Groupe de travail Réseau
Request for Comments : 4862
RFC rendue obsolète : 2462
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

S. Thomson, Cisco
T. Narten, IBM
T. Jinmei, Toshiba
septembre 2007

Auto configuration d'adresse IPv6 sans état

Résumé
Le présent document spécifie les étapes parcourues par un hôte pour décider comment autoconfigurer ses interfaces en IP version 6. Le processus d'autoconfiguration comporte de générer une adresse de liaison locale, de générer des adresses mondiales via l'autoconfiguration d'adresse sans état, et la procédure de détection d'adresse dupliquée pour vérifier l'unicité des adresses sur une liaison.

Table des Matières

1. Introduction
2. Terminologie
2.1 Exigences
3. Buts du concept
4. Vue d'ensemble du protocole
4.1 Dénumérotage de site
5. Spécification du protocole
5.1 Variables de configuration de nœud
5.2 Structures en rapport avec l'autoconfiguration
5.3 Création des adresses de liaison locale
5.4 Détaction d'adresse dupliquée
5.5 Création d'adresses mondiales
5.6 Cohérence de la configuration
5.7 Conserver les adresses configurées pour des raisons de stabilité
6. Considérations pour la sécurité
7. Remerciements
8. Références
8.1 Références normatives
8.2 Références informatives
Appendice A. Suppression du bouclage et détection d'adresse dupliquée
Appendice B. Changements par rapport à la RFC1971
Appendice C. Changements par rapport à la RFC2462
Déclaration complète de droits de reproduction

1. Introduction

Le présent document spécifie les étapes parcourues par un hôte pour décider comment autoconfigurer ses interfaces dans IP version 6 (IPv6). Le processus d'autoconfiguration inclut de générer une adresse de liaison locale, de générer des adresses mondiales via l'autoconfiguration d'adresse sans état, et la procédure de détection d'adresse dupliquée pour vérifier l'unicité des adresses sur une liaison.

Le mécanisme d'autoconfiguration sans état de IPv6 n'exige pas de configuration manuelle des hôtes, une configuration minimale (s'il en est) des routeurs, et pas de serveur supplémentaire. Le mécanisme sans état permet à un hôte de générer ses propres adresses en utilisant une combinaison d'informations disponibles localement et d'informations annoncées par les routeurs. Les routeurs annoncent les préfixes qui identifient le ou les sous-réseaux associés à une liaison, alors que les hôtes génèrent un "identifiant d'interface" qui identifie de façon univoque une interface sur un sous-réseau. Une adresse est formée en combinant les deux. En l'absence de routeur, un hôte ne peut générer que des adresses de liaison locales. Cependant, les adresses de liaison locales sont suffisantes pour permettre la communication parmi les nœuds rattachés à la

même liaison.

L'approche sans état est utilisée lorsque un site n'est pas particulièrement concerné par les adresses exactes qu'utilisent les hôtes, pour autant qu'elles soient uniques et correctement acheminables. D'un autre côté, le protocole de configuration dynamique d'hôte pour IP version 6 (DHCPv6, *Dynamic Host Configuration Protocol for IPv6*) [RFC3315] est utilisé lorsque un site exige un contrôle plus étroit sur les allocations exactes d'adresses. L'autoconfiguration d'adresse sans état et DHCPv6 peuvent tous deux être utilisés simultanément.

Les adresses IPv6t sont prêtées à une interface pour une durée fixe (éventuellement infinie). Chaque adresse a une durée de vie associée qui indique combien de temps une adresse est liée à une interface. Lorsque une durée de vie expire, le lien (et l'adresse) deviennent invalides et l'adresse peut être réallouée à une autre interface ailleurs dans l'Internet. Pour traiter en douceur l'expiration des liens d'adresses, une adresse passe par deux phases distinctes lorsque elle est allouée à une interface. Initialement, un adresse est "préférée", ce qui signifie que son utilisation dans une communication arbitraire n'est soumise à aucune restriction. Plus tard, une adresse devient "déconseillée" en anticipant que le lien actuel de l'interface va devenir invalide. Lorsque une adresse est dans l'état déconseillé, son utilisation est déconseillée, mais pas formellement interdite. Une nouvelle communication (par exemple, l'ouverture d'une nouvelle connexion TCP) devrait utiliser une adresse préférée lorsque possible. Une adresse déconseillée devrait n'être utilisée que par des applications qui l'ont déjà utilisée et qui auraient des difficultés à passer à une autre adresse sans interruption de service.

Pour s'assurer que toutes les adresses configurées sont vraisemblablement uniques sur une liaison donnée, les nœuds font fonctionner un algorithme de "détection d'adresse dupliquée" sur les adresses avant de les allouer à une interface. L'algorithme de détection d'adresse dupliquée est effectué sur toutes les adresses, sans considération du fait qu'elles seraient obtenues via l'autoconfiguration sans état ou via DHCPv6. Le présent document définit l'algorithme de détection d'adresse dupliquée.

Le processus d'autoconfiguration spécifié dans le présent document ne s'applique qu'aux hôtes et non aux routeurs. Comme l'autoconfiguration d'hôte utilise les informations annoncées par les routeurs, les routeurs devront être configurés par d'autres moyens. Cependant, il est prévu que les routeurs vont générer des adresses de liaison locales en utilisant le mécanisme décrit dans le présent document. De plus, les routeurs sont supposés réussir la procédure de détection d'adresse dupliquée décrite dans ce document sur toutes les adresses avant de les allouer à une interface.

La Section 2 donne les définitions pour la terminologie utilisée dans le présent document. La Section 3 décrit les objectifs du concept qui conduit à la procédure actuelle d'autoconfiguration. La Section 4 donne une vue d'ensemble du protocole, tandis que lé Section 5 décrit le protocole dans ses détails.

2. Terminologie

IP – Protocole Internet version 6. Les termes IPv4 et IPv6 ne sont utilisés que dans les contextes où il est nécessaire d'éviter l'ambiguïté.

nœud – un appareil qui met en œuvre IP.

routeur – un nœud qui transmet des paquets IP non explicitement adressés à lui-même.

hôte – tout nœud qui n'est pas un routeur.

couche supérieure – une couche de protocole immédiatement au-dessus de IP. Des exemples sont les protocoles de transport tels que TCP et UDP, des protocoles de contrôle tels que ICMP, des protocoles d'acheminement tels que OSPF, et les protocoles Internet ou de couche inférieure qui sont "tunnelés" dessus (c'est-à-dire, encapsulés dans) IP tels que IPX, AppleTalk, ou IP lui-même.

liaison – une facilité ou support de communication sur lequel chaque nœud peut communiquer à la couche liaison, c'est-à-dire, la couche immédiatement au-dessous de IP. Des exemples sont les Ethernets (simples ou pontés) ; les liaisons PPP ; X.25, les réseaux en relais de trame ou ATM; et les "tunnels" de couche Internet (ou supérieure) comme les tunnels sur IPv4 ou IPv6 lui-même. Le protocole décrit dans le présent document sera utilisé sur tous les types de liaisons sauf spécification contraire dans le document spécifique de type de liaison qui décrit comment faire fonctionner IP sur la liaison conformément à la [RFC4861].

interface – c'est le rattachement d'un nœud à une liaison.

paquet – c'est un en-tête IP plus une charge utile.

adresse – c'est un identifiant de couche IP pour une interface ou ensemble d'interfaces.

adresse d'envoi individuel – c'est un identifiant pour une seule interface. Un paquet envoyé à une adresse d'envoi individuel est livre à l'interface identifiée par cette adresse.

adresse de diffusion groupée – c'est un identifiant pour un ensemble d'interfaces (appartenant normalement à différents nœuds). Un paquet envoyé à une adresse de diffusion groupée est livré à toutes les interfaces identifiées par cette adresse.

adresse d'envoi à la cantonade – c'est un identifiant pour un ensemble d'interfaces (appartenant normalement à différents nœuds). Un paquet envoyé à une adresse d'envoi à la cantonade est livré à une des interfaces identifiées par cette adresse (la "plus proche", selon la mesure de distance du protocole d'acheminement). Voir la [RFC4291].

adresse de diffusion groupée de nœud sollicité – c'est une adresse de diffusion groupée à laquelle sont envoyés les messages de sollicitation de voisin. L'algorithme pour le calcul de l'adresse est donné dans la [RFC4291].

adresse de couche de liaison – c'est un identifiant de couche de liaison pour une interface. Des exemples sont les adresses IEEE 802 pour les liaisons Ethernet et les adresses E.164 pour les liaisons de réseau numérique à intégration de services (RNIS).

adresse de liaison locale – c'est une adresse qui n'a de portée que sur la liaison et qui peut être utilisée pour atteindre les nœuds voisins rattachés à la même liaison. Toutes les interfaces ont une adresse d'envoi individuel de liaison locale.

adresse mondiale – c'est une adresse avec une portée illimitée.

communication – tout échange de paquet entre des nœuds qui exige que l'adresse de chaque nœud utilisée dans l'échange reste la même pour la durée de l'échange de paquets. Par exemple, une connexion TCP ou une demande/réponse UDP.

tentative d'adresse – c'est une adresse dont l'unicité sur une liaison est en train d'être vérifiée, avant son allocation à une interface. Une tentative d'adresse n'est pas considérée comme allouée à une interface au sens habituel. Une interface élimine les paquets reçus qui sont adressés à une tentative d'adresse, mais accepte les paquets de découverte de voisin qui se rapportent à la détection d'adresse dupliquée pour la tentative d'adresse.
adresse préférée – c'est une adresse allouée à une interface dont l'utilisation par les protocoles de couche supérieure n'est soumise à aucune restriction. Les adresses préférées peuvent être utilisées comme adresses de source (ou de destination) des paquets envoyés de (ou à) l'interface.

adresse déconseillée – c'est une 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 une nouvelle communication, mais les paquets envoyés de ou à une adresse déconseillée sont livrés comme prévu. Une adresse déconseillée peut continuer d'être utilisée comme adresse de source dans des communications où le passage à une adresse préférée causerait des difficultés à une activité spécifique de couche supérieure (par exemple, une connexion TCP existante).

adresse valide – c'est une adresse préférée ou déconseillée. Une adresse valide peut apparaître comme adresse de source ou de destination d'un paquet, et le système d'acheminement de l'Internet est supposé livrer les paquets envoyés à une adresse valide à leurs destinataires prévus.

adresse invalide – c'est une adresse qui n'est allouée à aucune interface. Une adresse valide devient invalide lorsque sa durée de vie valide expire. Les adresses invalides ne devraient pas apparaître comme adresse de destination ou de source d'un paquet. Dans le premier cas, le système d'acheminement de l'Internet va être incapable de livrer le paquet ; dans le second cas, le receveur du paquet sera incapable d'y répondre.

durée de vie préférée – c'est la durée pendant laquelle une adresse valide est préférée (c'est-à-dire, le temps qui s'écoule jusqu'à ce qu'elle soit déconseillée). Lorsque la durée de vie préférée expire, l'adresse devient déconseillée.

durée de vie valide – c'est la durée pendant laquelle une adresse reste dans l'état valide (c'est-à-dire, le temps qui s'écoule jusqu'à son invalidation). La durée de vie valide doit être supérieure ou égale à la durée de vie préférée. Lorsque la durée de vie valide expire, l'adresse devient invalide.

identifiant d'interface – c'est un identifiant qui dépend de la liaison pour une interface qui est (au moins) unique sur la liaison [RFC4291]. L'autoconfiguration d'adresse sans état combine un identifiant d'interface avec un préfixe pour former une adresse. Du point de vue de l'autoconfiguration d'adresse, un identifiant d'interface est une chaîne binaire de longueur connue. La longueur exacte d'un identifiant d'interface et la façon dont il est créé sont définies dans un document distinct spécifique du type de liaison qui couvre les questions qui se rapportent à la transmission de IP sur un type particulier de

liaison (par exemple, la [RFC2464]). Noter que l'architecture des adresses [RFC4291] définit aussi la longueur des identifiants d'interface pour certains ensembles d'adresses, mais les deux ensembles de définitions doivent être cohérents. Dans de nombreux cas, l'identifiant sera déduit de l'adresse de couche liaison de l'interface.

2.1 Exigences

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

Noter que le présent document limite intentionnellement l'utilisation des mots-clés à la spécification du protocole (Section 5).

3. Buts du concept

L'autoconfiguration sans état est conçue en ayant en vue les objectifs suivants :

- La configuration manuelle de machines individuelles avant de les connecter au réseau ne devrait pas être exigée. Par conséquent, un mécanisme est nécessaire pour permettre à un hôte d'obtenir ou de créer des adresses univoques pour chacune de ses interfaces. L'autoconfiguration d'adresse suppose que chaque interface peut fournir un identifiant univoque pour cette interface (c'est-à-dire, un "identifiant d'interface"). Dans le cas le plus simple, un identifiant d'interface consiste en l'adresse de couche liaison de l'interface. Un identifiant d'interface peut être combiné avec un préfixe pour former une adresse.

- Les petits sites consistant en un ensemble de machines rattachées à une seule liaison ne devrait pas requérir la présence d'un serveur ou routeur DHCPv6 comme préalable à la communication. La communication prête à l'emploi est réalisée par l'utilisation des adresses de liaison locale. Les adresses de liaison locale ont un préfixe bien connu qui identifie la liaison partagée (la seule) à laquelle se rattache un ensemble de nœuds. Un hôte forme une adresse de liaison locale en ajoutant un identifiant d'interface au préfixe de liaison locale.

- Un grand site avec plusieurs réseaux et routeurs ne devrait pas avoir besoin de la présence d'un serveur DHCPv6 pour la configuration d'adresse. Afin de générer des adresses mondiales, les hôtes doivent déterminer les préfixes qui identifient les sous réseaux auxquels ils se rattachent. Les routeurs génèrent des annonces de routeur périodiques qui comportent des options qui énumèrent l'ensemble des préfixes actifs sur une liaison.

- La configuration d'adresse devrait faciliter la dénumérotation en douceur des machines d'un site. Par exemple, un site peut souhaiter dénuméroter tous ses nœuds lorsque il passe à un nouveau fournisseur de service réseau. Le dénumérotage est achevé par l'allocation des adresses aux interfaces et l'allocation de plusieurs adresses à la même interface. Les durées de vie des prêts fournissent le mécanisme par lequel un site élimine les vieux préfixes. L'allocation de plusieurs adresses à une interface permet une période de transition durant laquelle à la fois une nouvelle adresse et celle qui est en train d'être éliminée fonctionnent simultanément.

4. Vue d'ensemble du protocole

La présente section donne une vue d'ensemble des étapes normales qui ont lieu lorsque une interface s'autoconfigure. L'autoconfiguration n'est effectuée que sur des liaisons capables de diffusion groupée et commence lorsque une interface capable de diffusion groupée est activée, par exemple, durant le démarrage du système. Les nœuds (hôtes et routeurs) commencent le processus d'autoconfiguration en générant une adresse de liaison locale pour l'interface. Une adresse de liaison locale est formée en ajoutant un identifiant de l'interface au préfixe de liaison locale bien connu [RFC4291].

Avant que l'adresse de liaison locale puisse être allouée à une interface et utilisée, un nœud doit cependant essayer de vérifier que cette "tentative" d'adresse n'est pas déjà utilisée par un autre nœud sur la liaison. Précisément, il envoie un message Sollicitation de voisin contenant la tentative d'adresse comme cible. Si un autre nœud utilise déjà cette adresse, il va retourner une annonce de voisin le disant. Si un autre nœud tente aussi d'utiliser la même adresse, il va envoyer aussi une sollicitation de voisin pour la cible. Le nombre exact de fois que la sollicitation de voisin est (re)transmise et le délai entre les sollicitations consécutives sont spécifiques de la liaison et peuvent être réglés par la gestion du système.

Si un nœud détermine que sa tentative d'adresse de liaison locale n'est pas unique, l'autoconfiguration s'arrête et la configuration manuelle de l'interface est requise. Pour simplifier la récupération dans ce cas, il devrait être possible à un administrateur de fournir un autre identifiant d'interface qui se substitue à l'identifiant par défaut de façon telle que le

mécanisme d'autoconfiguration puisse alors s'appliquer en utilisant le nouvel identifiant (présumé univoque) d'interface. Autrement, les adresses de liaison locale et autres devront être configurées manuellement.

Une fois qu'un nœud s'est assuré que sa tentative d'adresse de liaison locale est unique, il alloue l'adresse à l'interface. À ce point, le nœud a la connexité de niveau IP avec les nœuds du voisinage. Les étapes d'autoconfiguration restantes ne sont effectuées que par les hôtes ; la (auto)configuration des routeurs sort du domaine d'application du présent document.

La phase d'autoconfiguration suivante implique d'obtenir une annonce de routeur ou de déterminer qu'aucun routeur n'est présent. Si des routeurs sont présents, ils vont envoyer des annonces de routeur qui spécifient quelle sorte d'autoconfiguration peut faire un hôte. Noter que le service DHCPv6 de configuration d'adresse peut encore être disponible même si aucun routeur n'est présent.

Les routeurs envoient périodiquement des annonces de routeur, mais le délai entre les annonces successives va généralement être plus long que ce qu'un hôte qui effectue l'autoconfiguration veut attendre [RFC4861]. Pour obtenir rapidement une annonce, un hôte envoie une ou plusieurs sollicitations de routeur au groupe de diffusion groupée Tous-les-routeurs.

Les annonces de routeur contiennent aussi zéro, une ou plusieurs options d'informations de préfixes qui contiennent des informations utilisées par l'autoconfiguration d'adresse sans état pour générer des adresses mondiales. On notera qu'un hôte peut utiliser à la fois l'autoconfiguration d'adresse sans état et DHCPv6 simultanément. Un champ d'options d'informations de préfixe, le fanion "configuration autonome d'adresse", indique si l'option s'applique ou non à l'autoconfiguration sans état. Si elle s'applique, des champs d'option supplémentaires contiennent un préfixe de sous réseau, avec les valeurs de durée de vie, qui indiquent pendant combien de temps les adresses créées à partir du préfixe restent préférées et valides.

Parce que les routeurs génèrent périodiquement des annonces de routeur, les hôtes vont continuellement recevoir de nouvelles annonces. Les hôtes traitent les informations contenues dans chaque annonce comme décrit ci-dessus, ajoutant aux informations reçues dans les annonces précédentes et les rafraîchissant.

Par défaut, l'unicité de toutes les adresses devrait être vérifiée avant leur allocation à une interface, par sauvegarde. La vérification devrait être faite individuellement sur toutes les adresses obtenues manuellement, via l'autoconfiguration d'adresse sans état, ou via DHCPv6. Pour s'accommoder des sites qui pensent que la surcharge de la réalisation de la détection d'adresse dupliquée dépasse les bénéfices qu'elle rapporte, l'utilisation de la détection d'adresse dupliquée peut être désactivée par le réglage administratif d'un fanion de configuration par interface.

Pour accélérer le processus d'autoconfiguration, un hôte peut générer son adresse de liaison locale (et vérifier son unicité) en parallèle avec l'attente d'une annonce de routeur. Parce qu'un routeur peut tarder à répondre à une sollicitation de routeur pendant quelques secondes, le temps total nécessaire pour achever l'autoconfiguration peut être significativement plus long si les deux étapes sont faites l'une après l'autre.

4.1 Dénumérotage de site

Le prêt d'adresse facilite le dénumérotage de site en fournissant un mécanisme pour périmer les adresses allouées aux interfaces dans les hôtes. À présent, les protocoles de couche supérieure comme TCP ne fournissent aucun soutien pour changer les adresses de point d'extrémité lorsque une connexion est ouverte. Si une adresse de point d'extrémité devient invalide, les connexions existantes s'interrompent et toute communication pour l'adresse invalide échoue. Même lorsque les applications utilisent UDP comme protocole de transport, les adresses doivent généralement rester les mêmes durant un échange de paquets.

Diviser les adresses valides en catégories préférée et déconseillée donne un moyen pour indiquer aux couches supérieures qu'une adresse valide peut devenir invalide sous peu et que de futures communications utilisant l'adresse échoueront si la durée de vie valide de l'adresse expire avant la fin de la communication. Pour éviter ce scénario, les couches supérieures devraient utiliser une adresse préférée (en supposant qu'il en existe une de portée suffisante) pour augmenter la probabilité qu'une adresse reste valide pour la durée de la communication. Il dépend de l'administrateur du système de régler les durées de vie de préfixe appropriées pour minimiser l'impact de l'échec d'une communication lorsque le dénumérotage a lieu. La période déconseillée devrait être assez longue pour que la plupart, sinon toutes, les communications utilisent la nouvelle adresse au moment où une adresse devient invalide.

La couche IP est supposée fournir le moyen pour que les couches supérieures (y compris d'applications) choisissent l'adresse de source la plus appropriée pour une destination particulière et en fonction d'autres contraintes éventuelles. Une application peut choisir de sélectionner elle-même l'adresse de source avant de commencer une nouvelle communication, ou peut laisser l'adresse non spécifiée, auquel cas les couches supérieures de réseautage vont utiliser le mécanisme fourni par la couche IP pour choisir une adresse convenable au nom de l'application.

Les règles détaillées de sélection d'adresse sortent du domaine d'application du présent document et sont décrites dans la [RFC3484].

5. Spécification du protocole

L'autoconfiguration est effectuée sur la base de l'interface sur les interfaces capables de diffusion groupée. Pour les hôtes multi rattachements, l'autoconfiguration est effectuée indépendamment sur chaque interface. L'autoconfiguration s'applique principalement aux hôtes, avec deux exceptions. Les routeurs sont supposés générer une adresse de liaison locale en utilisant la procédure décrite ci-dessous. De plus, les routeurs effectuent la détection d'adresse dupliquée sur toutes les adresses avant de les allouer à une interface.

5.1 Variables de configuration de nœud

Un nœud DOIT permettre que soient configurées les variables d'autoconfiguration suivantes par la gestion de système pour chaque interface capable de diffusion groupée :

DupAddrDetectTransmits
C'est le nombre de messages Sollicitation de voisin consécutifs envoyés lors de la réalisation de la détection d'adresse dupliquée sur une tentative d'adresse. Une valeur de zéro indique que la détection d'adresse dupliquée n'est pas effectuée sur les tentatives d'adresse. Une valeur de un indique une seule transmission sans retransmission à suivre.
Par défaut : 1, mais peut être outrepassé par une valeur spécifique du type de liaison dans le document qui traite des questions qui se rapportent à la transmission de IP sur un type de liaison particulier (par exemple, [RFC2464]).

L'autoconfiguration suppose aussi la présence de la variable RetransTimer telle que définie dans la [RFC4861]. Pour les besoins de l'autoconfiguration, RetransTimer spécifie le délai entre les transmissions consécutives des sollicitations de voisin effectuées durant la détection d'adresse dupliquée (si DupAddrDetectTransmits est supérieur à 1) ainsi que le temps pendant lequel un nœud veut attendre après l'envoi de la dernière sollicitation de voisin avant de terminer le processus de détection d'adresse dupliquée.

5.2 Structures en rapport avec l'autoconfiguration

Au delà de la formation d'une adresse de liaison locale et de l'utilisation de la détection d'adresse dupliquée, la façon dont les routeurs (auto)configurent leurs interfaces sort du domaine d'application du présent document.

Un hôte tient une liste des adresses ainsi que leurs durées de vie correspondantes. La liste des adresses contient à la fois des adresses autoconfigurées et des adresses configurées manuellement.

5.3 Création des adresses de liaison locale

Un nœud forme une adresse de liaison locale chaque fois qu'une interface est activée. Une interface peut devenir active après l'un des événements suivants :
- l'interface est initialisée au moment du démarrage du système ;
- l'interface est réinitialisée après une défaillance temporaire de l'interface ou après avoir été temporairement désactivée par la gestion du système ;
- l'interface se rattache à une liaison pour la première fois ; cela inclut le cas où la liaison de rattachement est changée dynamiquement du fait d'un changement du point d'accès des réseaux sans fil ;
- l'interface est activée par la gestion du système après avoir été désactivée administrativement.

Une adresse de liaison locale est formée en combinant le préfixe de liaison locale bien connu FE80::0 [RFC4291] (de la longueur appropriée) avec un identifiant d'interface comme suit :

1. Les bits les plus à gauche de la "longueur de préfixe" de l'adresse sont ceux du préfixe de liaison locale.

2. Les bits dans l'adresse qui sont à droite du préfixe de liaison locale sont tous mis à zéro.

3. Si la longueur de l'identifiant d'interface est N bits, les N bits les plus à droite de l'adresse sont remplacés par l'identifiant d'interface.

Si la somme de la longueur du préfixe de liaison locale et de N est supérieure à 128, l'autoconfiguration échoue et la configuration manuelle est requise. La longueur de l'identifiant d'interface est définie dans un document spécifique du type de liaison distinct, qui devrait aussi être cohérent avec l'architecture des adresses de la [RFC4291] (voir la Section 2). Ces documents définiront soigneusement la longueur afin que les adresses de liaison locale puissent être autoconfigurées sur la liaison.

Une adresse de liaison locale a une durée de vie préférée infinie et valide ; elle n'est jamais périmée.

5.4 Détection d'adresse dupliquée

La détection d'adresse dupliquée DOIT être effectuée sur toutes les adresses d'envoi individuel avant de les allouer à une interface, sans considérer si elles sont obtenues par autoconfiguration sans état, DHCPv6, ou configuration manuelle, avec les exceptions suivantes :

- Une interface dont la variable DupAddrDetectTransmits est réglée à zéro n'effectue pas la détection d'adresse dupliquée.

- La détection d'adresse dupliquée NE DOIT PAS être effectuée sur des adresses d'envoi à la cantonade (noter que les adresses d'envoi à la cantonade ne peuvent pas être syntaxiquement distinguées des adresses d'envoi individuel).

- L'unicité de chaque adresse d'envoi individuel DEVRAIT être vérifiée. Noter qu'il existe des mises en œuvre qui n'effectuent que la détection d'adresse dupliquée pour l'adresse de liaison locale et sautent la vérification de l'adresse mondiale qui utilise le même identifiant d'interface que celui de l'adresse de liaison locale. Bien que le présent document n'invalide pas de telles mises en œuvre, cette sorte "d'optimisation" N'EST PAS RECOMMANDÉE, et les nouvelles mises en œuvre NE DOIVENT PAS faire cette optimisation. Cette optimisation est venue de l'hypothèse que toutes les adresses d'une interface sont générées à partir du même identifiant. Cependant, l'hypothèse ne tient pas en réalité ; de nouveaux types d'adresses ont été introduits où les identifiants d'interface ne sont pas nécessairement les mêmes pour toutes les adresses d'envoi individuel sur une seule interface [RFC4941], [RFC3972]. Exiger que la détection d'adresse dupliquée soit effectuée pour toutes les adresses d'envoi individuel rendra l'algorithme robuste pour les identifiants d'interface actuels et pour les futurs identifiants particuliers.

La procédure pour la détection d'adresse dupliquée utilise les messages de sollicitation et d'annonce de voisin comme décrit ci-dessous. Si une adresse dupliquée est découverte durant la procédure, l'adresse ne peut pas être allouée à l'interface. Si l'adresse est déduite d'un identifiant d'interface, un nouvel identifiant devra être alloué à l'interface, ou toutes les adresses IP pour l'interface devront être configurées manuellement. Noter que la méthode pour détecter les duplications n'est pas complètement fiable, et il est possible que des adresses dupliquées existent encore (par exemple, si la liaison a subi une partition pendant qu'était effectuée la détection d'adresse dupliquée).

Une adresse sur laquelle est appliquée la procédure de détection d'adresse dupliquée est dite être une tentative jusqu'à ce que la procédure s'achève par son succès. Une tentative d'adresse n'est pas considérée comme "allouée à une interface" au sens traditionnel. C'est à dire que l'interface doit accepter les messages de sollicitation et d'annonce de voisin qui contiennent la tentative d'adresse dans le champ Adresse cible, mais traite de tels paquets différemment de ceux dont Adresse cible correspond à une adresse allouée à l'interface. Les autres paquets adressés à la tentative d'adresse devraient être éliminés en silence. Noter que les "autres paquets" incluent les messages de sollicitation et d'annonce de voisin qui ont la tentative d'adresse (c'est-à-dire, en envoi individuel) comme adresse de destination IP et qui contiennent la tentative d'adresse dans le champ Adresse cible. Un tel cas ne devrait cependant pas se produire en fonctionnement normal, car ces messages sont en diffusion groupée dans la procédure de détection d'adresse dupliquée.

On devrait aussi noter que la détection d'adresse dupliquée doit être effectuée avant d'allouer une adresse à une interface afin d'empêcher que plusieurs nœuds utilisent simultanément la même adresse. Si un nœud commence à utiliser une adresse en parallèle avec la détection d'adresse dupliquée et qu'un autre nœud utilise déjà l'adresse, le nœud qui effectue la détection d'adresse dupliquée va traiter à tort le trafic destiné à l'autre nœud, ce qui peut déboucher sur d'éventuelles conséquences négatives comme de réinitialiser les connexions TCP ouvertes.

Les paragraphes qui suivent décrivent les essais spécifiques qu'effectue un nœud pour vérifier l'unicité d'une adresse. Une adresse est considérée comme unique si aucun des essais n'indique la présence d'une adresse dupliquée pendant RetransTimer millisecondes après avoir envoyé DupAddrDetectTransmits sollicitations de voisins. Une fois qu'une adresse est déterminée comme unique, elle peut être allouée à une interface.

5.4.1 Validation de message

Un nœud DOIT éliminer en silence tout message de sollicitation ou d'annonce de voisin qui ne réussit pas les essais de validité spécifiés dans la [RFC4861]. Un message de sollicitation ou d'annonce de voisin qui réussit ces essais de validité

est appelé respectivement, une sollicitation valide, ou une annonce valide.

5.4.2 Envoi des messages de sollicitation de voisin

Avant d'envoyer une sollicitation de voisin, une interface DOIT se joindre à l'adresse de diffusion groupée Tous-les-nœuds et à l'adresse de diffusion groupée de Nœud-sollicité de la tentative d'adresse. La première assure que le nœud recevra les annonces de voisin de la part des autres nœuds qui utilisent déjà l'adresse ; la seconde assure que deux nœuds qui tentent d'utiliser simultanément la même adresse devraient détecter leur présence mutuelle.

Pour vérifier une adresse, un nœud envoie DupAddrDetectTransmits sollicitations de voisin, séparées chacune par RetransTimer millisecondes. L'adresse cible de la sollicitation est réglée à l'adresse qu'on vérifie, la source IP est réglée à l'adresse non spécifiée, et la destination IP est réglée à l'adresse de diffusion groupée de nœud sollicité de l'adresse cible.

Si la sollicitation de voisin est le premier message envoyé d'une interface après son initialisation ou réinitialisation, le nœud DEVRAIT différer de se joindre à l'adresse de diffusion groupée de nœud sollicité d'un délai aléatoire compris entre 0 et MAX_RTR_SOLICITATION_DELAY comme spécifié dans la [RFC4861]. Cela sert à alléger l'encombrement lorsque de nombreux nœuds démarrent au même moment sur la liaison, comme après une coupure de courant, et peut aider à éviter une condition de compétition lorsque plus d'un nœud essaye de solliciter la même adresse au même moment.

Même si la sollicitation de voisin n'est pas le premier message envoyé, le nœud DEVRAIT différer de se joindre à l'adresse de diffusion groupée de nœud sollicité d'un délai aléatoire compris entre 0 et MAX_RTR_SOLICITATION_DELAY si l'adresse à vérifier est configurée par un message d'annonce de routeur envoyé à une adresse de diffusion groupée. Le délai va éviter de la même façon l'encombrement lorsque plusieurs nœuds sont en train de configurer des adresses en recevant la même annonce de routeur par une seule diffusion groupée.

Noter que lorsque un nœud se joint à une adresse de diffusion groupée, il envoie normalement un message de rapport de découverte d'écoutant de diffusion groupée (MLD, *Multicast Listener Discovery*) [RFC2710], [RFC3810] pour l'adresse de diffusion groupée. Dans le cas de la détection d'adresse dupliquée, le message de rapport de MLD est exigé afin d'informer les commutateurs qui surveillent les MLD, plutôt que les routeurs, pour transmettre les paquets de diffusion groupée. Dans la description ci-dessus, le retard à se joindre à l'adresse de diffusion groupée signifie donc de retarder la transmission du message de rapport de MLD correspondant. Comme les spécifications de MLD ne demandent pas un retard aléatoire pour éviter les conditions de compétition, le simple retard de la sollicitation de voisin causerait un encombrement avec les messages de rapport de MLD. L'encombrement empêcherait alors les commutateurs qui surveillent les MLD de fonctionner correctement et, par suite, empêcherait la détection d'adresse dupliquée de fonctionner. L'exigence d'inclure le retard pour le rapport de MLD dans ce cas évite ce scénario. La [RFC3590] parle aussi de certaines questions d'interaction entre la détection d'adresse dupliquée et MLD, et spécifie quelle adresse de source devrait être utilisée pour le rapport MLD dans ce cas.

Afin d'améliorer la robustesse de l'algorithme de détection d'adresse dupliquée, une interface DOIT recevoir et traiter les datagrammes envoyés à l'adresse de diffusion groupée Tous-les-nœuds ou à l'adresse de diffusion groupée Nœud-sollicité de la tentative d'adresse durant la période de retard. Cela n'entre pas nécessairement en conflit avec l'exigence de retarder de se joindre au groupe de diffusion groupée. En fait, dans certains cas, il est possible à un nœud de commencer à écouter le groupe durant la période de retard, avant la transmission du rapport de MLD. On notera cependant que dans certains environnements de couche liaison, en particulier avec les commutateurs qui surveillent MLD, aucune réception de diffusion groupée ne sera disponible jusqu'à l'envoi du rapport de MLD.

5.4.3 Réception des messages de sollicitation de voisin

À réception d'un message Sollicitation de voisin valide sur une interface, le comportement du nœud va dépendre de si l'adresse cible est ou non une tentative. Si l'adresse cible n'est pas une tentative (c'est-à-dire, si elle est allouée à l'interface receveuse) la sollicitation est traitée comme décrit dans la [RFC4861]. Si l'adresse cible est une tentative, et si l'adresse de source est une adresse d'envoi individuel, l'envoyeur de la sollicitation est en train d'effectuer une résolution d'adresse sur la cible ; la sollicitation devrait être ignorée en silence. Autrement, le traitement a lieu comme décrit ci-dessous. Dans tous les cas, un nœud NE DOIT PAS répondre à une sollicitation de voisin pour une tentative d'adresse.

Si l'adresse de source de la sollicitation de voisin est l'adresse non spécifiée, la sollicitation vient d'un nœud qui effectue la détection d'adresse dupliquée. Si la sollicitation vient d'un autre nœud, la tentative d'adresse est une duplication et ne devrait pas être utilisée (par l'un ou l'autre nœud). Si la sollicitation vient du nœud lui-même (parce que le nœud fait un rebouclage sur les paquets en diffusion groupée) la sollicitation n'indique pas la présence d'une adresse dupliquée.

Note de mise en œuvre : De nombreuses interfaces fournissent un moyen pour que les couches supérieures activent et désactivent de façon sélective le rebouclage des paquets de diffusion groupée. Les détails de la façon dont une

telle facilité est mise en œuvre peuvent empêcher la détection d'adresse dupliquée de fonctionner correctement. Voir à l'Appendice A un exposé plus complet de cette question.

Les essais suivants identifient les conditions dans lesquelles une tentative d'adresse n'est pas unique :

- Si une sollicitation de voisin pour une tentative d'adresse est reçue avant qu'une ne soit envoyée, la tentative d'adresse est une duplication. Cette condition survient lorsque deux nœuds font fonctionner simultanément la détection d'adresse dupliquée, mais transmettent la sollicitation initiale à un moment différent (par exemple, en choisissant des valeurs de retard aléatoire différentes avant de se joindre à l'adresse de diffusion groupée Nœud-sollicité et de transmettre une sollicitation initiale).

- Si le nombre réel de sollicitations de voisin reçu excède le nombre attendu sur la base de la sémantique du rebouclage (par exemple, l'interface ne renvoie pas le paquet, alors que une ou plusieurs sollicitations ont été reçues) la tentative d'adresse est une duplication. Cette condition survient lorsque deux nœuds font fonctionner simultanément la détection d'adresse dupliquée et transmettent les sollicitations a peu près en même temps.

5.4.4 Réception des messages d'annonce de voisin

À réception d'un message Annonce de voisin valide sur une interface, le comportement du nœud va dépendre de si l'adresse cible est une tentative ou correspond à une adresse en envoi individuel ou en envoi à la cantonade allouée à l'interface :

1. Si l'adresse cible est une tentative, la tentative d'adresse n'est pas unique.

2. Si l'adresse cible correspond à une adresse d'envoi individuel allouée à l'interface receveuse, cela pourrait indiquer que l'adresse est dupliquée mais qu'elle n'a pas été détectée par la procédure de détection d'adresse dupliquée (on rappelle que la détection d'adresse dupliquée n'est pas complètement fiable). Le traitement de ce cas sort du domaine d'application du présent document.

3. Autrement, l'annonce est traitée comme décrit dans la [RFC4861].

5.4.5 Quand échoue la détection d'adresse dupliqué

Une tentative d'adresse qui se révèle être une adresse dupliquée selon ce qui est décrit ci-dessus NE DOIT PAS être allouée à une interface, et le nœud DEVRAIT enregistrer une erreur de gestion du système.

Si l'adresse est une adresse de liaison locale formée à partir d'un identifiant d'interface fondé sur l'adresse du matériel, qui est supposée être allouée de façon univoque (par exemple, EUI-64 pour une interface Ethernet) le fonctionnement de IP DEVRAIT être désactivé sur l'interface. En désactivant le fonctionnement de IP, le nœud va alors :
- ne pas envoyer de paquet IP à partir de l'interface,
- abandonner en silence tout paquet IP reçu sur l'interface, et
- ne pas transmettre de paquet IP à l'interface (lorsque elle agit comme routeur ou traite un paquet avec un en-tête Routing).

Dans ce cas, la duplication d'adresse IP signifie probablement que des adresses de matériel dupliquées sont utilisées, et essayer de se récupérer de cela en configurant une autre adresse IP ne va pas donner un réseau utilisable. En fait, cela rend probablement les choses pires en créant des problèmes qui sont plus difficiles à diagnostiquer que de simplement désactiver le fonctionnement du réseau sur l'interface ; l'usager verra un réseau qui fonctionne partiellement où certaines choses fonctionnent, et d'autres pas.

D'un autre côté, si l'adresse de liaison locale dupliquée n'est pas formée à partir d'un identifiant d'interface fondé sur l'adresse du matériel, qui est supposée être allouée de façon univoque, le fonctionnement de IP sur l'interface PEUT se poursuivre.

Note : comme spécifié à la Section 2, "IP" signifie "IPv6" dans la description ci-dessus. Bien que les raisons de fond sur l'adresse de matériel soient indépendantes des protocoles réseau, leurs effet sur les autres protocoles sortent du domaine d'application du présent document.

5.5 Création d'adresses mondiales

Les adresses mondiales sont formées en ajoutant un identifiant d'interface à un préfixe d'une longueur appropriée. Les préfixes sont obtenus à partir des options d'informations de préfixes contenues dans les annonces de routeur. La création

des adresses mondiales telle que décrite dans cette section DEVRAIT être configurable en local. Cependant, le traitement décrit ci-dessous DOIT être activé par défaut.

5.5.1 Solliciter des annonces de routeur

Les annonces de routeur sont envoyées périodiquement à l'adresse de diffusion groupée Tous-les-nœuds. Pour obtenir rapidement une annonce, un hôte envoie des sollicitations de routeur selon la description de la [RFC4861].

5.5.2 Absence d'annonce de routeur

Même si une liaison n'a pas de routeur, le service DHCPv6 pour obtenir les adresses peut être quand même disponible, et les hôtes peuvent vouloir utiliser le service. Dans la perspective de l'autoconfiguration, une liaison n'a pas de routeur si aucune annonce de routeur n'est reçue après avoir envoyé un petit nombre de sollicitations de routeur, comme décrit dans la [RFC4861].

Noter qu'il est possible qu'il n'y ait pas de routeur sur la liaison dans ce sens, mais qu'il y ait un nœud avec la capacité de transmettre les paquets. Dans ce cas, l'adresse du nœud transmetteur doit être configurée manuellement dans les hôtes pour qu'elle soit capable d'envoyer des paquets hors liaison, car le seul mécanisme pour configurer automatiquement l'adresse du routeur par défaut est celle qui utilise les annonces de routeur.

5.5.3 Traitement d'annonce de routeur

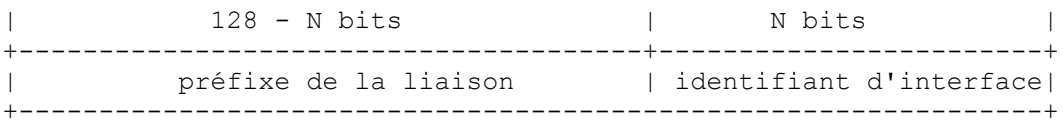
Pour chaque option Information de préfixe dans l'annonce de routeur :

a) Si le fanion Autonome n'est pas établi, ignorer en silence l'option Information de préfixe.

b) Si le préfixe est le préfixe de liaison locale, ignorer en silence l'option Information de préfixe.

c) Si la durée de vie préférée est supérieure à la durée de vie valide, ignorer en silence l'option Information de préfixe. Un nœud PEUT souhaiter enregistrer une erreur de gestion du système dans ce cas.

d) Si le préfixe annoncé n'est pas égal au préfixe d'une adresse déjà configurée par l'autoconfiguration sans état de la liste des adresses associée à l'interface (où "égal" signifie que les longueurs des deux préfixes sont les mêmes et que le premier bit de longueur de préfixe des deux préfixes est identique) et si la durée de vie valide n'est pas 0, former une adresse (et l'ajouter à la liste) en combinant le préfixe annoncé avec un identifiant d'interface de la liaison comme suit :



Si la somme de la longueur de préfixe et de la longueur de l'identifiant d'interface n'est pas égale à 128 bits, l'option Information de préfixe DOIT être ignorée. Une mise en œuvre PEUT souhaiter enregistrer une erreur de gestion du système dans ce cas. La longueur de l'identifiant d'interface est définie dans un document séparé spécifique du type de liaison, qui devrait aussi être cohérent avec l'architecture d'adresse de la [RFC4291] (voir la Section 2).

Il est de la responsabilité de l'administrateur du système de s'assurer que les longueurs des préfixes contenus dans les annonces de routeur sont cohérentes avec la longueur des identifiants d'interface pour ce type de liaison. On devrait cependant noter que cela ne signifie pas que la longueur du préfixe annoncée est sans signification. En fait, la longueur annoncée a une signification non triviale pour la détermination en-liaison dans la [RFC4861] où la somme de la longueur de préfixe et la longueur de l'identifiant d'interface peut n'être pas égale à 128. Donc, il devrait être sûr de valider ici la longueur de préfixe annoncée, afin de détecter et éviter une erreur de configuration en spécifiant une longueur de préfixe invalide dans le contexte de l'autoconfiguration d'adresse.

Noter qu'une future révision de l'architecture d'adresse [RFC4291] et un futur document spécifique du type de liaison, qui seront encore cohérents l'un avec l'autre, pourraient permettre un identifiant d'interface d'une longueur autre que la valeur définie dans les documents actuels. Donc, une mise en œuvre ne devrait pas supposer une constante particulière. Elle devrait plutôt s'attendre à n'importe quelles longueurs d'identifiants d'interface.

Si une adresse a réussi à être formée et qu'elle n'est pas encore dans la liste, l'hôte l'ajoute à la liste des adresses allouées à l'interface, initialisant ses valeurs de durée de vie préférée et valide à partir de l'option Information de préfixe. Noter que la vérification sur le préfixe effectuée au début de cette étape ne peut pas toujours détecter un conflit

d'adresses dans la liste. Il serait possible qu'une adresse déjà dans la liste, configurée manuellement ou par DHCPv6, se trouve être identique à l'adresse nouvellement créée, bien qu'un tel cas serait atypique.

e) Si le préfixe annoncé est égal au préfixe d'une adresse configurée par l'autoconfiguration sans état de la liste, la durée de vie préférée de l'adresse est rétablie à la durée de vie préférée de l'annonce reçue. L'action spécifique à effectuer pour la durée de vie valide de l'adresse dépend de la durée de vie valide dans l'annonce reçue et du temps restant à l'expiration de la durée de vie valide de la précédente adresse autoconfigurée. On appelle le temps restant la "durée de vie restante" dans la suite de l'exposé :

1. Si la durée de vie valide reçue est supérieure à deux heures ou supérieure à la durée de vie restante, régler la durée de vie valide de l'adresse correspondante à la durée de vie valide annoncée.

2. Si la durée de vie restante est inférieure ou égale à deux heures, ignorer l'option Information de préfixe en ce qui concerne la durée de vie valide, sauf si l'annonce de routeur d'où cette option a été obtenue a été authentifiée (par exemple, via la découverte de voisin sécurisée de la [RFC3971]). Si l'annonce de routeur a été authentifiée, la durée de vie valide de l'adresse correspondante devrait être réglée à la durée de vie valide dans l'option reçue.

3. Autrement, rétablir la durée de vie valide de l'adresse correspondante à deux heures.

Les règles ci-dessus visent une attaque de déni de service spécifique dans laquelle une fausse annonce pourrait contenir des préfixes avec une très courte durée de vie valide. Sans les règles ci-dessus, une seule annonce non authentifiée contenant de fausses options Information de préfixe avec des durées de vie courtes pourrait causer l'expiration prématurée de toutes les adresses d'un nœud. Ces règles assurent que les annonces légitimes (qui sont envoyées périodiquement) vont "annuler" les courtes durées de vie valides avant qu'elles ne prennent réellement effet.

Noter que la durée de vie préférée de l'adresse correspondante est toujours rétablie à la durée de vie préférée figurant dans l'option Information de préfixe reçue sans considérer si la durée de vie valide est aussi rétablie ou ignorée. La différence vient du fait que l'attaque possible sur la durée de vie préférée est relativement mineure. De plus, il est même indésirable d'ignorer la durée de vie préférée lorsque un administrateur valide veut déconseiller une adresse particulière en envoyant une durée de vie préférée courte (et que la durée de vie valide est accidentellement ignorée).

5.5.4 Expiration de la durée de vie de l'adresse

Une adresse préférée devient déconseillée lorsque sa durée de vie préférée arrive à expiration. Une adresse déconseillée DEVRAIT continuer d'être utilisée comme adresse de source dans les communications existantes, mais NE DEVRAIT PAS être utilisée pour initier de nouvelles communications si une autre adresse (non déconseillée) de portée suffisante peut facilement être utilisée à la place.

Noter que la faisabilité de l'initiation d'une nouvelle communication en utilisant une adresse non déconseillée peut être une décision spécifique de l'application, car seule l'application peut avoir connaissance de ce que l'adresse (maintenant) déconseillée était (ou est toujours) utilisée par l'application. Par exemple, si une application spécifie explicitement que la pile de protocoles utilise une adresse déconseillée comme adresse de source, la pile de protocoles doit l'accepter ; l'application pourrait le demander parce que cette adresse IP est utilisée dans une communication de niveau supérieur et qu'il pourrait y avoir l'exigence que les multiples connexions d'un tel groupement utilisent la même paire d'adresses IP.

Les couches IP et supérieures (par exemple, TCP, UDP) DOIVENT continuer d'accepter et traiter normalement les datagrammes destinés à une adresse déconseillée car une adresse déconseillée est toujours une adresse valide pour l'interface. Dans le cas de TCP, cela signifie que les segments SYN TCP envoyés à une adresse déconseillée reçoivent réponse en utilisant l'adresse déconseillée comme adresse de source dans l'ACK SYN correspondant (si la connexion est admise par ailleurs).

Une mise en œuvre PEUT empêcher toute nouvelle communication d'utiliser une adresse déconseillée, mais la gestion de système DOIT avoir la capacité de désactiver une telle facilité, et la facilité DOIT être désactivée par défaut.

D'autres cas subtils devraient aussi être notés à propos de la sélection d'adresse de source. Par exemple, la description ci-dessus ne précise pas quelle adresse devrait être utilisée entre une adresse déconseillée, une adresse de plus courte portée et une adresse non déconseillée de portée suffisante. Les détails de la sélection d'adresse incluant ce cas sont décrits dans la [RFC3484] et sortent du domaine d'application du présent document.

Une adresse (et son association à une interface) devient invalide à l'expiration de sa durée de vie valide. Une adresse invalide NE DOIT PAS être utilisée comme adresse de source dans les communications sortantes et NE DOIT PAS être reconnue comme destination sur une interface de réception.

5.6 Cohérence de la configuration

Il est possible aux hôtes d'obtenir des informations sur les adresses en utilisant à la fois l'autoconfiguration sans état et DHCPv6 car tous deux peuvent être activés en même temps. Il est aussi possible que les valeurs des autres paramètres de configuration, comme la taille de MTU et la limite des bonds, soient apprises à la fois par les annonces de routeur et par DHCPv6. Si les mêmes informations de configuration sont fournies par plusieurs sources, la valeur de ces informations devrait être cohérente. Cependant, il n'est pas considéré que ce soit une erreur fatale si les informations reçues de plusieurs sources ne sont pas cohérentes. Les hôtes acceptent l'union de toutes les informations reçues via la découverte de voisin et DHCPv6.

Si des informations contradictoires sont apprises de différentes sources, une mise en œuvre peut vouloir donner la préséance aux informations apprises de source sûre sur les informations apprises sans protection. Par exemple, la Section 8 de la [RFC3971] expose comment traiter les informations apprises par la découverte de voisin sûre qui sont en conflit avec des informations apprises par la découverte de voisin traditionnelle. La même discussion peut s'applique à la préférence entre les informations apprises par la découverte de voisin traditionnelle et les informations apprises via DHCPv6 sécurisé, et ainsi de suite.

Dans tous les cas, si il n'y a pas de différence de sécurité, les valeurs obtenues le plus récemment DEVRAIENT avoir la préséance sur les informations plus anciennes.

5.7 Conserver les adresses configurées pour des raisons de stabilité

Une mise en œuvre qui a une mémorisation stable peut vouloir conserver les adresses dans cette mémoire lorsque les adresses ont été acquises en utilisant l'autoconfiguration d'adresse sans état. En supposant que les durées de vie utilisées sont raisonnables, cette technique implique qu'une panne temporaire (moins que la durée de vie valide) d'un routeur ne va jamais résulter en la perte d'une adresse mondiale par le nœud, même si il devait se réamorcer. Lorsque cette technique est utilisée, on devrait aussi noter que les heures d'expiration de la durée de vie préférée et valide doivent être conservées, afin d'empêcher l'utilisation d'une adresse après qu'elle est devenue déconseillée ou invalide.

Les autres détails sur cette sorte d'extension sortent du domaine d'application du présent document.

6. Considérations pour la sécurité

L'autoconfiguration d'adresse sans état permet à un hôte de se connecter à un réseau, de configurer une adresse, et de commencer à communiquer avec les autres nœuds sans jamais s'enregistrer ou s'authentifier auprès du site local. Bien que cela permette à des usagers non autorisés de se connecter à un réseau et à l'utiliser, la menace est inhérente à l'architecture Internet. Tout nœud qui a un rattachement physique à un réseau peut générer une adresse (en utilisant diverses techniques ad hoc) qui fournissent la connexité.

L'utilisation de l'autoconfiguration d'adresse sans état et de la détection d'adresse dupliquée ouvre la possibilité de plusieurs attaques de déni de service. Par exemple, tout nœud peut répondre aux sollicitations de voisin pour une tentative d'adresse, causant le rejet de l'adresse comme dupliquée par l'autre nœud. Un autre document [RFC3756] discute les détails de ces attaques, qui peuvent être contrées avec le protocole de découverte de voisin sûre [RFC3971]. On devrait aussi noter que la [RFC3756] souligne que l'utilisation de la sécurité IP n'est pas toujours possible dans tous les environnements de réseau.

7. Remerciements

Thomas Narten et Susan Thompson sont les auteurs des RFC1971 et 2462. Pour la présente révision de la RFC, Tatuya Jinmei était le seul éditeur.

Les auteurs de la RFC2461 tiennent à remercier les membres des deux groupes de travail IPNG (qui s'appelle maintenant IPV6) et ADDRCONF pour leurs apports. Merci en particulier à Jim Bound, Steve Deering, Richard Draves, et Erik Nordmark. Nos remerciements vont aussi à John Gilmore pour avoir alerté le groupe de travail sur les faiblesses contre l'attaque de déni de service "Annonce de préfixe de durée de vie 0" ; le présent document incorporé des changements qui corrigent cette faiblesse.

Un certain nombre de gens ont contribué à identifier les problèmes de la RFC2461 et à proposer des solutions à ces

problèmes, qui sont reflétées dans cette version du document. En plus de ceux cités ci-dessus, on inclura parmi les contributeurs Jari Arkko, James Carlson, Brian E. Carpenter, Gregory Daley, Elwyn Davies, Ralph Droms, Jun-ichiro Itojun Hagino, Christian Huitema, Suresh Krishnan, Soohong Daniel Park, Markku Savela, Pekka Savola, Hemant Singh, Bernie Volz, Margaret Wasserman, et Vlad Yasevich.

8. Références

8.1 Références normatives

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

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

[RFC4291] R. Hinden, S. Deering, "Architecture d'adressage IP version 6", février 2006. *(Remplace* RFC3513*) (D.S.)*

[RFC4861] T. Narten et autres, "Découverte du voisin pour IP version 6 (IPv6)", septembre 2007. *(Remplace* RFC2461*) (D.S.)*

8.2 Références informatives

[RFC1112] S. Deering, "Extensions d'hôte pour diffusion groupée sur IP", STD 5, août 1989.

[RFC2710] S. Deering, W. Fenner et B. Haberman, "Découverte d'écouteur de diffusion groupée (MLD) pour IPv6", octobre 1999.

[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.

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

[RFC3590] B. Haberman, "Sélection d'adresse de source pour le protocole de découverte d'écoutant de diffusion groupée (MLD)", septembre 2003. *(P.S.)*

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

[RFC3810] R. Vida, L. Costa, éd., "Découverte d'écouteur de diffusion groupée version 2 (MLDv2) pour IPv6", juin 2004.

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

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

[RFC4941] T. Narten et autres, "Extensions de confidentialité pour l'auto configuration d'adresse sans état dans IPv6", septembre 2007. *(Remplace* RFC3041*) (D.S.)*

[IEEE802.11] IEEE, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", ANSI/IEEE STd 802.11, août 1999.

Appendice A. Suppression du bouclage et détection d'adresse dupliquée

Déterminer si une sollicitation de diffusion groupée reçue a été rebouclés sur l'envoyeur ou si elle vient réellement d'un autre nœud dépend de la mise en œuvre. Un cas problématique se présente lorsque deux interfaces rattachées à la même liaison se trouvent avoir le même identifiant et la même adresse de couche liaison, et qu'elles envoient toutes deux des paquets avec un contenu identique à peu près au même moment (par exemple, des sollicitations de voisin pour une tentative d'adresse au titre de messages de détection d'adresse dupliquée). Bien qu'un receveur reçoive les deux paquets, il ne peut pas déterminer quel paquet a été rebouclé et quel paquet vient de l'autre nœud en comparant simplement les contenus (c'est-à-dire, que les contenus sont identiques). Dans ce cas particulier, il n'est pas nécessaire de savoir précisément quel paquet a été rebouclé et lequel a été envoyé par un autre nœud ; si l'une reçoit plus de sollicitations qu'il n'en a été envoyé, la tentative d'adresse est une duplication. Cependant, la situation peut n'être pas toujours aussi simple.

La spécification de la diffusion groupée IPv4 [RFC1112] recommande que l'interface du service fournisse un moyen pour qu'un protocole de couche supérieure inhibe la livraison locale des paquets envoyés à un groupe de diffusion groupée dont l'hôte envoyeur est membre. Certaines applications savent qu'il n'y a pas d'autre membre du groupe sur le même hôte, et supprimer le rebouclage les empêche d'avoir à recevoir (et éliminer) les paquets qu'elles ont elles-mêmes envoyés. Une façon directe de mettre en œuvre cette facilité est de désactiver le rebouclage au niveau du matériel (si c'est mis en œuvre par le matériel) les paquets étant rebouclés (si nécessaire) par le logiciel. Sur les interfaces dans lesquelles le matériel lui-même supprime les rebouclages, un nœud qui fait fonctionner la détection d'adresse dupliquée compte simplement le nombre de sollicitation de voisins reçues pour une tentative d'adresse et les compare à leur nombre prévu. Si il y a discordance, la tentative d'adresse est dupliquée.

Dans les cas où le matériel ne peut pas supprimer les rebouclages, une heuristique logicielle cependant possible pour filtrer les rebouclages non désirés est d'éliminer tout paquet reçu dont l'adresse de source de couche liaison est la même que celle de l'interface de réception. Il y a même une spécification de couche liaison qui exige que de tels paquets soient éliminés [IEEE802.11]. Malheureusement, l'utilisation de ce critère résulte aussi en l'élimination de tous les paquets envoyés par un autre nœud et qui utilisent la même adresse de couche liaison. La détection d'adresse dupliquée va échouer sur les interfaces qui filtrent les paquets reçus de cette manière :

- Si un nœud qui effectue la détection d'adresse dupliquée élimine les paquets reçus qui ont la même adresse de source de couche liaison que l'interface de réception, il va aussi éliminer les paquets provenant d'autres nœuds qui utilisent aussi la même adresse de couche liaison, y compris les annonces de voisin et les message Sollicitation de voisins nécessaires pour faire fonctionner correctement la détection d'adresse dupliquée. On peut éviter ce problème particulier en désactivant temporairement la suppression logicielle des rebouclages lorsque un nœud effectue la détection d'adresse dupliquée, si il est possible de désactiver la suppression.

- Si un nœud utilisant déjà une adresse IP particulière élimine les paquets reçus qui ont la même adresse de source de couche liaison que l'interface, il va aussi éliminer les message Sollicitation de voisin en rapport avec la détection d'adresse dupliquée envoyés par d'autres nœuds qui utilisent aussi la même adresse de couche liaison. Par conséquent, la détection d'adresse dupliquée va échouer, et l'autre nœud va configurer une adresse non unique. Comme il est généralement impossible de savoir quand un autre nœud effectue la détection d'adresse dupliquée, ce scénario ne peut être évité que si la suppression logicielle du rebouclage est désactivée en permanence.

Donc, pour effectuer la détection d'adresse dupliquée correctement dans le cas où deux interfaces utilisent la même adresse de couche liaison, une mise en œuvre doit avoir une bonne compréhension de la sémantique du rebouclage de diffusion groupée de l'interface, et l'interface ne peut pas éliminer les paquets reçus simplement parce que l'adresse de source de couche liaison est la même que celle de l'interface. On notera aussi qu'une spécification de couche liaison peut être en conflit avec la condition nécessaire pour faire fonctionner la détection d'adresse dupliquée.

Appendice B. Changements par rapport à la RFC1971

- On utilise le terme "identifiant d'interface" plutôt que "jeton d'interface" par cohérence avec les autres documents IPv6.
- O, précise la définition d'adresse déconseillée pour rendre clair s'il faut continuer d'envoyer ou recevoir des adresses déconseillées.
- Ajout des règles du paragraphe 5.5.3 sur le traitement des annonces de routeur pour régler la question de potentielles attaques de déni de service lorsque les préfixes sont annoncés avec des durées de vie très courtes.
- Précise la formulation du paragraphe 5.5.4 pour dire clairement que tous les protocoles de couche supérieure doivent traiter (c'est-à-dire, envoyer et recevoir) les paquets envoyés à des adresses déconseillées.

Appendice C. Changements par rapport à la RFC2462

Des changements majeurs peuvent affecter les mises en œuvre existantes :
- Un nœud qui effectue la détection d'adresse dupliquée retarde de se joindre au groupe de diffusion groupée Nœud sollicité, et pas seulement d'envoyer les sollicitations de voisin, et explication des raisons détaillées.
- Ajout d'une exigence d'un retard aléatoire avant l'envoi des sollicitations de voisin pour la détection d'adresse dupliquée si l'adresse vérifiée est configurée par des annonces de routeur en diffusion groupée.
- Précision qu'en cas d'échec de la détection d'adresse dupliquée, le fonctionnement du réseau IP devrait être désactivé et qu'on devrait appliquer la règle lorsque l'adresse de matériel est supposée être unique.

Précisions majeures :
- que la longueur des identifiants d'interface devrait être déterminée ; on décrit la relation avec la longueur du préfixe annoncé dans les annonces de routeur, en évitant d'utiliser dans ce document une longueur particulière fixée.
- précision du traitement des annonces de voisin reçues en effectuant la détection d'adresse dupliquée.
- suppression du texte concernant les fanions M et O, vu la maturité des mises en œuvre et les expériences du fonctionnement. Les fanions ManagedFlag et OtherConfigFlag ont été supprimés en conséquence. (Noter que ce changement ne signifie pas que l'utilisation de ces fanions soit déconseillée.)
- on évite la terminologie "configuration à état plein", qui prête à confusion, pour dire simplement "DHCPv6" chaque fois que c'est approprié.
- on recommande d'effectuer plus énergiquement la détection d'adresse dupliquée pour toutes les adresses d'envoi individuel, en considérant une variété de différents identifiants d'interface, tout en faisant attention aux mises en œuvre existantes.

- précision de la formulation du paragraphe 5.5.4 pour rendre clair qu'une adresse déconseillée spécifiée par une application peut être utilisée pour toute communication
- précisé que la vérification de préfixe décrite au paragraphe 5.5.3 en utilisant des termes plus appropriés, et que la vérification est faite par rapport aux préfixes des adresses configurées par l'autoconfiguration sans état.
- changement des références à l'en-tête d'authentification de la sécurité IP pour faire référence à la RFC3971 (Découverte de voisin sûr). Et révision de la section Considérations pour la sécurité avec une référence à la RFC3756.
- ajout d'une note pour quand une mise en œuvre utilise une mémorisation stable pour les adresses autoconfigurées.
- ajout de considérations sur les préférences entre des ensembles discordants d'informations, l'un de source sûre et l'autre apprise sans protection.

Autre précisions diverses :

- suppression des références à "site local" et révision de la formulation autour des mots clés.
- suppression d'un code redondant dans la protection contre le déni de service au paragraphe 5.5.3.
- précision qu'une sollicitation ou annonce de voisin en envoi individuel devrait être éliminée lorsque on effectue la détection d'adresse dupliquée.
- on note au paragraphe 5.3 qu'une interface peut être considérée comme devenant activée lorsque un point d'accès sans fil change.

Adresse des auteurs

Thomas Narten
IBM Corporation
P.O. Box 12195

Research Triangle Park,
NC 27709-2195 USA
téléphone : +1 919-254-7798
mél : narten@us.ibm.com

Susan Thomson
Cisco Systems
mél :
sethomso@cisco.com

Tatuya Jinmei
Corporate Research & Development Center, Toshiba Corp.
1 Komukai Toshiba-cho, Saiwai-ku

Kawasaki-shi, Kanagawa 212-8582
Japan
téléphone : +81 44-549-2230
mél : jinmei@isl.rdc.toshiba.co.jp

Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est fourni par l'activité de soutien administratif (IASA) de l'IETF