'exige pas de structure interne, et il n'y a pas de raison d'être capable d'agréger les préfixes.

Les auteurs pensent qu'un préfixe /7 résultant en un espace d'identifiant mondial de 41 bits (incluant le bit L) est un bon choix. Cela assure un grand nombre d'allocations (c'est-à-dire, $2{,}2*10^{12}$) et en même temps utilise moins de 0,8 % de l'espace d'adresses IPv6 total. Il est peu probable que cet espace arrive à épuisement. Si il en fallait plus, de l'espace d'adresse IPv6 supplémentaire pourrait être alloué à cette fin.

3.2 Identifiant mondial

L'allocation des identifiants mondiaux est pseudo aléatoire [RFC4086]. Ils NE DOIVENT PAS être alloués en séquence ou avec des numéros bien connus. C'est pour assurer qu'il n'y aura pas de relation entre les allocations et pour aider à clarifier que ces préfixes ne sont pas destinés à un acheminement mondial. Précisément, ces préfixes ne sont pas conçus pour être agrégés.

Le présent document définit une méthode locale spécifique pour allouer les identifiants mondiaux, indiquée par le réglage du bit L à 1. Une autre méthode, indiquée par le bit L à zéro, pourra être définie ultérieurement. À part la méthode d'allocation, toutes les adresses IPv6 locales se comportent et sont traitées de façon identique.

Les allocations locales sont auto générées et n'ont besoin d'aucune coordination ou allocation centrale, mais ont une probabilité extrêmement forte d'être uniques.

3.2.1 Identifiants mondiaux alloués en local

Les identifiants mondiaux alloués en local DOIVENT être générés avec un algorithme pseudo aléatoire cohérent avec la [RFC4086]. Le paragraphe 3.2.2 décrit un algorithme suggéré. Il est important que tous les sites qui génèrent des identifiants mondiaux utilisent un algorithme fonctionnellement similaire pour assurer qu'il y a une forte probabilité d'unicité.

L'utilisation d'un algorithme pseudo aléatoire pour générer des identifiants mondiaux dans le préfixe d'allocation locale donne l'assurance que tout réseau numéroté en utilisant un tel préfixe a une très faible probabilité d'avoir un conflit d'adresse avec tout autre réseau qui aurait un autre préfixe d'allocation locale. C'est une propriété particulièrement utile lorsque on considère un certain nombre de scénarios, incluant des fusions de réseau, des espaces d'adresse de VPN qui se chevauchent, ou des hôtes mobiles entre de tels réseaux.

3.2.2 Exemple de code pour algorithme d'identifiant mondial pseudo aléatoire

L'algorithme décrit ci-dessous est destiné à être utilisé pour des identifiants mondiaux alloués en local. Dans chaque cas, l'identifiant mondial résultant sera utilisé dans le préfixe approprié comme défini au paragraphe 3.2.

1) Obtenir l'heure actuelle en format NTP à 64 bits [RFC1305].

2) Obtenir un identifiant EUI-64 du système qui fournit cet algorithme. Si un EUI-64 n'existe pas, on peut en créer un à partir de l'adresse MAC de 48 bits comme spécifié dans la [RFC3513]. Si un EUI-64 ne peut pas être obtenu ou créé, un identifiant univoque convenable, local pour le nœud, devrait être utilisé (par exemple, le numéro de série du système).

3) Enchaîner l'heure actuelle et l'identifiant spécifique du système afin de créer une clé.

4) Calculer le résumé SHA-1 de la clé comme spécifié dans [FIPS] et la [RFC3174] ; la valeur résultante fait 160 bits.

5) Utiliser les 40 bits de moindre poids comme identifiant mondial.

6) Enchaîner FC00::/7, le bit L réglé à 1, et les 40 bits de l'identifiant mondial pour créer un préfixe d'adresse IPv6 locale.

Cet algorithme va résulter en un identifiant mondial qui est raisonnablement unique et peut être utilisé pour créer un préfixe d'adresse IPv6 locale allouée en local.

3.2.3 Analyse de l'unicité des identifiants mondiaux

Le choix d'un identifiant mondial pseudo aléatoire est similaire au choix d'un identifiant SSRC dans RTP/RTCP défini au paragraphe 8.1 de la [RFC3550]. La présente analyse est adaptée de ce document.

Comme les identifiants mondiaux sont choisis au hasard (et de façon indépendante) il est possible que des réseaux séparés aient choisi le même identifiant mondiaL. Pour un réseau donné, avec un ou plusieurs identifiants mondiaux aléatoires, qui a des interconnexions avec d'autres réseaux semblables, ayant un total de N de ces identifiants, la probabilité que deux ou plus de ces identifiants soient identiques peut être approximée par la formule : "P = 1 - exp(-N**2 / 2**(L+1))" où P est la probabilité de collision, N est le nombre d'identifiants mondiaux interconnectés, et L est la longueur de l'identifiant mondial.

Le tableau suivant montre la probabilité d'une collision pour une gamme de connexions utilisant un champ Identifiant mondial de 40 bits.

Connexions	Probabilité de collision
2	1,81*10^-12
10	4,54*10^-11
100	4,54*10^-09
1000	4,54*10^-07
10000	4,54*10^-05

Sur la base de cette analyse, l'unicité des identifiants mondiaux générés en local est adéquate pour les sites qui prévoient une quantité petite à modérée de communications inter sites utilisent des identifiants mondiaux générés en local.

3.3 Définition de portée

Par défaut, la portée de ces adresses est mondiale. C'est-à-dire qu'elles ne sont pas limitées par des ambiguïtés comme les adresses de site local définies dans la [RFC3513]. Ces préfixes sont plutôt uniques au monde, et à ce titre, leur applicabilité est supérieure à celles des adresses de site local. Leur limitation est dans la capacité d'acheminement de leurs préfixes, qui est limitée à un site et à tout accord d'acheminement explicite avec d'autres sites pour les propager (voir aussi le paragraphe 4.1). À la différence des sites locaux, un site peut avoir plus d'un de ces préfixes et les utiliser en même temps.

4. Lignes directrices pour le fonctionnement

Les lignes directrices de cette section n'exigent aucun changement de l'acheminement normal ni des fonctionnalités de transmission d'un hôte ou routeur IPv6. Ce sont des directives de configuration et d'usage.

4.1 Acheminement

Les adresses IPv6 locales sont conçues pour être acheminées au sein d'un site de la même manière que les autres types d'adresses d'envoi individuel. Elles peuvent être portées dans tout protocole d'acheminement IPv6 sans aucun changement.

On s'attend à ce qu'elles partagent les mêmes identifiants de sous réseau que les adresses d'envoi individuel mondiales de fournisseur d'accès (FAI) avec lesquelles elles seraient utilisées concurremment [RFC3587].

Le comportement par défaut des sessions de protocole d'acheminement extérieur entre les régions administratives d'acheminement doit être d'ignorer la réception et ne pas annoncer les préfixes dans le bloc FC00::/7. Un opérateur de réseau peut spécifiquement configurer des préfixes plus longs que FC00::/7 pour les communications inter sites.

Si BGP est utilisé à la bordure du site avec un FAI, la configuration BGP par défaut doit filtrer tous les préfixes d'adresse IPv6 locales, aussi bien entrantes que sortantes. Elle doit être réglée à la fois à empêcher tout préfixe d'adresse IPv6 locale d'être annoncé à l'extérieur du site ainsi qu'à empêcher ces préfixes d'être appris d'un autre site. L'exception à cela est si elles sont des chemins /48 spécifiques ou plus longs créés pour un ou plusieurs préfixes IPv6 locaux.

Pour les protocoles de passerelle intérieure (IGP, *Interior Gateway Protocol*) d'état de liaison, il est suggéré qu'un site qui utilise des préfixes d'adresse IPv6 locales soit contenu dans un domaine ou zone d'IGP. En restreignant le préfixe d'adresse IPv6 locale à une seule zone ou domaine d'état de liaison, la distribution des préfixes peut être contrôlée.

4.2 Dénumérotage et fusion de sites

L'utilisation d'adresses IPv6 locales dans un site résulte à faire des communications qui utilisent ces adresses indépendamment du dénumérotage des adresses mondiales fondées sur le fournisseur de service d'un site.

Lors de la fusion de multiples sites, les adresses créées avec ces préfixes ont peu de chances de devoir être dénumérotées parce que toutes les adresses ont une forte probabilité d'unicité. Les chemins pour chaque préfixe spécifique devraient être configurés pour permettre que l'acheminement fonctionne correctement entre les sites anciennement séparés.

4.3 Routeur de bordure de site et filtrage de paquet par un pare-feu

Bien qu'aucun dommage sérieux ne puisse résulter de l'envoi de paquets avec ces adresses en dehors d'un site via un chemin par défaut, il est recommandé que les routeurs soient configurés par défaut à empêcher les paquets qui ont des adresses IPv6 locales de fuir hors du site et d'empêcher tout préfixe de site d'être annoncé en dehors de son site.

Les routeurs et pare-feu de bordure de site devraient être configurés à ne pas transmettre de paquets avec des adresses IPv6 de source ou destination locales en dehors du site, sauf si elles ont été explicitement configurées avec des informations d'acheminement sur des préfixes IPv6 locaux spécifiques /48 ou plus longs. Cela va assurer que les paquets qui ont des adresses IPv6 locales de destination ne seront pas transmis en dehors du site via un chemin par défaut. Le comportement par défaut de ces appareils devrait être d'installer un chemin de "rejet" pour ces préfixes. Les routeurs de bordure de site devraient répondre par le message ICMPv6 approprié "Destination injoignable" pour informer la source que le paquet n'a pas été transmis [RFC2463]. Ce retour est important pour éviter les fins de temporisation de protocole de transport.

Les routeurs qui entretiennent les arrangements d'échange de trafic entre systèmes autonomes à travers l'Internet devraient respecter les recommandations pour les routeurs de bordure de site, sauf si ils sont configurés autrement.

4.4 Problèmes relatifs au DNS

Pour l'instant, il n'est pas recommandé que les enregistrements AAAA et PTR pour les adresses IPv6 locales allouées en local soient installées dans le DNS mondial.

Sur les fondements de cette recommandation, un des soucis concernant l'ajout des enregistrements AAAA et PTR au DNS mondial pour les adresses IPv6 locales allouées en local découle de l'absence d'une assurance complète que les préfixes sont uniques. Il y a une faible possibilité que les mêmes adresses IPv6 locales allouées en local soient utilisées par deux organisations différentes prétendant toutes deux être d'autorité avec des contenus différents. Dans ce scénario, il est probable qu'il y aura une tentative de connexion à l'hôte le plus proche avec l'adresse IPv6 locale allouée en local correspondante. Il peut en résulter des fins de temporisation de connexion, des échecs de connexion indiqués par des messages ICMP "Destination injoignable", ou des connexions réussies sur le mauvais hôte. À cause de ce souci, l'ajout des enregistrements AAAA pour ces adresses au DNS global est estimé prématuré.

Les interrogations inverses (d'adresse à nom) pour les adresses IPv6 locales allouées en local NE DOIVENT PAS être envoyées aux serveurs de noms pour le DNS mondial, à cause de la charge que de telles interrogations créeraient pour les serveurs de noms d'autorité pour la zone ip6.arpa. Cette forme de charge d'interrogation n'est pas spécifique des adresses IPv6 locales allouées en local ; toute forme d'adressage local crée une charge supplémentaire de cette sorte, à cause des interrogations inverses qui sortent du site. Cependant, comme permettre que de telles interrogations s'échappent du site ne sert à rien d'utile, il n'y a aucune bonne raison pour empirer le problème de charge existant.

La façon recommandée d'éviter d'envoyer de telles interrogations aux serveurs de noms pour le DNS mondial est que les mises en œuvre de serveur de noms récurrents agissent comme si ils étaient d'autorité pour une zone d.f.ip6.arpa vide et retournent RCODE 3 pour toute interrogation de cette nature. Les mises en œuvre qui choisissent cette stratégie devraient permettre qu'elle soit outrepassée, mais retourner une réponse RCODE 3 pour de telles interrogations devrait être le comportement par défaut, à la fois parce que cela réduit le problème de la charge des interrogations et aussi parce que si

l'administrateur du site n'a pas établi l'arborescence inverse correspondant aux adresses IPv6 locales allouées en local utilisée, retourner le RCODE 3 est en fait la réponse correcte.

4.5 Problèmes d'application et de protocole de niveau supérieur

Les protocoles d'application et autres de niveau supérieur peuvent traiter les adresses IPv6 locales de la même manière que les autres types d'adresses d'envoi individuel mondiales. Aucun traitement particulier n'est requis. Ce type d'adresse peut n'être pas accessible, mais n'est pas différent des autres types d'adresse IPv6 d'envoi individuel mondiale. Les applications doivent être capables de traiter plusieurs adresses qui peuvent être ou non accessibles à tout moment. Dans la plupart des cas, cette complexité devrait être cachée dans les API.

Du point de vue de l'hôte, la différence entre IPv6 local et les autres types d'adresses d'envoi individuel mondiales apparaît comme une accessibilité différente et pourrait être traitée par défaut de cette façon. Dans certains cas, il vaut mieux pour les nœuds et les applications les traiter différemment des adresses d'envoi individuel mondiales. Un point de départ pourrait être de leur donner la préférence sur l'envoi individuel mondial, mais revenir à l'envoi individuel mondial si une destination particulière se trouve injoignable. En grande partie, ce comportement peut être contrôlé par la façon dont elles sont allouées aux nœuds et mises dans le DNS. Cependant, il est utile si un hôte peut avoir les deux types d'adresses et les utiliser de façon appropriée.

Noter que les mécanismes de choix d'adresse de la [RFC3484], et en particulier le mécanisme d'outrepassement de politique qui remplace le choix d'adresse par défaut, sont supposés être utilisés sur un site où les adresses IPv6 locales sont configurées.

4.6 Utilisation d'adresses IPv6 locales pour les communications locales

Les adresses IPv6 locales, comme les adresses d'envoi individuel de portée mondiale, ne sont allouées aux nœuds que si leur utilisation a été activée (via l'autoconfiguration d'adresse IPv6 [RFC2462], DHCPv6 [RFC3315], ou manuellement). Elles ne sont pas créées automatiquement comme le sont les adresses IPv6 de liaison locale et ne vont pas apparaître ou être utilisées sauf si elles sont configurées à cette fin.

Pour que les hôtes autoconfigurent les adresses IPv6 locales, les routeurs doivent être configurés à annoncer les préfixes /64 IPv6 locaux dans les annonces de routeur, ou un serveur DHCPv6 doit avoir été configuré à les allouer. Pour qu'un nœud apprenne l'adresse IPv6 locale d'un autre nœud, l'adresse IPv6 locale doit avoir été installée dans un système de désignation (par exemple, le DNS, un système de désignation propriétaire, etc.). Pour ces raisons, le contrôle de leur usage dans un site est direct.

Pour limiter l'utilisation des adresses IPv6 locales, les directives suivantes s'appliquent :

- Nœuds qui ne sont accessible qu'à l'intérieur d'un site : le DNS local devrait être configuré à seulement inclure les adresses IPv6 locales de ces nœuds. Les nœuds qui ont seulement des adresses IPv6 locales ne doivent pas être installés dans le DNS mondial.

- Nœuds qui sont limités à ne communiquer qu'avec d'autres nœuds sur le site : ces nœuds devraient être réglés à seulement autoconfigurer des adresses IPv6 locales via la [RFC2462] ou à seulement recevoir des adresses IPv6 locales via la [RFC3315]. Noter que pour le cas où les deux préfixes IPv6 mondiaux et locaux sont annoncés sur un sous réseau, cela va exiger qu'un commutateur dans l'appareil autoconfigure seulement les adresses IPv6 locales.

- Nœuds qui sont accessibles de l'intérieur du site et de l'extérieur du site : le DNS devrait être configuré à inclure les adresses mondiales de ces nœuds. Le DNS local peut être configuré à aussi inclure les adresses IPv6 locales de ces nœuds.

- Nœuds qui peuvent communiquer avec d'autres nœuds à l'intérieur du site et à l'extérieur du site : ces nœuds devraient autoconfigurer des adresses mondiales via la [RFC2462] ou recevoir une adresse mondiale via la [RFC3315]. Ils peuvent aussi obtenir des adresses IPv6 locales via les mêmes mécanismes.

4.7 Utilisation d'adresses IPv6 locales avec des VPN

Les adresses IPv6 locales peuvent être utilisées pour des réseaux virtuels privés (VPN, *Virtual Private Network*) inter site si des chemins appropriés sont établis. Parce que les adresses sont uniques, ces VPN vont travailler de façon fiable et sans qu'il soit besoin de traduction. Ils ont la propriété supplémentaire de continuer à travailler si les sites individuels sont dénumérotés ou fusionnés.

5. Considérations d'acheminement global

Le paragraphe 4.1 donne des directives de fonctionnement qui interdisent l'acheminement par défaut des adresses locales entre sites. Des problèmes ont été soulevés dans le groupe de travail IPv6 et à l'IETF en général sur le fait que les sites peuvent tenter d'utiliser les adresses locales comme des adresses d'acheminement mondial indépendantes du fournisseur d'accès. Cette section décrit pourquoi l'utilisation d'adresses locales comme des adresses d'acheminement mondial indépendantes du fournisseur d'accès est déconseillée.

5.1 Du point de vue de l'Internet

Il y a une discordance entre la structure des adresses IPv6 locales et le modèle normal d'acheminement de large zone IPv6. Le préfixe /48 des adresses IPv6 locales ne rentre nulle part dans la hiérarchie normale des adresses IPv6 en envoi individuel. Les adresses d'envoi individuel IPv6 normales peuvent être acheminées en descendant la hiérarchie jusqu'au niveau du sous réseau physique (liaison) et avoir seulement à être acheminées à plat sur le sous réseau physique. Les adresses IPv6 locales devraient être acheminées à plat même sur l'Internet large zone.

Donc, les paquets dont l'adresse de destination est une adresse IPv6 locale ne pourraient être acheminées sur la large zone que si le préfixe /48 correspondant était porté par le protocole d'acheminement de large zone utilisé, comme BGP. Cela contrevient aux hypothèses de fonctionnement selon lesquelles les longs préfixes seront agrégés en beaucoup moins de préfixes courts, pour limiter la taille de tableau et le temps de convergence du protocole d'acheminement. Si un réseau utilise à la fois les adresses IPv6 normales de la [RFC3513] et les adresses IPv6 locales, ces types d'adresses ne vont certainement pas s'agréger les uns avec les autres, car ils diffèrent à partir du bit de plus fort poids. Et les adresses IPv6 locales ne vont pas s'agréger les unes aux autres, à cause de leurs schémas aléatoires de bits. Cela signifie qu'il y aurait une pénalisation très significative du fonctionnement à tenter d'utiliser les préfixes d'adresses IPv6 locales génériques avec la technologie actuellement connue pour l'acheminement de large zone.

5.2 Du point de vue d'un site

Il y a un certain nombre de facteurs de conception dans les adresses IPv6 locales qui réduisent la probabilité qu'elles soient utilisées comme adresses d'envoi individuel mondiales arbitraires. Cela inclut :

- Les règles par défaut pour filtrer les paquets et les chemins rendent très difficile d'utiliser les adresses IPv6 locales pour un usage arbitraire à travers l'Internet. Pour qu'un site les utilise comme adresses d'envoi individuel générales, il faudrait s'assurer que les règles par défaut ne sont pas utilisées par tous les autres sites et FAI intermédiaires pour leurs communications actuelles et futures.

- Il n'est pas mathématiquement garanti qu'elles soient uniques et ne soient pas enregistrées dans des bases de données publiques. Les collisions, bien que très improbables, sont possibles et une collision peut compromettre l'intégrité des communications. Le manque d'enregistrement public crée des problèmes de fonctionnement.

- Les adresses sont allouées au hasard. Si un site a plusieurs préfixes qu'il veut utiliser mondialement, le coût de leur annonce serait très élevé parce qu'ils ne peuvent pas être agrégés.

- Elles on un long préfixe (c'est-à-dire, /48) de sorte qu'un seul préfixe d'adresse locale ne fournit pas assez d'espace d'adresse pour être utilisé exclusivement par les plus grandes organisations.

6. Avantages et inconvénients

6.1 Avantages

Cette approche a les avantages suivants :

- Fournir des préfixes IPv6 locaux qui peuvent être utilisés de façon indépendante de toute allocation d'adresse IPv6 d'envoi individuel s'appuyant sur un fournisseur. Ceci est utile pour des sites qui ne sont pas toujours connectés à l'Internet ou des sites qui souhaitent avoir un préfixe distinct qui pourrait être utilisé pour localiser du trafic à l'intérieur du site.

- Les applications peuvent traiter ces adresses d'une façon identique à celle de tout autre type d'adresses IPv6 d'envoi individuel mondiales.

- Des sites peuvent être fusionnés sans aucun dénumérotage des adresses IPv6 locales.

- Les sites peuvent changer leur adresse IPv6 d'envoi individuel fondée sur le fournisseur sans interrompre de communication qui utilise les adresses IPv6 locales.

- Un préfixe bien connu qui permet un filtrage aisé à la frontière du site.

- Peut être utilisée pour les VPN inter sites.

- Si il y a une fuite accidentelle en dehors d'un site via l'acheminement ou le DNS, il n'y a pas de conflit avec d'autres adresses.

6.2 Inconvénients

Cette approche présente les inconvénients suivants :

- Il n'est pas possible d'acheminer les préfixes IPv6 locaux sur l'Internet mondial avec la technologie d'acheminement actuelle. Par conséquent, il est nécessaire d'avoir le comportement par défaut des routeurs frontière de site pour filtrer ces adresses.

- Il y a une très faible probabilité de non unicité des identifiants mondiaux alloués en local générés par l'algorithme du paragraphe 3.2.3. Ce risque peut être ignoré pour toutes les questions pratiques, mais cela conduit à un risque théorique de conflit de préfixes d'adresses.

7. Considérations pour la sécurité

Les adresses IPv6 locales ne fournissent aucune sécurité inhérente aux nœuds qui les utilisent. Elles peuvent être utilisées avec des filtres aux frontières de site pour garder le trafic IPv6 local à l'intérieur du site, mais ceci n'est ni plus ni moins sûr que de filtrer tout autre type d'adresse IPv6 mondiale en envoi individuel.

Les adresses IPv6 locales permettent bien des mécanismes de sécurité fondés sur l'adresse, incluant IPsec, à travers les connexions de bout en bout de VPN

8. Considérations relatives à l'IANA

L'IANA a alloué le préfixe FC00::/7 à "Unique Local Unicast".

9. Références

9.1 Références normatives

[FIPS] Federal Information Processing Standards Publication, (FIPS PUB) 180-1, "Secure Hash Standard", 17 avril 1995.

[RFC1305] D. Mills, "Protocole de l'heure du réseau, version 3, spécification, mise en œuvre et analyse", STD 12, mars 1992. *(Remplacée par* RFC5905)

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC2460] S. Deering et R. Hinden, "Spécification du protocole Internet, version 6 (IPv6)", décembre 1998. *(MàJ par* 5095, 6564 *; D.S ; Remplacée par* RFC8200, STD 86*)*

[RFC2463] A. Conta, S. Deering, "Protocole de message de contrôle Internet (ICMPv6) pour le protocole Internet version 6 (IPv6)", décembre 1998. (*Obsolète, voir* RFC4443) *(D.S.)*

[RFC3174] D. Eastlake 3 et P. Jones, "Algorithme US de hachage sécurisé n° 1 (SHA1)", sept. 2001. *(Info, MàJ par 4634 et 6234)*

[RFC3513] R. Hinden et S. Deering, "Architecture d'adressage du protocole Internet version 6 (IPv6)", avril 2003. (*Obs. voir* RFC4291)

[RFC3587] R. Hinden, S. Deering, E. Nordmark, "Format mondial d'adresse IPv6 en envoi individuel", août 2003. *(Information)*

[RFC4086] D. Eastlake 3rd, J. Schiller, S. Crocker, "Exigences d'aléa pour la sécurité", juin 2005. (*Remplace* RFC1750) (BCP0106)

9.2 Références pour information

[POPUL] Population Reference Bureau, "World Population Data Sheet of the Population Reference Bureau 2002", août 2002.

[RFC2462] S. Thomson, T. Narten, "Autoconfiguration d'adresse IPv6 sans état", décembre 1998. (*Obsolète, voir* RFC4862) *(D.S.)*

[RFC3315] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins et M. Carney, "Protocole de configuration dynamique d'hôte pour IPv6 (DHCPv6)", juillet 2003. (*MàJ par* RFC6422 et RFC6644, RFC7227 *; rendue obsolète par* RFC8415)

[RFC3484] R. Draves, "Choix d'adresse par défaut pour le protocole Internet version 6 (IPv6)", février 2003. (*Remplacée par la* RFC6724) *(P.S.)*

[RFC3550] H. Schulzrinne, S. Casner, R. Frederick et V. Jacobson, "RTP : un protocole de transport pour les applications en temps réel", STD 64, juillet 2003. *(MàJ par* RFC7164, RFC7160, RFC8083, RFC8108)

Adresse des auteurs

Robert M. Hinden
Nokia
313 Fairchild Drive
Mountain View, CA 94043
USA
téléphone : +1 650 625-2004
mél : bob.hinden@nokia.com

Brian Haberman
Johns Hopkins University
Applied Physics Lab
11100 Johns Hopkins Road
Laurel, MD 20723
USA
téléphone : +1 443 778 1319
mél : brian@innovationslab.net

Déclaration complète de droits de reproduction

mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr .

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf- ipr@ietf.org .

Remerciement
Le financement de la fonction d'édition des RFC est actuellement fourni par la Internet Society.