Groupe de travail Réseau
Request for Comments : 4429
Catégorie : Sur la voie de la normalisation

N. Moore, Monash University CTIE
avril 2006
Traduction Claude Brière de L'Isle

Détection optimiste d'adresse dupliquée (DAD) pour IPv6

Statut de ce mémoire

Le présent document spécifie un protocole de l'Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Normes officielles des protocoles de l'Internet" (STD 1) pour connaître l'état de la normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé

La détection optimiste d'adresse dupliquée est une modification interopérable de la découverte de voisin IPv6 existante (RFC 2461) et du processus d'autoconfiguration d'adresse sans état (RFC 2462). L'intention est de minimiser les délais de configuration d'adresse dans le cas de succès, de réduire l'interruption autant que possible en cas d'échec, et de rester interopérable avec des hôtes et routeurs non modifiés.

Table des matières

1. Introduction

La détection optimiste d'adresse dupliquée (DAD, *Duplicate Address Detection*) est une modification des processus existants de découverte de voisin IPv6 (ND, *Neighbor Discovery*) [RFC2461] et d'autoconfiguration d'adresse sans état (SLAAC, *Stateless Address Autoconfiguration*) [RFC2462]. L'intention est de minimiser les délais de configuration d'adresse dans le cas de succès, de réduire l'interruption autant que possible en cas d'échec.

DAD optimiste est une optimisation utile parce que dans la plupart des cas, DAD a beaucoup plus de chances de réussir que d'échouer. Ceci est discuté plus en détails à l'Appendice A. L'interruption est minimisée en limitant la participation des nœuds à la découverte de voisin alors que leurs adresses sont encore optimistes.

Il n'est pas dans les intentions du présent mémoire d'améliorer la sécurité, la fiabilité, ou la robustesse de DAD au delà des normes existantes, mais simplement de fournir une méthode de la rendre plus rapide.

1.1 Position du problème

Les mécanismes existants de configuration d'adresse IPv6 fournissent des mécanismes adéquats de détection de collision pour les hôtes fixes pour lesquels ils ont été conçus. Cependant, une population croissante de nœuds a besoin de maintenir un accès réseau continu en dépit des changements fréquents de leur rattachement réseau. Des optimisations au processus de DAD sont nécessaires pour fournir à ces nœuds une configuration d'adresse suffisamment rapide.

Une méthode de DAD optimisée a besoin de :
* fournir l'interopérabilité avec les nœuds qui utilisent les normes actuelles,
* supprimer le délai de RetransTimer *(temporisateur de retransmission)* durant la configuration d'adresse,
* assurer que la probabilité de collision de l'adresse n'est pas augmentée,
* améliorer les mécanismes de résolution pour les collisions d'adresse,
* minimiser l'interruption dans le cas de collision.

Il n'est pas suffisant de simplement réduire RetransTimer afin de réduire le délai de transfert inter cellulaire, car les valeurs de RetransTimer assez longues pour garantir la détection d'une collision sont trop longues pour éviter l'interruption des services pour lesquels le temps est critique.

1.2 Définitions

Les définitions des mots clés des exigences ("NE DOIT PAS", "NE DEVRAIT PAS", "PEUT", "DEVRAIT", "DOIT"') sont conformes aux BCP 14, [RFC2119]

Résolution d'adresse - processus défini au paragraphe 7.2 de la [RFC2461].

Détection d'inaccessibilité de voisin (NUD, *Neighbor Unreachability Detection*) - processus défini au paragraphe 7.3 de la [RFC2461].

Nœud standard - nœud conforme aux [RFC2461] et [RFC2462].

Nœud optimiste (ON, *nœud optimiste*) - nœud conforme aux règles spécifiées dans le présent mémoire.

Liaison - facilité ou support de communication sur lequel les nœuds peuvent communiquer à la couche liaison.

Voisins - nœuds sur la même liaison, qui peuvent donc être en compétition pour la même adresse IP.

1.3 Types d'adresse

Tentative d'adresse (selon la [RFC2462]) - adresse dont l'unicité sur une liaison est vérifiée avant son allocation à une interface. Une tentative d'adresse n'est pas considérée comme allouée à une interface au sens usuel. Une interface élimine les paquets reçus adressés à une tentative d'adresse, mais accepte les paquets de découverte de voisin en rapport avec la détection d'adresse dupliquée pour la tentative d'adresse.

Adresse optimiste - adresse qui est allouée à une interface et disponible à l'utilisation, sous réserve de restrictions, pendant

qu'est vérifiée son unicité sur une liaison. Le présent mémoire introduit l'état optimiste et définit son comportement et les restrictions.

Adresse préférée (selon la [RFC2462]) - adresse allouée à une interface dont l'utilisation par les protocoles de couche supérieure n'est pas restreinte. Les adresses préférées peuvent être utilisées comme adresse de source (ou destination) des paquets envoyés de (ou à) l'interface.

Adresse déconseillée (selon la [RFC2462]) - adresse allouée à une interface dont l'utilisation est déconseillée, mais pas interdite. Une adresse déconseillée ne devrait plus être utilisée comme adresse de source dans de nouvelles communications, mais les paquets envoyés de ou à des adresses déconseillées sont livrés comme attendu. Une adresse déconseillée peut continuer d'être utilisée comme adresse de source dans les communications où le passage à une adresse préférée cause des difficultés à une activité spécifique de couche supérieure (par exemple, une connexion TCP existante).

1.4 Abréviations

DAD *(Duplicate Address Detection)* : détection d'adresse dupliquée. Technique utilisée pour SLAAC. Voir au paragraphe 5.4 de la [RFC2462].

Redirection ICMP - voir au paragraphe 4.5 de la [RFC2461].

NA *(Neighbor Advertisement)* : annonce de voisin. Voir au paragraphe 4.3 et à la Section 7 de la [RFC2461].

NC *(Neighbor Cache)* : antémémoire de voisins. Voir les paragraphes 5.1 et 7.3 de la [RFC2461].

ND *(Neighbor Discovery)* : découverte de voisins. Processus décrit dans la [RFC2461].

NS *(sollicitation de voisin)* : sollicitation de voisins. Voir au paragraphe 4.3 et à la Section 7 de la [RFC2461].

RA *(Router Advertisement)* : annonce de routeur. Voir au paragraphe 4.2 et à la Section 6 de la [RFC2462].

RS (Router Solicitation) : sollicitation de routeur. Voir au paragraphe 4.1 et à la Section 6 de la [RFC2461]..

SLAAC *(StateLess Address AutoConfiguration)* : autoconfiguration d'adresse sans état. Processus décrit dans la [RFC2462].

SLLAO *(Source Link-Layer Address Option)* : option d'adresse de source de couche liaison. Option des messages NS, RA, et RS, qui donne l'adresse de couche liaison de la source du message. Voir au paragraphe 4.6.1 de la [RFC2461].

TLLAO *(Target Link-Layer Address Option)* : option d'adresse cible de couche liaison. Option des messages de redirection ICMP et des annonces de voisin. Voir les paragraphes 4.4, 4.5, et 4.6.1 de la [RFC2461].

2. Comportements de DAD optimiste

Cette Section non normative expose les comportements de DAD optimiste.

2.1 Adresses optimistes

La [RFC2462] introduit le concept de tentative d'adresse (en 5.4) et d'adresse déconseillée (en 5.5.4). Les adresses qui ne sont ni de tentative ni déconseillées sont dites préférées. Les tentatives d'adresses ne peuvent pas être utilisées pour la communication, et les adresses déconseillées ne devraient pas être utilisées pour de nouvelles communications. Ces états d'adresses peuvent aussi être utilisés par d'autres documents de normalisation, par exemple, le choix d'adresse par défaut [RFC3484].

Le présent mémoire introduit un nouvel état d'adresse, "Optimiste", qui est utilisé pour marquer une adresse qui est disponible à l'utilisation mais qui n'a pas achevé la DAD.

Sauf notation contraire, les composants de la pile de protocoles IPv6 devraient traiter les adresses dans l'état optimiste de façon équivalente à celles qui sont dans l'état déconseillé, indiquant que l'adresse est disponible à l'utilisation mais ne

devrait pas être utilisée si une autre adresse convenable est disponible. Par exemple, le choix d'adresse par défaut [RFC3484] utilise l'état d'adresse pour décider quelle adresse de source utiliser pour un paquet sortant. Les mises en œuvre devraient traiter une adresse dans l'état optimiste comme si elle était dans l'état déconseillé. Si les états d'adresse sont enregistrés comme des fanions individuels, cela peut être facilement réalisé en réglant aussi "déconseillé" quand "optimiste" est établi.

Il est important de noter que les règles de durée de vie d'adresse de la [RFC2462] s'appliquent encore, et donc qu'une adresse peut être déconseillé aussi bien qu'optimiste. Quand DAD s'achève sans incident, l'adresse devient soit préférée, soit déconseillée, selon la [RFC2462].

2.2 Évitement d'interruption

Afin d'éviter les interférences, il est important qu'un nœud optimiste n'envoie aucun message à partir d'une adresse optimiste qui va écraser les entrées d'antémémoire de voisin (NC, *Neighbor Cache*) de ses voisins pour l'adresse qu'il essaye de configurer : le faire interromprait le possesseur légitime de l'adresse en cas de collision.

Cela se fait en :

* Réglant à zéro de fanion "Outrepasser" dans les annonces de voisin des adresses optimistes, ce qui empêche les voisins d'écraser leurs entrées de NC existantes. Le fanion "Outrepasser" est déjà défini dans la [RFC2461] et utilisé pour l'annonce de voisin mandataire.

* Ne jamais envoyer de sollicitations de voisin à partir d'une adresse optimiste. Les NS incluent une option d'adresse de source de couche liaison (SLLAO, *Source Link-Layer Address Option*) qui peut causer l'interruption de l'antémémoire de voisin. Les NS envoyées au titre de DAD le sont à partir de l'adresse inspécifiée, sans SLLAO.

* Ne jamais utiliser une adresse optimiste comme adresse de source d'une Sollicitation de routeur avec une SLLAO. Une autre adresse, ou l'adresse inspécifiée, doit être utilisée, ou la RS peut être envoyée sans SLLAO.

Une collision d'adresse avec un routeur peut causer la mise à zéro des fanions IsRouter des routeur du voisinage pour cette adresse. Cependant, les routeurs n'utilisent jamais le fanion IsRouter, et la NA envoyée en réponse à la collision va rétablir le fanion IsRouter.

2.3 Redirection de routeur

Les sollicitations de voisin ne peuvent pas être envoyées à partir des adresses optimistes, et donc un ON ne peut pas contacter directement un voisin qui n'est pas déjà dans son antémémoire de voisin. À la place, le ON transmet les paquets via son routeur par défaut, s'appuyant sur le routeur pour transmettre les paquets à leur destination. Conformément à la RFC 2461, le routeur devrait alors fournir à l'ON une Redirection ICMP, qui peut inclure une option d'adresse cible de couche de liaison (TLLAO, *Target Link-Layer Address Option*). Si il le fait, cela va mettre à jour la NC de l'ON, et une communication directe peut commencer. Si il ne le fait pas, les paquets vont continuer d'être transmis via le routeur jusqu'à ce que l'ON ait une adresse non optimiste à partir de laquelle envoyer une NS.

2.4 Contact du routeur

Généralement, une RA va inclure une SLLAO, cependant, cela "PEUT être omis pour faciliter l'équilibrage de charges entrantes sur les interfaces dupliquées" [RFC2461]. Un nœud qui a seulement des adresses optimistes est dans l'incapacité de déterminer l'adresse de couche de liaison du routeur car il ne peut ni envoyer une RS pour demander une RA en envoi individuel, ni envoyer une NS pour demander une NA. Dans ce cas, l'ON va être incapable de communiquer avec le routeur jusqu'à ce qu'au moins une de ses adresses ne soit plus optimiste.

3. Modifications au comportement obligatoire des RFC

Tout le texte normatif du présent mémoire est contenu dans cette Section.

3.1 Généralités

* Une DAD optimiste DEVRAIT n'être utilisée que lorsque la mise en œuvre sait que l'adresse se fonde sur un identifiant d'interface très probablement unique (comme dans la [RFC2464]) généré de façon aléatoire [RFC3041], ou par une fonction de hachage bien répartie [RFC3972] ou alloué par le protocole de configuration dynamique d'hôte pour IPv6 (DHCPv6, *Dynamic Host Configuration Protocol for IPv6*) [RFC3315]. Une DAD optimiste NE DEVRAIT PAS être utilisée pour des adresses entrées manuellement.

3.2 Modifications à la découverte de voisin de la RFC 2461

* (modifie le paragraphe 6.3.7) Un nœud NE DOIT PAS envoyer une sollicitation de routeur avec une SLLAO à partir d'une adresse optimiste. Les sollicitations de routeur DEVRAIENT être envoyées à partir d'une adresse non optimiste ou de l'adresse inspécifiée ; cependant, elles PEUVENT être envoyées à partir d'une adresse optimiste si la SLLAO n'est pas incluse.

* (modifie le paragraphe 7.2.2) Un nœud NE DOIT PAS utiliser une adresse optimiste comme adresse de source d'une sollicitation de voisin.

* Si la SLLAO du routeur dans une RA n'est pas dite à l'ON, et si il ne peut pas déterminer ces informations sans enfreindre les règles ci-dessus, il DOIT laisser la tentative d'adresse jusqu'à ce que la DAD s'achève en dépit de son incapacité à envoyer des paquets au routeur.

* (modifie le paragraphe 7.2.2) Quand un nœud a un paquet à envoyer en envoi individuel à partir d'une adresse optimiste à un voisin, mais qu'il ne connaît pas l'adresse de couche de liaison du voisin, il NE DOIT PAS effectuer la résolution d'adresse. Il DEVRAIT transmettre le paquet à un routeur par défaut sur la liaison dans l'espoir que le paquet sera redirigé. Autrement, il DEVRAIT mettre le paquet dans une mémoire tampon jusqu'à ce que la DAD soit achevée.

3.3 Modifications à l'autoconfiguration d'adresse sans état de la RFC 2462

* (modifie le paragraphe 5.5) Un hôte PEUT choisir de configurer une nouvelle adresse comme adresse optimiste. Un hôte qui ne connaît pas la SLLAO de son routeur NE DEVRAIT PAS configurer une nouvelle adresse comme optimiste. Un routeur NE DEVRAIT PAS configurer une adresse optimiste.

* (modifie le paragraphe 5.4.2) L'hôte DOIT joindre l'adresse de diffusion groupée "Tous les nœuds" et l'adresse de diffusion groupée de nœud sollicité de la tentative d'adresse. L'hôte NE DEVRAIT PAS attendre avant d'envoyer des messages de sollicitation de voisin.

* (modifie le paragraphe 5.4) L'adresse optimiste est configurée et disponible pour être utilisée immédiatement sur l'interface. L'adresse DOIT avoir le fanion "Optimiste".

* Quand la DAD s'achève pour une adresse optimiste, l'adresse n'est plus optimiste et elle devient préférée ou déconseillée selon les règles de la RFC 2462.

* (modifie le paragraphe 5.4.3) Le nœud NE DOIT PAS répondre à une sollicitation de voisin pour une adresse optimiste provenant de l'adresse inspécifiée. La réception d'une telle NS indique que l'adresse est un dupliqué, et elle DOIT être déconfigurée selon le comportement spécifié dans la RFC 2462 pour les Tentatives d'adresses.

* (modifie le paragraphe 5.4.3) Le nœud DOIT répondre à une sollicitation de voisin pour une adresse optimiste provenant d'une adresse d'envoi individuel, mais la réponse DOIT avoir le fanion Outrepasser à zéro (O=0).

4. Fonctionnement du protocole

Cette section non normative apporte des précisions sur les interactions entre les nœuds optimistes, et entre les nœuds optimistes et les nœuds standard.

Les cas suivants considèrent tous un nœud optimiste (ON) qui reçoit une annonce de routeur contenant un nouveau préfixe et qui décide d'auto configurer une nouvelle adresse optimiste sur ce préfixe.

L'ON va immédiatement envoyer une sollicitation de voisin pour déterminer si sa nouvelle adresse optimiste est déjà utilisée.

4.1 Cas simple

Dans le cas de non collision, l'adresse optimiste configurée par le nouveau nœud n'est pas utilisée et n'est pas présente dans les antémémoires de voisin d'un de ses voisins.

Il n'y aura pas de réponse à sa NS (envoyée de ::) et cette NS ne va pas modifier l'état des antémémoires de voisin de ses voisins.

L'ON a déjà l'adresse de couche de liaison du routeur (provenant de la RA) et le routeur peut déterminer l'adresse de couche de liaison de l'ON par la résolution d'adresse standard. Les communications peuvent commencer aussitôt que le routeur et l'ON ont l'adresse de couche de liaison de l'autre.

Après l'achèvement du délai de DAD approprié, l'adresse n'est plus optimiste, et devient préférée ou déconseillée conformément à la RFC 2462.

4.2 Cas de collision

Dans le cas de collision, l'adresse optimiste configurée par le nouveau nœud est déjà utilisée par un autre nœud, et est présente dans les antémémoires de voisins (NC, *Neighbor Cache*) des voisins qui communiquent avec ce nœud.

La NS envoyée par l'ON a l'adresse de source inspécifiée, ::, et pas de SLLAO. Cette NS ne va pas causer de changement des entrées de NC des hôtes voisins.

L'ON va heureusement déjà savoir tout ce dont il a besoin sur le routeur d'après la RA initiale. Cependant, si il en a besoin il peut toujours envoyer une RS pour demander plus d'informations, mais il ne doit pas inclure de SLLAO. Cela force une réponse de diffusion groupée à tous les nœuds de la part du routeur, mais ne va pas perturber les NC des autres nœuds.

Dans le cours de l'établissement de connexions, l'ON peut avoir envoyé des NA en réponse aux NS reçues. Comme les NA envoyées à partir des adresses optimistes ont O=0, elles n'auront pas outrepassé les entrées existantes de NC, bien qu'il ait pu en résulter une entrée en collision qui change pour l'état PÉRIMÉ. Ce changement est récupérable par une NUD standard.

Quand une NA est reçue de celui qui défend l'adresse, l'ON arrête immédiatement d'utiliser l'adresse et la déconfigure.

Bien sûr, pendant ce temps l'ON peut avoir envoyé des paquets qui l'identifient comme possesseur de sa nouvelle adresse optimiste (par exemple, mise à jour de liens dans IPv6 mobile [RFC3775]). Cela peut pénaliser l'ON, sous la forme de connexions rompues, et pénaliser le possesseur légitime de l'adresse, car il va recevoir les paquets mal dirigés (et éventuellement y répondre). C'est pour cette raison que la DAD optimiste ne devrait être utilisée que lorsque la probabilité de collision est très faible.

4.3 Cas d'interopération

Une fois que l'adresse optimiste a achevé la DAD, elle agit exactement comme une adresse normale, et donc les cas d'interopération ne se produisent que lorsque l'adresse est optimiste.

Si un ON tente de configurer une adresse actuellement en tentative allouée à un nœud standard, celui-ci va voir la sollicitation de voisin et déconfigurer l'adresse.

Si un nœud tente de configurer l'adresse optimiste d'un ON, celui-ci va voir la NS et déconfigurer l'adresse.

4.4 Cas pathologiques

La DAD optimiste souffre de problèmes similaires à ceux de la DAD standard ; par exemple, il n'est pas garanti que les adresses dupliquées soient détectées si des paquets sont perdus.

Ces problèmes existent, et ne sont pas récupérables en douceur dans la DAD standard. Leur probabilité dans la DAD optimiste aussi bien que standard peut être réduite en augmentant la variable DupAddrDetectTransmits de la RFC 2462 au delà de 1.

Cette version de la DAD optimiste dépend des détails du comportement du routeur, par exemple, si le routeur inclut des SLLAO dans les RA et si le routeur accepte de rediriger le trafic pour l'ON. Lorsque le routeur ne se comporte pas de cette façon, le comportement de la DAD optimiste revient inexorablement à celui de la DAD standard.

5. Considérations sur la sécurité

Il existe des problèmes de sécurité concernant la découverte de voisin et l'autoconfiguration d'adresse sans état, et le présent mémoire ne prétend pas les régler. Cependant, il n'augmente pas non plus de façon significative ces problèmes de sécurité.

La découverte de voisin sécurisée (SEND, *Secure Neighbor Discovery*) [RFC3971] assure la protection contre les menaces sur la découverte de voisin décrites dans la [RFC3756]. La détection d'adresse dupliquée optimiste n'introduit aucune menace supplémentaire à la découverte de voisin si SEND est utilisé.

La DAD optimiste prend des mesures pour assurer que si un autre nœud utilise déjà une adresse, l'adresse appropriée de couche de liaison dans les entrées d'antémémoires de voisin n'est pas remplacée par l'adresse de couche de liaison du nœud optimiste. Cependant, il y a encore des scénarios où des entrées incorrectes peuvent être créées, même si c'est seulement temporaire. Par exemple, si un routeur (lors de la transmission d'un paquet) envoie une sollicitation de voisin pour une adresse, le nœud optimiste peut répondre le premier, et si le routeur n'a pas d'adresse de couche de liaison préexistante pour cette adresse IP, il va accepter la réponse et (à tort) transmettre tous les paquets en file d'attente au nœud optimiste. Le nœud optimiste peut alors répondre d'une façon incorrecte (par exemple, en envoyant un RST TCP en réponse à une connexion TCP inconnue). De telles conditions temporaires devraient être brèves dans la plupart des cas.

De même, un nœud optimiste peut quand même injecter des paquets IP dans l'Internet qui seront en effet des paquets "usurpés" paraissant venir du nœud légitime. Dans certains cas, ces paquets peuvent conduire à des erreurs ou autres problèmes de fonctionnement, bien qu'on puisse s'attendre à ce que les protocoles de couche supérieure traitent généralement de tels paquets avec robustesse, de la même façon qu'ils doivent traiter les vieux paquets et autres dupliqués.

Appendice A. Probabilité de collision

En affirmant l'utilité de la détection d'adresse dupliquée, la probabilité de collision doit être considérée. Les divers mécanismes comme SLAAC [RFC2462] et DHCPv6 [RFC3315] tentent de garantir l'unicité de l'adresse. L'unicité de SLAAC dépend de la fiabilité du processus manufacturier (de sorte que les adresses de couche de liaison dupliquées ne soient pas allouées) et des facteurs humains si les adresses de couche de liaison peuvent être allouées manuellement. L'unicité des adresses allouées par DHCPv6 s'appuie sur la correction de la mise en œuvre pour s'assurer que la même adresse n'est pas donnée à deux nœuds.

"Extensions de confidentialité à SLAAC" [RFC3041] évite ces cas d'erreur potentiels en prenant au hasard un identifiant d'interface (IID, *Interface Identifier*) parmi 2^62 identifiants de 64 bits possibles (en laissant de côté les bits réservés U et G). Aucune tentative n'est faite pour garantir l'unicité, mais la probabilité peut être facilement estimée, et comme le montre la discussion suivante, la probabilité de collision est excessivement faible.

A.1 Paradoxe de l'anniversaire

Quand on considère la probabilité de collision, on mentionne généralement le paradoxe de l'anniversaire. Quand on choisit au hasard k valeurs parmi n possibilités, la probabilité que deux valeurs soient la même est :

$$Pb(n,k) = 1-(n! / [(n-k)! . n^k])$$

Le calcul de la probabilité de collision avec cette méthode est cependant difficile, car un des termes des n!, et (2^62)! est un nombre peu maniable. On peut cependant calculer une limite supérieure de la probabilité de collision :

$$Pb(n,k) \leq 1-([(n-k+1)/n] \wedge [k-1])$$

qui permet de calculer que même pour de grands réseaux la probabilité de collision de deux nœud est très petite :

Pb(2^62, 500) ≤ 5,4e-14
Pb(2^62, 5000) ≤ 5,4e-12
Pb(2^62, 50000) ≤ 5,4e-10
Pb(2^62, 500000) ≤ 5,4e-08

La formule de la limite supérieure utilisée ci-dessus est tirée de "Génération aléatoire d'identifiants d'interfaces", de M. Bagnulo, I. Soto, A. Garcia-Martinez, et A. Azcorra, et est utilisée avec la gracieuse permission des auteurs.

A.2 Nœuds individuels

Quand on considère l'effet de collisions sur un nœud individuel, on n'a pas besoin de considérer le paradoxe de l'anniversaire. Quand un nœud passe dans un réseau avec K nœuds existants, la probabilité qu'il n'entre pas en collision avec une des adresses distinctes utilisées est simplement 1-K/N. Si il passe M fois dans de tels réseaux, la probabilité qu'il ne cause pas de collision sur un de ces mouvements est (1-K/N)^M ; donc, la probabilité qu'il cause au moins une collision est :

Pc(n,k,m) = 1-[(1-k/n)^m]

Même en considérant un très grand nombre de mouvements (m = 600000, légèrement plus qu'un mouvement par minute pour un an) et des réseaux plutôt encombrés (k=50000 nœuds par réseau) les chances de collision pour un certain nœud sont étonnamment faibles :

Pc(2^62, 5000, 600000) = 6.66e-10
Pc(2^62, 50000, 600000) = 6.53e-09

Chacune de ces collisions affecte deux nœuds, de sorte que la probabilité d'être affecté par une collision est deux fois cela. Même si le nœud passe dans des réseaux de 50 000 nœuds une fois par minute pendant 100 ans, la probabilité qu'il cause ou souffre d'une collision à tout moment est un peu au dessus de 1 sur un million.

Pc(2^62, 50000, 60000000) * 2 = 1.3e-06

Références normatives

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

[RFC2461] T. Narten, E. Nordmark, W. Simpson, "Découverte de voisins pour IP version 6 (IPv6)", décembre 1998. (*Obsolète, voir* RFC4861) *(D.S.)*

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

Références pour information

[RFC2464] M. Crawford, "Transmission de paquets IPv6 sur réseaux Ethernet", décembre 1998. *(P.S. ; MàJ par* RFC8064)

[RFC3041] T. Narten, R. Draves, "Extensions de confidentialité pour l'auto-configuration d'adresse sans état dans IPv6", janvier 2001. (*Obsolète, voir* RFC4941) *(P.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.)*

[RFC3756] P. Nikander, éd., "Modèles de confiance et menaces pour la découverte de voisin IPv6 (ND)", mai 2004. *(Information)*

[RFC3775] D. Johnson, C. Perkins, J. Arkko, "Prise en charge de la mobilité dans IPv6", juin 2004. *(P.S.) (Obs., voir* RFC6275)

[RFC3971] J. Arkko et autres, "Découverte de voisin sécurisée (SEND)", mars 2005. (*MàJ par* RFC6494) *(P.S.)*

[RFC3972] T. Aura, "Adresses générées cryptographiquement (CGA)", mars 2005. (*MàJ par* RFC4581, RFC4982) *(P.S.)*

Remerciements

Le présent travail a eu des précédents dans des projets Internet arrivés à expiration et dans des discussions au sein de la liste de diffusion du groupe de travail MobileIP ainsi qu'à l'IETF-54. Un concept similaire apparaît dans le bit "Optimiste" utilisé par R. Koodli et C. Perkins dans le projet maintenant expiré, "Transferts inter cellulaires rapides dans IPv6 mobile".

Merci à Greg Daley, Richard Nelson, Brett Pentland et Ahmet Sekercioglu de Monash University CTIE pour leurs retours et leurs encouragements. Plus d'informations sont disponibles à : <http://www.ctie.monash.edu.au/ipv6/fastho/>

Merci à tous les membres des groupes de travail MobileIP et IPng/IPv6 qui ont contribué au débat, en particulier par ordre alphabétique : Jari Arkko, Marcelo Bagnulo, JinHyeock Choi, Youn-Hee Han, James Kempf, Thomas Narten, Pekka Nikander, Erik Nordmark, Soohong 'Daniel' Park, Mohan Parthasarathy, Ed Remmel, Pekka Savola, Hesham Soliman, Ignatious Souvatzis, Jinmei Tatuya, Dave Thaler, Pascal Thubert, Christian Vogt, Vladislav Yasevich, et Alper Yegin.

Ce travail a été soutenu par le "Australian Telecommunications Cooperative Research Centre" (ATcrc) : <http://www.telecommunications.crc.org.au/>

Adresse de l'auteur

Nick 'Sharkey' Moore
Centre for Telecommunications and Information Engineering
Monash University 3800
Victoria, Australia

Les commentaires devraient être envoyés à <sharkey@zoic.org> et/ou à la liste de diffusion du groupe de travail IPv6.
Prière d'inclure "RFC4429" dans la ligne "Subject".

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 fourni par l'activité de soutien administatif de l'IETF (IASA, *IETF Administrative Support Activity*).