Groupe de travail Réseau
Request for Comments : 5380
RFC rendue obsolète : 4140
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

H. Soliman, Elevate Technologies
C. Castelluccia, INRIA
K. ElMalki, Athonet
L. Bellier, INRIA
octobre 2008

Gestion de la mobilité pour IPv6 mobile hiérarchique

Résumé
Le présent document introduit des extensions à IPv6 mobile et à la découverte de voisin IPv6 pour permettre le traitement local de la mobilité. La gestion de la mobilité hiérarchique pour IPv6 mobile est conçue pour réduire la quantité de signalisation entre le nœud mobile, ses nœuds correspondants, et son agent de rattachement. Le point d'ancrage de mobilité (MAP, *Mobility Anchor Point*) décrit dans ce document peut aussi être utilisé pour améliorer les performances de IPv6 mobile en termes de vitesse de transfert inter-cellulaire.

Table des matières

1. Introduction

La présente spécification introduit le concept de réseau hiérarchique IPv6 mobile, utilisant un nouveau nœud appelé le point d'ancrage de mobilité (MAP, *Mobility Anchor Point*).

IPv6 mobile [RFC3775] permet aux nœuds de se déplacer dans la topologie de l'Internet tout en conservant son accessibilité et les connexions en cours entre les nœuds mobiles et correspondants. Pour ce faire, un nœud mobile envoie des mises à jour de lien (BU, *Binding Update*) à son agent de rattachement (HA, *Home Agent*) chaque fois qu'il se déplace.

Le nœud mobile peut envoyer des paquets de données via son agent de rattachement immédiatement après l'envoi de la mise à jour de lien, mais l'agent de rattachement ne va pas être capable de réacheminer le trafic au nœud mobile avant qu'il ait reçu la mise à jour de lien. Cela prend au moins la moitié d'un délai d'aller-retour avant que les paquets soient à nouveau transmis au bon endroit. Il y a un délai supplémentaire pour envoyer les paquets de données si le nœud mobile choisit d'attendre un accusé de réception de mise à jour de lient (BA, *Binding Acknowledgement*). Le temps d'aller-retour peut être relativement long si le nœud mobile et son agent de rattachement sont dans des parties du monde différentes.

Un délai supplémentaire sera aussi subi si le nœud mobile emploie l'optimisation de chemin. L'authentification des mises à jour de lien exige approximativement 1,5 temps d'aller retour entre le nœud mobile et chaque nœud correspondant (pour toute la procédure d'acheminement de retour dans le meilleur de cas, c'est-à-dire, sans perte de paquet). Cela peut être fait en parallèle avec l'envoi des mises à jour de lien à l'agent de rattachement, et il y a d'autres optimisations qui réduisent les 1,5 allers retours requis [RFC4449], [RFC4651], [RFC4866].

Néanmoins, les échanges de signalisation nécessaires pour mettre à jour la localisation vont toujours causer des perturbations aux connexions actives. Des paquets vont être perdus. Avec les délais d'établissement de connexion de couche de liaison et de couche IP, il peut y avoir des effets sur les protocoles de couche supérieure. Réduire ces délais durant la période critique de transfert inter cellulaire va améliorer les performances de IPv6 mobile.

De plus, dans le cas de liaisons sans fil, cette solution réduit le nombre de messages envoyés sur l'interface radio à tous les nœuds correspondants et à l'agent de rattachement. Un point d'ancrage local va aussi permettre à IPv6 mobile de bénéficier d'une signalisation de mobilité réduite avec les réseaux externes.

Pour ces raisons, un nouveau nœud mobile IPv6, appelé le point d'ancrage de mobilité, est utilisé et peut être situé à tout niveau d'un réseau hiérarchique de routeurs, incluant le routeur d'accès (AR, *Access Router*). Le MAP va limiter la quantité de signalisation IPv6 mobile en dehors du domaine local.

L'introduction du MAP donne une solution aux problèmes soulignés plus tôt, de la façon suivante :

- Le nœud mobile envoie des mises à jour de lien au MAP local plutôt qu'à l'agent de rattachement (HA, *Home Agent*) (qui est normalement plus loin) et aux nœuds correspondants (CN, *Corresponding Node*).

- Un seul message de mise à jour de lien a besoin d'être transmis par le nœud mobile (MN, *Mobile Node*) avant que le trafic provenant du HA et de tous les CN soit réacheminé à sa nouvelle localisation. Ceci est indépendant du nombre de CN avec lequel le MN communique.

Un MAP est essentiellement un agent de rattachement local. Le but de l'introduction du modèle de gestion de mobilité hiérarchique dans IPv6 mobile est d'améliorer les performances de IPv6 mobile tout en minimisant l'impact sur IPv6 mobile ou d'autres protocoles IPv6. De plus, HMIPv6 permet aux nœuds mobiles de cacher leur localisation aux nœuds correspondants et agents de rattachement, tout en utilisant l'optimisation de chemin IPv6 mobile. Les différences de sécurité entre le MAP et l'agent de rattachement sont décrites à la Section 12.

Il est pertinent de noter que l'utilisation du MAP ne s'appuie pas sur, ni ne suppose la présence d'un agent de rattachement permanent. En d'autres termes, un nœud mobile n'a pas besoin d'avoir une adresse de rattachement ou d'agent de rattachement permanent afin d'avoir la capacité HMIPv6 ou d'utiliser les caractéristiques de la présente spécification. Un MAP peut être utilisé par un nœud mobile de façon nomade pour réaliser la gestion de mobilité au sein d'un domaine local. Le paragraphe 6.5 décrit ce scénario.

2. Terminologie

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

De plus, on introcuit les termes suivants :

Routeur d'accès (AR, *Access Router*) : c'est le routeur par défaut du nœud mobile. L'AR agrège le trafic sortant des nœuds mobiles.

Point d'ancrage de mobilité (MAP, *Mobility Anchor Point*) : c'est un routeur situé dans un réseau visité par le nœud mobile. Le MAP est utilisé par le MN comme un HA local. Un ou plusieurs MAP peuvent exister dans un réseau visité.

Adresse d'entretien régionale (RCoA, *Regional Care-of Address*) : c'est une adresse allouée par le MAP au nœud mobile.

Nœud mobile à capacité HMIPv6 : c'est un nœud mobile qui peut recevoir et traiter l'option MAP reçue de son routeur par défaut. Un nœud mobile à capacité HMIPv6 doit aussi être capable d'envoyer les mises à jour de lien local (mise à jour de lien avec le fanion M établi).

Adresse d'entretien en liaison (LCoA) : c'est l'adresse d'entretien sur la liaison configurée sur l'interface du nœud mobile sur la base du préfixe annoncé par son routeur par défaut. Dans la [RFC3775], elle est simplement appelée l'adresse d'entretien. Cependant, dans le présent mémoire on utilise LCoA pour la distinguer de la RCoA.

Mise à jour de lien local : le MN envoie une mise à jour de lien local au MAP afin d'établir un lien entre la RCoA et la LCoA.

3. Vue d'ensemble de HMIPv6

Ce schéma de IPv6 mobile hiérarchique introduit une nouvelle fonction, le MAP, et des extensions mineures au fonctionnement du nœud mobile. Les opérations du nœud correspondant et de l'agent de rattachement ne vont pas être affectées.

Tout comme pour IPv6 mobile, cette solution est indépendante de la technologie d'accès sous-jacente, permettant la mobilité au sein ou entre différents types de réseaux d'accès.

Un nœud mobile qui entre dans un domaine de MAP va recevoir des annonces de routeur contenant des informations sur un ou plusieurs MAP locaux. Le MN peut lier sa localisation actuelle (LCoA) à une adresse sur le sous réseau du MAP (RCoA). Agissant comme un HA local, le MAP va recevoir tous les paquets au nom du nœud mobile qu'il sert et va les encapsuler et les transmettre directement à l'adresse actuelle du nœud mobile. Si le nœud mobile change son adresse actuelle dans un domaine local du MAP (LCoA) il a seulement besoin d'enregistrer la nouvelle adresse auprès du MAP. Donc, seule la CoA régionale (RCoA) a besoin d'être enregistrée auprès des nœuds correspondants et du HA. La RCoA ne change pas tant que le MN bouge dans un domaine de MAP (voir la définition plus loin). Cela rend la mobilité du nœud mobile transparente aux nœuds correspondants avec lesquels il communique.

Les frontières du domaine d'un MAP sont définies par les routeurs d'accès (AR, *Access Router*) qui annoncent les informations de MAP aux nœuds mobiles rattachés. Le détail des extensions à IPv6 mobile et au fonctionnement des différents nœuds sera expliqué plus loin dans ce document.

On devrait noter que le concept de HMIPv6 est simplement une extension du protocole IPv6 mobile. Un nœud mobile à capacité HMIPv6 avec une mise en œuvre de IPv6 mobile DEVRAIT choisir d'utiliser le MAP quand il découvre une telle capacité dans un réseau visité. Cependant, dans certains cas, le nœud mobile peut préférer simplement utiliser la mise en œuvre standard IPv6 mobile. Par exemple, le nœud mobile peut être situé dans un réseau visité au sein de son site de rattachement. Dans ce cas, le HA est situé près du réseau visité et pourrait être utilisé à la place d'un MAP. Dans ce scénario, le nœud mobile va seulement mettre à jour le HA chaque fois qu'il bouge. La méthode pour déterminer si le HA est dans le voisinage du MN (par exemple, le même site) sort du domaine d'application du présent document.

3.1 Fonctionnement de HMIPv6

L'architecture de réseau montrée à la Figure 1 illustre un exemple de l'utilisation du MAP dans un réseau visité.

Dans la Figure 1, le MAP peut aider à fournir une mobilité sans interruption au nœud mobile lorsque il passe du routeur d'accès 1 (AR1) au routeur d'accès 2 (AR2), tout en communiquant avec le nœud correspondant. Une hiérarchie multi niveaux n'est pas exigée pour de meilleures performances de transfert inter cellulaires. Donc, il est suffisant de localiser un ou plusieurs MAP (éventuellement couvrant le même domaine) dans n'importe quelle position dans le réseau de l'opérateur.

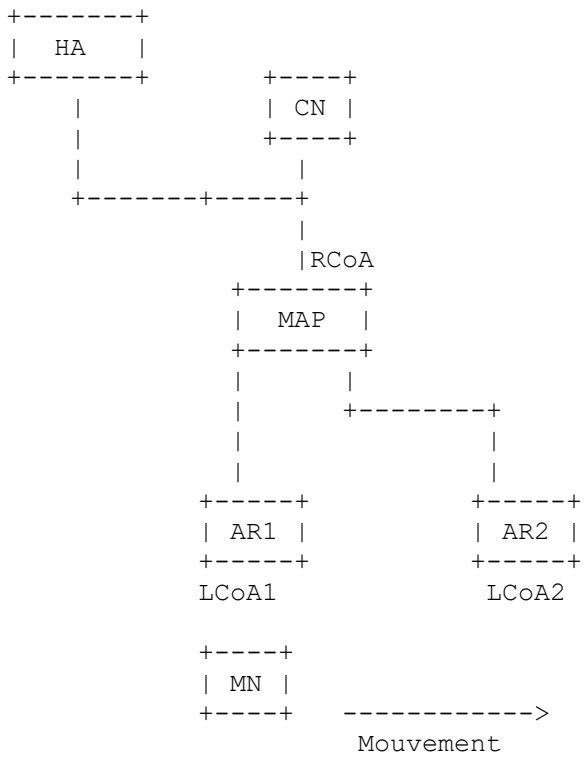

Figure 1 : Domaine IPv6 mobile hi"rarchisue

À l'arrivée dans un réseau visité, le nœud mobile va découvrir l'adresse mondiale du MAP. Cette adresse est mémorisée dans les routeurs d'accès et communiquée au nœud mobile via des annonces de routeur (RA, *Router Advertisement*). Une nouvelle option pour les RA est définie plus loin. C'est nécessaire pour informer les nœuds mobiles de la présence du MAP (découverte de MAP). La phase de découverte va aussi informer le nœud mobile de la distance du MAP au nœud mobile. Par exemple, la fonction de MAP pourrait être mise en œuvre comme montré à la Figure 1, et, en même temps, être aussi mise en œuvre dans AR1 et AR2. Dans ce cas, le nœud mobile peut choisir le MAP de premier bond ou un plus loin dans la hiérarchie des routeurs. Les détails de la façon de choisir un MAP sont donnés à la Section 10.

Le processus de découverte de MAP se poursuit lorsque le nœud mobile passe d'un sous réseau à un autre. Chaque fois que le nœud mobile détecte un mouvement, il va aussi détecter si il est encore dans le même domaine de MAP. L'annonce de routeur utilisée pour détecter le mouvement va aussi informer le nœud mobile, par la découverte de voisin [RFC4861] et l'option MAP, de si il est encore dans le même domaine du MAP. Comme le nœud mobile circule dans un domaine de MAP, il va continuer de recevoir la même option de MAP incluse dans les annonces de routeur provenant de son AR. Si un changement est reçu dans l'adresse de MAP annoncée, le nœud mobile DOIT agir sur le changement en envoyant des mises à jour de lien à son HA et ses nœuds correspondants.

Si le nœud mobile n'a pas la capacité HMIPv6, aucune découverte de MAP ne va être effectuée, ce qui fait que le nœud mobile utilise le protocole IPv6 mobile [RFC3775] pour la gestion de sa mobilité. Par ailleurs, si le nœud mobile a la capacité HMIPv6, il DEVRAIT choisir d'utiliser sa mise en œuvre HMIPv6. Si il le fait, le nœud mobile va d'abord devoir s'enregistrer auprès d'un MAP en lui envoyant une BU contenant son adresse de rattachement et son adresse d'entretien en liaison (LCoA). L'adresse de rattachement utilisée dans la BU est la RCoA, que le nœud mobile acquiert via les mécanismes de la Section 9 de la [RFC4877] quand il prend contact avec un MAP. Le MAP DOIT mémoriser ces informations dans son antémémoire de liens pour être capable de transmettre les paquets à leur destination finale quand ils

sont reçus des différents nœuds correspondants ou HA.

Le nœud mobile va toujours avoir besoin de savoir l'envoyeur original de tout paquet reçu pour déterminer si l'optimisation de chemin est requise. Cette information va être disponible au nœud mobile parce que le MAP ne modifie pas le contenu du paquet original. Le traitement normal des paquets reçus (comme décrit dans la [RFC3775]) va donner au nœud mobile les informations nécessaires.

Pour utiliser la bande passante du réseau de manière plus efficace, un nœud mobile peut décider de s'enregistrer simultanément avec plus d'un MAP et d'utiliser chaque adresse de MAP pour un groupe spécifique de nœuds correspondants. Par exemple, dans la Figure 1, si le nœud correspondant se trouve exister sur la même liaison que le nœud mobile, il serait plus efficace d'utiliser le MAP de premier bond (dans ce cas on suppose que c'est AR1) pour communiquer entre eux. Cela va éviter d'envoyer tous les paquets via le "plus haut" MAP dans la hiérarchie et donc va résulter en un usage plus efficace de la bande passante du réseau. Le nœud mobile peut aussi utiliser son adresse en liaison actuelle (LCoA) comme CoA, comme spécifié dans la [RFC3775]. Noter que le nœud mobile NE DOIT PAS présenter une RCoA provenant d'un sous réseau du MAP comme une LCoA dans une mise à jour de lien envoyée à un autre MAP. La LCoA incluse dans la mise à jour de lien DOIT être l'adresse du nœud mobile, dérivée du préfixe annoncé sur sa liaison.

4. Extension IPv6 mobile – mise à jour de lien local

Cette section précise les extensions proposées à la mise à jour de lien spécifiée dans la [RFC3775].

Un nouveau fanion est ajouté : le fanion M, qui indique l'enregistrement de MAP. Quand un nœud mobile s'enregistre auprès du MAP, les fanions M et A DOIVENT être établis pour distinguer cet enregistrement d'une BU envoyée au HA ou au nœud correspondant.

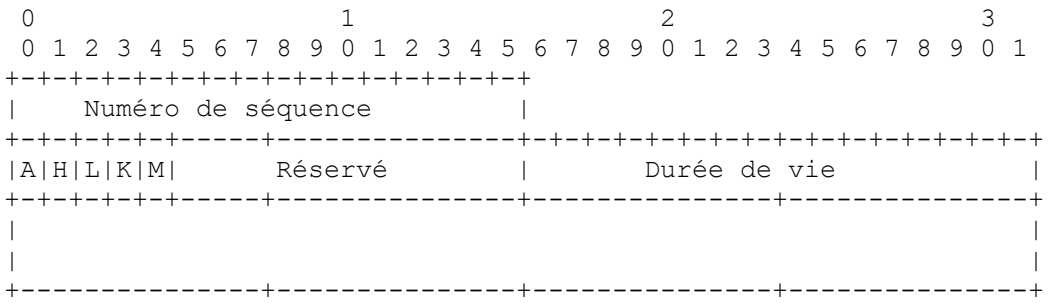

Figure 2 : Mise à jour de lien local

M : réglé à 1, il indique un enregistrement de MAP.

5. Extension de découverte de voisin : option MAP

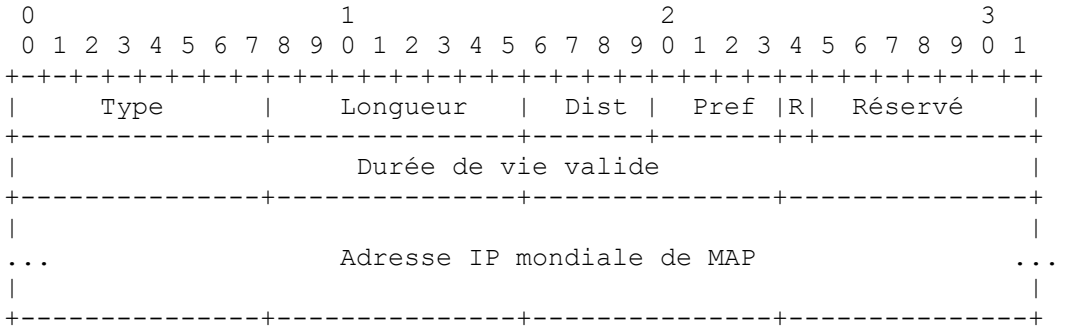

Figure 3 : Option MAP

Type : option Découverte de voisin IPv6. Sa valeur est 23.

Longueur : entier non signé de 8 bits. La longueur de l'option DOIT être réglée à 3.

Dist : entier non signé de 4 bits qui identifie la distance entre le MAP et le receveur de l'annonce, mesuré en nombre de bonds et commençant à 1 si le MAP est sur la même liaison que le nœud mobile. Une valeur de distance de zéro NE DOIT PAS être utilisée.

Pref : champ de préférence, utilisé comme indicateur de la préférence d'opérateur. Entier non signé de 4 bits. Une valeur décimale de 15 indique la plus forte préférence. Quand il compare deux MAP potentiels, le nœud mobile DEVRAIT inspecter ce champ comme départage des MAP qui ont d'égales valeurs de Distance.

R : réglé à 1, il indique que la RCoA est allouée au nœud mobile par le MAP sur la base de la Section 9 de la [RFC4877].

Durée de vie valide : valeur minimum (en secondes) de la durée de vie valide du préfixe utilisé pour former l'adresse du MAP et de celle utilisée pour former la RCoA. Cette valeur indique la validité de l'adresse du MAP's et de la RCoA.

Adresse mondiale : une des adresses mondiales du MAP.

6. Fonctionnement du protocole

Cette section décrit le protocole HMIPv6. Dans HMIPv6, le nœud mobile a deux adresses, une RCoA sur la liaison du MAP et une CoA en liaison (LCoA). Cette RCoA est formée sans état en combinant l'identifiant d'interface du nœud mobile et le préfixe de sous réseau reçu dans l'option MAP.

Comme illustré dans cette section, ce protocole exige de mettre à jour seulement la mise en œuvre de nœuds mobile. Le HA et le nœud correspondant sont inchangés. Le MAP effectue la fonction de HA "local" qui lie la RCoA du nœud mobile à une LCoA.

6.1 Fonctionnement du nœud mobile

Quand un nœud mobile passe dans un nouveau domaine de MAP (c'est-à-dire, son MAP change) il a besoin de configurer deux CoA : une RCoA sur la liaison du MAP et une CoA en liaison (LCoA). Après avoir employé la [RFC4877] pour acquérir une RCoA, le nœud mobile envoie une BU locale au MAP avec les fanions A et M établis. La BU locale est une BU définie dans la [RFC3775] et inclut la RCoA du nœud mobile dans l'option Adresse de rattachement. Aucune autre option de CoA n'est nécessaire dans ce message. La LCoA est utilisée comme adresse de source de la BU. Cette BU va lier la RCoA du nœud mobile (similaire à une adresse de rattachement) à sa LCoA. Le MAP (agissant comme un HA) va alors retourner un accusé de réception de lien au MN. Cet accusé de réception identifie le lien comme réussi ou contient le code de faute approprié. Aucun nouveau code d'erreur n'a besoin d'être pris en charge par le nœud mobile pour cette opération. Le nœud mobile DOIT ignorer en silence les accusés de réception de lien qui ne contiennent pas d'en-tête d'acheminement de type 2, qui inclut la RCoA du nœud mobile.

Suite à l'enregistrement réussi avec le MAP, un tunnel bidirectionnel entre le nœud mobile et le MAP est établi. Tous les paquets envoyés par le nœud mobile sont tunnelés au MAP. L'en-tête externe contient la LCoA du nœud mobile dans le champ d'adresse de source, et l'adresse du MAP dans le champ d'adresse de destination. L'en-tête interne contient la RCoA du nœud mobile dans le champ d'adresse de source, et l'adresse de l'homologue dans le champ d'adresse de destination. De même, tous les paquets adressés à la RCoA du nœud mobile sont interceptés par le MAP et tunnelés à la LCoA du nœud mobile.

La présente spécification permet à un nœud mobile d'utiliser plus d'une RCoA si il reçoit plus d'une option de MAP. Dans ce cas, le nœud mobile PEUT effectuer la procédure de mise à jour de lien pour chaque RCoA. De plus, le nœud mobile NE DOIT PAS utiliser une RCoA (par exemple, la RCoA1) déduite du préfixe d'un MAP (par exemple, le MAP1) comme adresse d'entretien dans sa mise à jour de lien à un autre MAP (par exemple, le MAP2). Cela forcerait les paquets à être encapsulés plusieurs fois (deux fois dans cet exemple) sur leur chemin vers le nœud mobile. Cette forme de hiérarchie multi niveaux réduirait l'efficacité et les performances du protocole.

Après l'enregistrement auprès du MAP, le nœud mobile DOIT enregistrer sa nouvelle RCoA auprès de ses HA en envoyant une BU qui spécifie le lien (RCoA, adresse de rattachement) comme dans IPv6 mobile. L'adresse de rattachement du nœud mobile est utilisée dans l'option Adresse de rattachement et la RCoA est utilisée comme adresse d'entretien dans le champ

d'adresse de source. Le nœud mobile peut aussi envoyer une BU similaire (c'est-à-dire, qui spécifie le lien entre l'adresse de rattachement et la RCoA) à ses nœuds correspondants courants.

Le nœud mobile DEVRAIT attendre l'accusé de réception du lien de la part du MAP avant d'enregistrer la RCoA auprès des autres nœuds (par exemple, CN ou HA, si disponibles). On devrait noter que quand on lie la RCoA au HA et les nœuds correspondants, la durée de vie du lien NE DOIT PAS être supérieure à la durée de vie du lien du nœud mobile avec le MAP, qui est reçue dans l'accusé de réception du lien.

Afin d'accélérer le transfert inter cellulaires entre les MAP et réduire les pertes de paquets, un nœud mobile DEVRAIT envoyer une BU locale à son MAP précédent, spécifiant sa nouvelle LCoA. Les paquets en transit qui atteignent le MAP précédent sont alors transmis à la nouvelle LCoA.

Le MAP va recevoir les paquets adressés à la RCoA du nœud mobile (provenant du HA ou des nœuds correspondants). Les paquets vont être tunnelés du MAP à la LCoA du nœud mobile. Le nœud mobile va désencapsuler les paquets et les traiter de façon normale.

Quand le nœud mobile bouge au sein du même domaine de MAP, il devrait seulement enregistrer sa nouvelle LCoA auprès de son MAP. Dans ce cas, la RCoA reste inchangée.

Noter qu'un nœud mobile peut envoyer une BU contenant sa LCoA (au lieu de sa RCoA) aux nœuds correspondants. Si ces nœuds sont connecté à la même liaison, les paquets vont alors être acheminés directement, sans passer par le MAP.

6.1.1 Envoi de paquets aux nœuds correspondants

Le nœud mobile peut communiquer avec un nœud correspondant à travers le HA, ou avec un chemin optimisé, comme décrit dans la [RFC3775]. Quand il communique à travers le HA, les formats de message de la [RFC3775] sont utilisés.

Si le nœud mobile communique directement avec le nœud correspondant (c'est-à-dire, si le CN a une entrée d'antémémoire de lien pour le nœud mobile) le nœud mobile DOIT utiliser la même adresse d'entretien qu'utilisée pour créer une entrée d'antémémoire de lien dans le nœud correspondant (RCoA) comme adresse de source. Conformément à la [RFC3775], le nœud mobile DOIT aussi inclure une option d'adresse de rattachement dans les paquets sortants. L'option d'adresse de rattachement DOIT contenir l'adresse de rattachement du nœud mobile.

6.2 Fonctionnement du MAP

Le MAP agit comme un HA ; il intercepte tous les paquets adressés aux nœuds mobiles enregistrés et les tunnelle à la LCoA correspondante, qui est mémorisée dans son antémémoire de lien.

Un MAP n'a pas connaissance de l'adresse de rattachement du nœud mobile. Le nœud mobile va envoyer une BU locale au MAP avec les fanions M et A établis. Le but de cette BU est de lier la RCoA (contenue dans la BU comme adresse de rattachement) à la LCoA du nœud mobile. Si cela réussit, le MAP DOIT retourner un accusé de réception de lien au nœud mobile, indiquant la réussite de l'enregistrement. Ceci est identique à l'opération du HA dans la [RFC3775]. Aucun nouveau code d'erreur n'est introduit pour HMIPv6. L'accusé de réception de lien DOIT inclure un en-tête d'acheminement de type 2 qui contient la RCoA du nœud mobile.

Le MAP DOIT être capable d'accepter les paquets tunnelés du nœud mobile, le nœud mobile étant le point d'entrée du tunnel et le MAP étant le point de sortie du tunnel.

Le MAP emploie les procédures de la Section 9 de la [RFC4877] pour l'allocation de la RCoA, et agit ensuite comme un HA pour la RCoA. Les paquets adressés à la RCoA sont interceptés par le MAP, en utilisant l'annonce de voisin mandataire, et ensuite encapsulés et acheminés à la LCoA du nœud mobile. Cette opération est identique à celle du HA décrite dans la [RFC3775].

Un MAP PEUT être configuré avec la liste des préfixes valides sur la liaison que les nœuds mobiles peuvent utiliser pour déduire les LCoA. Ceci est utile pour les opérateurs de réseau qui ont besoin d'arrêter la poursuite par les nœuds mobiles de l'utilisation du MAP après qu'ils sont passés à un domaine administratif différent. Si un nœud mobile envoie une mise à jour de lien contenant une LCoA qui n'est pas dans la liste des "préfixes valides sur la liaison" du MAP, le MAP pourrait rejeter la mise à jour de lien en utilisant le code d'erreur existant 129 (interdit administrativement).

6.3 Fonctionnement de l'agent de rattachement

La prise en charge de HMIPv6 est complètement transparente au fonctionnement du HA. Les paquets adressés à l'adresse de rattachement d'un nœud mobile vont être transmis au HA à sa RCoA, comme décrit dans la [RFC3775].

6.4 Fonctionnement de l'agent correspondant

HMIPv6 est complètement transparent aux nœuds correspondants.

6.5 Optimisation de la gestion de la mobilité locale dans un domaine MAP

Dans la [RFC3775], il est déclaré que pour une communication à court terme, en particulier une communication qui peut facilement être réessayée en cas d'échec, le nœud mobile PEUT choisir d'utiliser directement une de ses adresses d'entretien comme source du paquet, n'exigeant donc pas l'utilisation d'une option Adresse de rattachement dans le paquet. Une telle utilisation de la CoA va réduire les frais généraux d'envoi de chaque paquet du fait de l'absence d'options supplémentaires. De plus, elle va fournir un chemin optimal entre le nœud mobile et le nœud correspondant.

Les nœuds mobiles à capacité HMIPv6 peuvent utiliser leur RCoA comme adresse de source sans utiliser d'option Adresse de rattachement. En d'autres termes, la RCoA peut être utilisée comme adresse de source pour les couches supérieures. En utilisant cette caractéristique, le nœud mobile va être vu par le nœud correspondant comme un nœud fixe alors qu'il se déplace dans le domaine du MAP.

Cet usage de la RCoA n'est pas aussi coûteux que celui d'IPv6 mobile (c'est-à-dire, pas de liens ou d'options Adresse de rattachement envoyés sur l'Internet) mais fournit quand même à la gestion de la mobilité locale aux nœuds mobiles un acheminement presque optimal. Bien qu'une telle utilisation de la RCoA n'assure pas la mobilité mondiale (c'est-à-dire, la communication est coupée quand un nœud mobile change sa RCoA) elle serait utile pour plusieurs applications (par exemple, la navigation sur la Toile). La validité de la RCoA comme adresse de source utilisée par les applications va dépendre de la taille du domaine du MAP et de la vitesse du nœud mobile. De plus, parce que la prise en charge du traitement de BU dans les nœuds correspondants n'est pas exigée par la [RFC3775], ce mécanisme peut fournir un moyen d'obtenir l'optimisation de chemin sans envoyer de BU aux nœuds correspondants.

L'activation de ce mécanisme peut être faite en présentant la RCoA comme une adresse de rattachement temporaire pour le nœud mobile. Cela peut exiger qu'une mise en œuvre augmente son algorithme de choix d'adresse de source de la connaissance de la RCoA afin de l'utiliser pour les applications appropriées.

6.6 Confidentialité de la localisation

Dans HMIPv6, un nœud mobile cache sa LCoA à ses nœuds correspondants et à son agent de rattachement en utilisant sa RCoA dans le champ Source des paquets qu'il envoie. Par suite, le suivi de localisation fondé sur l'adresse d'un nœud mobile par ses nœuds correspondants ou son agent de rattachement est plus difficile parce que ils savent seulement sa RCoA et pas sa LCoA.

7. Découverte de MAP

Cette section décrit comment un nœud mobile obtient l'adresse et le préfixe de sous réseau du MAP, et comment les AR dans un domaine découvrent les MAP.

La présente spécification exige des administrateurs de réseau qu'il configurent manuellement les informations d'option MAP dans les AR ; des mécanismes futurs pourront être définis pour permettre que les MAP soient découverts de façon dynamique.

7.1 Fonctionnement du nœud mobile

Quand un nœud mobile à capacité HMIPv6 reçoit une annonce de routeur, il devrait chercher l'option MAP. Une ou plusieurs options peuvent être trouvées pour différentes adresses IP de MAP. Un nœud mobile DEVRAIT s'enregistrer auprès du MAP ayant la plus forte valeur de préférence. Un MAP avec une valeur de préférence de zéro NE DEVRAIT PAS être utilisé pour une nouvelle BU locale (c'est-à-dire, le nœud mobile peut rafraîchir les liens existants mais ne peut

pas en créer de nouveaux). Cependant, un nœud mobile PEUT choisir de s'enregistrer auprès d'un MAP plutôt que sur un autre, selon la valeur reçue dans le champ Distance, pourvu que la valeur de préférence soit supérieure à zéro.

Une option MAP contenant une valeur de durée de vie valide de zéro signifie que ce MAP NE DOIT PAS être choisi par le MN. Une durée de vie valide de zéro indique une défaillance du MAP. Quand cette option est reçue, un nœud mobile DOIT choisir un autre MAP et créer de nouveaux liens. Tout lien existant avec ce MAP peut être supposé perdu. Si aucun autre MAP n'est disponible, le nœud mobile NE DOIT PAS tenter d'utiliser HMIPv6.

Si un nœud mobile multi rattachements a accès à plusieurs AR simultanément (sur des interfaces différentes) il DEVRAIT utiliser une LCoA sur la liaison définie par l'AR qui annonce son MAP actuel.

Un nœud mobile DOIT mémoriser la ou les options reçues afin de choisir au moins un MAP avec lequel s'enregistrer. Mémoriser les options est essentiel, car elles vont être comparées aux autres options reçues plus tard pour les besoins de l'algorithme de détection de mouvement.

Si le fanion R est établi, le nœud mobile DOIT placer sa RCoA à la place de l'adresse de rattachement dans le message de mise à jour de lien. Cela cause la liaison de la RCoA à la LCoA dans l'antémémoire de lien du MAP.

Un nœud mobile PEUT choisir de s'enregistrer avec plus d'un MAP simultanément, ou d'utiliser à la fois la RCoA et sa LCoA comme adresses d'entretien simultanément avec différents nœuds correspondants.

8. Mise à jour des MAP précédents

Quand a nœud mobile passe dans un nouveau domaine de MAP, le nœud mobile peut envoyer une BU au MAP précédent pour lui demander de transmettre les paquets adressés à la nouvelle CoA du nœud mobile. Un administrateur PEUT interdire au MAP de transmettre les paquets aux LCoA extérieures au domaine du MAP. Cependant, il est RECOMMANDÉ que les MAP soient autorisés à transmettre les paquets aux LCoA associées à certains des AR dans les domaines de MAP du voisinage, pourvu qu'ils soient situés dans le même domaine administratif.

Par exemple, un MAP pourrait être configuré à transmettre des paquets aux LCoA associées aux AR qui sont géographiquement adjacents aux AR sur la frontière de son domaine. Cela va permettre une transition en douceur inter MAP car cela permet au nœud mobile de continuer à recevoir les paquets tout en mettant à jour le nouveau MAP, son HA et, potentiellement, les nœuds correspondants.

9. Note sur le choix de MAP par le nœud mobile

HMIPv6 donne un mécanisme souple pour la gestion de la mobilité locale au sein d'un réseau visité. Comme expliqué précédemment, un MAP peut exister n'importe où dans le réseau d'un opérateur (y compris l'AR). Plusieurs MAP peuvent être situés dans le même domaine indépendamment l'un de l'autre. De plus, des domaines de MAP en chevauchement sont aussi permis et recommandés. Des hiérarchies statiques et dynamiques sont prises en charge.

Quand le nœud mobile reçoit une annonce de routeur qui comporte une option MAP, il devrait effectuer des actions en accord avec les mécanismes de détection de mouvement suivantes. Dans un réseau IP mobile hiérarchique, comme celui décrit dans ce document, le nœud mobile devrait être :
- o "ardent" à effectuer de nouveaux liens ;
- o "paresseux" à libérer les liens existants.

Cela signifie que le nœud mobile devrait s'enregistrer avec tout "nouveau" MAP annoncé par le AR (ardent). La méthode par laquelle le nœud mobile détermine si le MAP est un "nouveau" MAP est décrite au paragraphe 9.1. Le nœud mobile ne devrait pas libérer les liens existants avant de ne plus recevoir l'option MAP (ou qu'il la reçoive avec une durée de vie de zéro) ou que la durée de vie de son lien existant arrive à expiration (paresseux). Cette approche ardent-paresseux, décrite ci-dessus, va aider à fournir un mécanisme de repli en cas de défaillance d'un des routeurs de MAP, car elle va réduire le temps nécessaire pour qu'un nœud mobile informe ses nœuds correspondants et le HA de sa nouvelle adresse d'entretien.

9.1 Choix de MAP dans un environnement de MAP réparti

Le nœud mobile DOIT examiner plusieurs facteurs pour choisir de façon optimale un ou plusieurs MAP, lorsque plusieurs

MAP sont disponibles dans le même domaine.

Il n'y a pas d'avantage prévu à choisir plus d'un MAP et de forcer les paquets à être envoyés depuis le MAP le plus élevé en descendant une hiérarchie de MAP. Cette approche peut ajouter des délais de transmission et éliminer la robustesse de l'acheminement IP entre le MAP le plus élevé et le nœud mobile ; donc, elle est interdite par cette spécification. Permettre plus d'un MAP ("au dessus" de l'AR) au sein d'un réseau ne devrait pas impliquer que le nœud mobile force les paquets à être acheminés en descendant la hiérarchie de MAP. Cependant, placer plus d'un MAP "au dessus" de l'AR peut être utilisé pour avoir de la redondance et comme optimisation des différents scénarios de mobilité rencontrés par les nœuds mobiles. Les MAP sont utilisés indépendamment l'un de l'autre par le MN (par exemple, chaque MAP est utilisé pour communiquer avec un certain ensemble de CN).

En terme de choix fondé sur la distance dans un réseau avec plusieurs MAP, un nœud mobile peut choisir de s'enregistrer avec le MAP le plus lointain pour éviter de fréquents réenregistrements. Ceci est particulièrement important pour les nœuds mobiles rapides qui vont effectuer de fréquentes itinérances. Dans ce scénario, le choix d'un AP plus distant va réduire la probabilité d'avoir à changer de MAP et d'informer tous les nœuds correspondants et le HA.

Dans un scénario où plusieurs MAP sont découverts par le nœud mobile dans un domaine, le nœud mobile peut avoir besoin d'algorithmes sophistiqués pour être capable de choisir le MAP approprié. Ces algorithmes auraient la vitesse du nœud mobile en entrée (pour le choix fondé sur la distance) combinée avec le champ de préférence dans l'option de MAP. Cependant, la présente spécification propose que le nœud mobile utilise l'algorithme suivant par défaut, lorsque d'autres algorithmes optimisés ne sont pas disponibles. L'algorithme suivant se fonde simplement sur le choix du MAP qui est le plus distant, pourvu que cette valeur de préférence n'atteigne pas la valeur de zéro. Le fonctionnement du nœud mobile est montré ci-dessous :

1. Recevoir et analyser toutes les options de MAP.

2. Arranger les MAP en ordre décroissant, en commençant par le MAP le plus éloigné (c'est-à-dire, l'option de MAP qui a le plus grand champ Dist).

3. Choisir le premier MAP de la liste.

4. Si les champs valeur de préférence ou durée de vie valide sont réglés à zéro, choisir le MAP suivant dans la liste.

5. Répéter l'étape (4) lorsque il existe encore de nouvelles options de MAP, jusqu'à ce que soit trouvé un MAP avec une valeur de préférence non zéro et une durée de vie valide non zéro.

La mise en œuvre des étapes ci-dessus va résulter en ce que les nœuds mobiles choisissent, par défaut, le MAP le plus distant ou le plus loin disponible. Cela va continuer jusqu'à ce que la valeur de préférence se réduise à zéro. À la suite de cela, les nœuds mobiles vont commencer à choisir un autre MAP.

9.2 Choix de MAP dans une architecture de mobilité plate

Les opérateurs de réseau peuvent choisir une architecture plate dans certains cas où un transfert IPv6 mobile peut être considéré comme un événement rare. Dans ces scénarios, les opérateurs peuvent choisir d'inclure la fonction de MAP seulement dans les AR. L'inclusion de la fonction de MAP dans les AR peut encore être utile pour réduire le temps requis pour mettre à jour tous les nœuds correspondants et le HA. Dans ce scénario, un nœud mobile peut choisir un MAP (dans l'AR) comme un point d'ancrage quand il effectue un transfert inter cellulaires. Cette sorte de hiérarchie dynamique (ou ancrage) n'est recommandée que dans les cas où le mouvement inter-AR n'est pas fréquent.

10. Détection et récupération de défaillances de MAP

La présente spécification introduit un MAP qui peut être vu comme un agent de rattachement local dans un réseau visité. Un MAP, comme un agent de rattachement, est un seul point de défaillance. Si un MAP a une défaillance, le contenu de son antémémoire de liens va être perdu, résultant en la perte de la communication entre les nœuds mobiles et correspondants. Cette situation peut être évitée en utilisant plus d'un MAP sur la même liaison et en utilisant une forme de protocole de transfert de contexte entre eux. Cependant, la redondance de MAP sort du domaine d'application du présent document.

Dans les cas où de tels protocoles ne sont pas pris en charge, le nœud mobile va avoir besoin de détecter les défaillances de MAP. Le nœud mobile peut détecter cette situation quand il reçoit une annonce de routeur contenant une option de MAP avec une durée de vie de zéro. Le nœud mobile devrait alors commencer le processus de découverte de MAP et tenter de s'enregistrer auprès d'un autre MAP. Après avoir choisi et s'être enregistré auprès d'un autre MAP, il va aussi devoir informer les nœuds correspondants et l'agent de rattachement si sa RCoA a changé. Noter qu'en présence d'un protocole qui transfère les entrées d'antémémoire de liens entre les MAP pour les besoins de redondance, un nouveau MAP peut être capable de fournir la même RCoA au nœud mobile (par exemple, si les deux MAP annoncent le même préfixe dans l'option de MAP). Cela épargnerait au nœud mobile la mise à jour des nœuds correspondants et de l'agent de rattachement.

Les routeurs d'accès peuvent être déclenchés à annoncer une option de MAP avec une durée de vie de zéro (indiquant la défaillance du MAP) de différentes façons :
- o par intervention manuelle,
- o de façon dynamique.

Une façon d'effectuer la détection dynamique d'une défaillance de MAP peut être en sondant le MAP régulièrement (par exemple, toutes les 10 secondes). Si aucune réponse n'est reçue, un AR PEUT essayer de sonder agressivement le MAP pendant une courte période (par exemple, une fois toutes les 5 secondes pendant 15 secondes) ; si aucune réponse n'est reçue, une option de MAP peut être envoyée avec une valeur de durée de vie valide de zéro. Les mécanismes exacts pour le sondage des MAP sortent du domaine d'application du présent document. Le texte ci-dessus donne simplement un exemple de détection de défaillance.

La présente spécification n'exige aucun mécanisme de récupération particulier. Cependant, tout mécanisme entre le MAP et un AR DEVRAIT être sécurisé pour permettre l'authentification, la protection de l'intégrité, et la protection contre les attaques en répétition du message.

Noter que la suggestion ci-dessus pour détecter une défaillance de MAP ne peut pas détecter les défaillances de MAP qui ont lieu entre les sondes, c'est-à-dire, si un MAP réamorce entre les sondes.

11. Impacts du tunnelage sur la MTU

La présente spécification exige que le nœud mobile tunnelle le trafic sortant pour le MAP. De même, le MAP tunnelle les paquets entrants pour le nœud mobile. Si le nœud mobile a un agent de rattachement ailleurs dans l'Internet, il va en résulter des doubles encapsulations des paquets entrants et sortants. Cela peut avoir un impact sur la MTU de chemin du nœud mobile. Donc, les nœuds mobiles DOIVENT tenir compte de l'encapsulation du trafic entre le nœud et le MAP quand ils calculent la MTU disponible pour les couches supérieures.

12. Considérations sur la sécurité

La présente spécification introduit un nouveau concept pour IPv6 mobile, à savoir, un point d'ancrage de mobilité qui agit comme un agent de rattachement local. Il est crucial que les relations de sécurité entre le nœud mobile et le MAP soient fortes ; elles DOIVENT impliquer l'authentification mutuelle, la protection de l'intégrité, et la protection contre les attaques en répétition. La confidentialité peut être nécessaire pour le trafic de charges utile, comme quand le nœud mobile ne veut révéler aucun trafic au réseau d'accès au delà de ce qui est nécessaire pour que le nœud mobile se rattache au réseau et communique avec un MAP. La confidentialité n'est pas requise pour les mises à jour de lien au MAP. L'absence de ces protections peut conduire des nœuds mobiles malveillants à se faire passer pour des nœuds légitimes ou pour un MAP. Toutes ces attaques vont sans doute causer des impacts indésirables sur la communication du nœud mobile avec tous les nœuds correspondants qui ont connaissance de la RCoA du nœud mobile.

Trois relations différentes (relatives à la sécurisation des mises à jour de lien) doivent être considérées :
1. nœud mobile - MAP
2. nœud mobile - nœud correspondant
3. nœud mobile - agent de rattachement

12.1 Sécurité nœud mobile – MAP

Afin de permettre à un nœud mobile d'utiliser le service de transmission du MAP, l'autorisation initiale (spécifiquement pour le service, non pour la RCoA) PEUT être nécessaire. Autoriser un nœud mobile à utiliser le service de MAP peut être

fait sur la base de l'identité du nœud mobile échangée durant leprocessus de négociation de l'association de sécurité (SA). L'autorisation peut être accordée sur la base de l'identité du nœud mobile ou sur l'identité d'une autorité de certification (CA) de confiance pour le MAP. Par exemple, si le nœud mobile présente un certificat signé par une entité de confiance (par exemple, une CA qui appartient au même domaine administratif, ou un autre partenaire d'itinérance de confiance) cela serait suffisant pour que le MAP autorise l'utilisation de son service. Noter que ce niveau d'autorisation est indépendant de l'autorisation de l'usage d'une RCoA particulière. De même, le nœud mobile fait confiance au MAP si il présente un certificat signé par la même CA ou par une autre CA que le nœud mobile est configuré à tenir pour de confiance (par exemple, un partenaire d'itinérance). Il est probable que certains déploiements vont se satisfaire de l'utilisation de certificats auto signés pour le nœud mobile ou le MAP ou les deux. Cela garantit que le nœud mobile et le MAP sont authentifiés pour l'allocation d'adresse et les futures mises à jour de lien sans avoir besoin de l'authentification de l'identité. Donc, l'utilisation de certificats d'un tiers de confiance n'est pas exigée par la présente spécification.

Il est important de noter que dans cette spécification, authentification et autorisation sont effectivement la même chose. Tout ce dont le MAP a besoin afin d'allouer une RCoA au nœud mobile est d'authentifier le nœud mobile et de vérifier qu'il appartient à un groupe de confiance (sur la base de son certificat).

IKEv2 DOIT être pris en charge par le nœud mobile et le MAP. IKEv2 permet l'utilisation du protocole d'authentification extensible (EAP, *Extensible Authentication Protocol*) comme mécanisme pour amorcer l'association de sécurité entre les homologues communicants.

Donc, EAP peut être utilisé avec IKEv2 pour appuyer l'infrastructure d'authentification, autorisation et comptabilité (AAA, *Authentication, Authorization, and Accounting*) pour amorcer la SA entre le nœud mobile et le MAP. Un tel mécanisme est utile dans les scénarios où un administrateur souhaite éviter la configuration et la gestion de certificats sur les nœuds mobiles. Un MAP PEUT prendre en charge l'utilisation de EAP sur IKEv2.

Si EAP est utilisé avec IKEv2, la méthode EAP fonctionne entre le nœud mobile et un serveur AAA. Suite à une authentification réussie, le matériel de chiffrement résultant peut être utilisé pour amorcer IKEv2 entre le MAP et le nœud mobile. La spécification de la méthode EAP qui devrait être utilisée ou comment les clés sont transportées entre le MAP et le serveur AAA sort du domaine d'application du présent document.

HMIPv6 utilise un enregistrement supplémentaire entre le nœud mobile et son MAP courant. Comme expliqué dans ce document, quand un nœud mobile passe à un nouveau domaine (c'est-à-dire, est servi par un nouveau MAP) il obtient une RCoA et une LCoA et enregistre le lien entre ces deux adresses auprès du nouveau MAP. Le MAP vérifie alors la BU et crée une entrée d'antémémoire de lien avec la RCoA et la LCoA. Chaque fois que le nœud mobile obtient une nouvelle LCoA, il a besoin d'envoyer une nouvelle BU qui spécifie le lien entre sa RCoA et sa nouvelle LCoA. Cette BU doit être authentifiée ; autrement, tout hôte pourrait envoyer une BU pour la RCoA du nœud mobile et capturer les paquets du nœud mobile.

Le MAP n'a pas besoin d'avoir préalablement connaissance de l'identité du nœud mobile ou de son adresse de rattachement. Par suite, la SA entre le nœud mobile et le MAP peut être établie en utilisant tout protocole d'établissement de clés comme IKEv2. Un essai d'acheminement de retour n'est pas nécessaire.

Le MAP doit établir la SA pour la RCoA (pas la LCoA). Cela peut être effectué avec IKEv2 [RFC4306]. Le nœud mobile utilise sa LCoA comme adresse de source, mais spécifie que la RCoA devrait être utilisée dans la SA.

Ceci est fait en utilisant la RCoA comme identité dans la négociation de la SA fille IKE. Cette étape est identique à l'utilisation de l'adresse de rattachement dans la SA fille IKE lors de la négociation avec l'agent de rattachement.

Les entrées IPsec dans la base de données d'autorisation d'homologue (PAD, *Peer Authorization Database*) et les charges utiles de configuration décrites dans la [RFC4877] pour allouer dynamiquement les adresses de rattachement DEVRAIENT être utilisées par le MAP pour allouer les RCoA aux nœuds mobiles. Les mises à jour de liens entre le MAP et le nœud mobile DOIVENT être protégées avec un en-tête d'authentification (AH) ou une charge utile de sécurité encapsulante (ESP) en mode transport. Quand ESP est utilisé, un algorithme d'authentification non nul DOIT être utilisé.

Les entrées de la base de données de politique de sécurité (SDP, *Security Policy Database*) chez l'agent de rattachement et le nœud mobile sont identiques à celles établies pour l'agent de rattachement et le nœud mobile dans la [RFC4877].

12.2 Sécurité nœud mobile – nœud correspondant

IPv6 mobile [RFC3775] définit une procédure d'acheminement de retour qui permet aux nœuds mobiles et correspondants

d'authentifier les mises à jour de lien et leurs accusés de réception. La présente spécification n'a pas d'impact sur l'essai d'acheminement de retour défini dans la [RFC3775]. Cependant, il est important de noter que les mises en œuvre de nœud mobile doivent faire attention dans le choix de l'adresse de source des messages HoTI et CoTI, définis dans la [RFC3775]. L'adresse de source utilisée dans les messages HoTI DEVRAIT être l'adresse de rattachement du nœud mobile sauf si le nœud mobile souhaite utiliser la RCoA pour l'optimisation de chemin. Le paquet contenant le message HoTI est encapsulé deux fois. L'en-tête encapsulant interne contient la RCoA dans le champ Adresse de source et l'adresse de l'agent de rattachement dans le champ d'adresse de destination. L'en-tête encapsulant externe contient la LCoA du nœud mobile dans le champ Adresse de source et l'adresse du MAP dans le champ de destination.

12.3 Sécurité nœud mobile – agent de rattachement

Les relations de sécurité entre le nœud mobile et son agent de rattachement, discutées dans la [RFC3775], ne sont pas impactées par la présente spécification.

Les relations entre le MAP et le nœud mobile ne sont pas impactées par la présence d'un agent de rattachement.

13. Considérations relatives à l'IANA

L'option MAP et le fanion M ont été alloués pour la RFC4140 et vont continuer d'être utilisés par cette spécification.

14. Remerciements

Les auteurs tiennent à remercier Conny Larsson (Ericsson) et Mattias Pettersson (Ericsson) de leurs précieux apports à ce document. Les auteurs veulent aussi remercier les membres du projet français RNRT MobiSecV6 (BULL, France Telecom, et INRIA) qui ont essayé la première mise en œuvre et ont fourni de précieux retours. Le projet INRIA HMIPv6 est partiellement financé par le gouvernement français.

De plus, les auteurs tiennent à remercier les membres suivants du groupe de travail, par ordre alphabétique : Samita Chakrabarti (Sun), Gregory Daley, Gopal Dommety (Cisco), Francis Dupont (GET/Enst Bretagne), Eva Gustaffson (Ericsson), Dave Johnson (Rice University), Annika Jonsson (Ericsson), James Kempf (Docomo labs), Martti Kuparinen (Ericsson), Fergal Ladley, Gabriel Montenegro (Microsoft), Nick "Sharkey" Moore, Vidya Narayanan (Qualcomm), Erik Nordmark (Sun), Basavaraj Patil (Nokia), Brett Pentland (NEC), Thomas Schmidt, et Alper Yegin (Samsung) de leurs commentaires sur le document.

15. Références

15.1 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)

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

[RFC4306] C. Kaufman, "Protocole d'échange de clés sur Internet (IKEv2)", décembre 2005. *(Obsolète, voir la* RFC5996)

[RFC4861] T. Narten et autres, "Découverte du voisin pour IP version 6 (IPv6)", septembre 2007. (*Remplace* RFC2461) *(D.S. ; MàJ par* RFC8028, RFC8319, RFC8425, RFC9131)

[RFC4877] V. Devarapalli, F. Dupont, "Fonctionnement de IPv6 mobile avec IKEv2 et l'architecture IPsec révisée", avril 2007. (*MàJ* RFC3776) *(P.S.)*

15.2 Références pour information

[RFC4449] C. Perkins, "Sécurisation de l'optimisation de chemin IPv6 mobile avec une clé partagée statique", juin 2006. *(P.S.)*

[RFC4651] C. Vogt, J. Arkko, "Taxonomie et analyse des améliorations à l'optimisation de l'acheminement IPv6 mobile", février 2007. *(Information)*

[RFC4866] J. Arkko, C. Vogt, W. Haddad, "Optimisation d'acheminement amélioré pour IPv6 mobile", mai 2007. *(P.S.)*

Appendice A. Changements par rapport à la RFC 4140

- La découverte dynamique de MAP a été supprimée.
- La Section des considérations sur la sécurité a été mise à jour pour utiliser IKEv2 au lieu de IKEv1.
- Le document a précisé que HMIPv6 peut être utilisé sans avoir besoin d'un agent de rattachement.
- Corrections rédactionnelles tout au long du document.
- IKEv2 est maintenant seul utilisé pour allouer le RCoA.

La RFC 4140 était mise en œuvre et son inter opérabilité a été vérifiée par au moins deux organisations différentes. Une suite d'essais incluant des cas d'essais pour la RFC 4140 a aussi été développée par Ericsson avec une confrontation aux deux mises en œuvre. Aucun problème majeur n'a été trouvé. L'adaptabilité de la découverte dynamique de MAP, définie dans la RFC 4140, a été perçue comme inappropriée pour les déploiements à grande échelle et enclins aux boucles. Elle a été supprimée de la spécification.

Pour l'instant, il n'y a pas de déploiement publiquement connu de cette spécification.

Adresse des auteurs'

Hesham Soliman
Elevate Technologies
hesham@elevatemobile.com

Claude Castelluccia
INRIA
claude.castelluccia@inria.fr

Karim ElMalki
Athonet
karim@elmalki.homeip.net

Ludovic Bellier
INRIA
mél : ludovic.bellier@inria.fr

Déclaration complète de droits de reproduction

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 le 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.