Groupe de travail Réseau
Request for Comments : 5213
Catégorie : Sur la voie de la normalisation

S. Gundavelli, éditeur, Cisco
K. Leung, Cisco
V. Devarapalli, Wichorus
K. Chowdhury, Starent Networks
B. Patil, Nokia

Traduction Claude Brière de L'Isle
août 2008

Mandataire IPv6 mobile

Résumé
La gestion de la mobilité fondée sur le réseau permet la mobilité IP pour un hôte sans exiger sa participation à de la signalisation en relation avec la mobilité. Le réseau est chargé de gérer la mobilité IP au nom de l'hôte. Les entités de mobilité dans le réseau sont chargées de suivre les mouvements de l'hôte et d'initier la signalisation de mobilité requise en son nom. La présente spécification décrit un protocole de gestion de la mobilité fondée sur le réseau appelé mandataire IPv6 mobile.

Table des Matières

1. Introduction

La mobilité IP pour les hôtes IPv6 est spécifiée dans IPv6 mobile [RFC3775]. IPv6 mobile exige la fonction de client dans la pile IPv6 d'un nœud mobile. L'échange des messages de signalisation entre le nœud mobile et l'agent de rattachement permet la création et le maintien d'un lien entre l'adresse de rattachement du nœud mobile et son adresse d'entretien. La mobilité comme spécifiée dans la [RFC3775] exige que l'hôte IP envoie des messages de signalisation de gestion de mobilité IP à l'agent de rattachement, qui est situé dans le réseau.

La mobilité fondée sur le réseau est une autre approche pour résoudre le défi de la mobilité IP. Il est possible de prendre en charge la mobilité pour les nœuds IPv6 sans implication de l'hôte en étendant les messages de signalisation IPv6 mobile [RFC3775] entre un nœud de réseau et un agent de rattachement. Cette approche de prise en charge de la mobilité n'exige pas que le nœud mobile soit impliqué dans l'échange des messages de signalisation entre lui-même et l'agent de rattachement. Un agent de mobilité mandataire dans le réseau effectue la signalisation avec l'agent de rattachement et fait la gestion de la mobilité au nom du nœud mobile rattaché au réseau. À cause de l'utilisation et de l'extension de signalisation IPv6 mobile et de la fonction d'agent de rattachement, ce protocole est appelé mandataire IPv6 mobile (PMIPv6).

Les déploiements de réseau qui sont conçus pour prendre en charge la mobilité vont ignorer les capacités dans la pile IPv6 des nœuds qu'ils desservent. La mobilité IP pour les nœuds qui ont une fonction de client IP mobile dans la pile IPv6 ainsi que ceux qui ne l'ont pas, va être prise en charge en activant la fonction de protocole de mandataire IPv6 mobile dans le réseau. Les avantages du développement d'un protocole de mobilité fondé sur le réseau sur IPv6 mobile sont :

- La réutilisation de la fonction d'agent de rattachement et des messages/formats utilisés dans la signalisation de mobilité. IPv6 mobile est un protocole mûr avec plusieurs mises en œuvre qui ont subi des essais d'interopérabilité.

- Un agent de rattachement commun va servir d'agent de mobilité pour tous les types de nœuds IPv6.

La position du problème et le besoin d'une solution de protocole de mobilité fondé sur le réseau a été documentée dans la [RFC4830]. Le mandataire IPv6 mobile est une solution qui répond à ces problèmes et exigences.

2. Conventions et terminologie

2.1 Conventions du présent document

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

2.2 Terminologie

Tous les termes généraux relatifs à la mobilité utilisés dans le présent document sont à interpréter comme défini dans la spécification de base IPv6 mobile [RFC3775]. Le présent document adopte les termes, ancre de mobilité locale (LMA, *Local Mobility Anchor*) et passerelle d'accès mobile (MAG, *Mobile Access Gateway*) provenant du document Objectifs de la gestion de la mobilité localisée sur la base des réseaux (NETLMM) [RFC4831]. Le présent document fournit aussi les explications spécifiques du contexte suivantes des termes utilisés dans ce document.

Domaine de mandataire IPv6 mobile (domaine PMIPv6) : domaine de mandataire IPv6 mobile se réfère au réseau où la gestion de mobilité d'un nœud mobile est traitée en utilisant le protocole de mandataire IPv6 mobile comme défini dans la présente spécification. Le domaine de mandataire IPv6 mobile inclut des ancres de mobilité locales et des passerelles d'accès mobile entre lesquelles des associations de sécurité peuvent être établies et où l'autorisation d'envoyer des mises à jour de lien de mandataire au nom des nœuds mobiles peut être assurée.

Ancre de mobilité locale (LMA) : l'ancre de mobilité locale est l'agent de rattachement pour le nœud mobile dans un domaine de mandataire IPv6 mobile. C'est le point d'ancrage topologique pour le ou les préfixes de réseau de rattachement du nœud mobile et c'est l'entité qui gère l'état de lien du nœud mobile. L'ancre de mobilité locale a les capacités fonctionnelles d'un agent de rattachement comme défini dans la spécification de base IPv6 mobile [RFC3775] avec les capacités supplémentaires requises pour prendre en charge le protocole de mandataire IPv6 mobile comme défini dans la la présente spécification.

Passerelle d'accès mobile (MAG) : c'est une fonction d'un routeur d'accès qui gère la signalisation relative à la mobilité pour un nœud mobile qui est rattaché à sa liaison d'accès. Elle est chargée de suivre les mouvements du nœud mobile de et vers la liaison d'accès et pour signaler l'ancre de mobilité locale du nœud mobile.

Nœud mobile (MN, *Mobile Node*) : dans le présent document, le terme de nœud mobile est utilisé pour se référer à un hôte ou routeur IP dont la mobilité est gérée par le réseau. Le nœud mobile peut être un nœud seulement IPv4, un nœud seulement IPv6, ou un nœud double pile et n'est pas obligé de participer à de la signalisation relative à la mobilité IP pour réaliser la mobilité pour une adresse IP obtenue dans ce domaine de mandataire IPv6 mobile.

Adresse de LMA (LMAA) : adresse mondiale configurée sur l'interface de l'ancre de mobilité locale et est le point d'extrémité de transport du tunnel bidirectionnel établi entre l'ancre de mobilité locale et la passerelle d'accès mobile. C'est l'adresse à laquelle la passerelle d'accès mobile envoie les messages de mise à jour de lien de mandataire. Quand il supporte la traversée de IPv4, c'est-à-dire, quand le réseau entre l'ancre de mobilité locale et la passerelle d'accès mobile est un réseau IPv4, cette adresse va être une adresse IPv4 et va être appelée une IPv4-LMAA, comme spécifié dans la [RFC5844].

Adresse d'entretien de mandataire (Proxy-CoA, *Proxy Care-of Address*) : Proxy-CoA est l'adresse mondiale configurée sur l'interface de sortie de la passerelle d'accès mobile et est le point d'extrémité de transport du tunnel entre l'ancre de mobilité locale et la passerelle d'accès mobile. L'ancre de mobilité locale voit cette adresse comme l'adresse d'entretien du nœud mobile et l'enregistre dans l'entrée d'antémémoire de liens pour ce nœud mobile. Quand le réseau de transport entre la passerelle d'accès mobile et l'ancre de mobilité locale est un réseau IPv4 et si l'adresse d'entretien qui est enregistrée à l'ancre de mobilité locale est une adresse IPv4, le terme de IPv4-Proxy-CoA est utilisé, comme spécifié dans la [RFC5844].

Préfixe de réseau de rattachement de nœud mobile (MN-HNP, *Mobile Node's Home Network Prefix*) : le MN-HNP est un préfixe alloué à la liaison entre le nœud mobile et la passerelle d'accès mobile. Plus d'un préfixe peut être alloué à la liaison entre le nœud mobile et la passerelle d'accès mobile, et dans ce cas, tous les préfixes alloués sont gérés comme un ensemble associé à une session de mobilité. Le nœud mobile configure son interface avec une ou plusieurs adresses provenant de son ou ses préfixes de réseau de rattachement. Si le nœud mobile se connecte au domaine de mandataire IPv6 mobile par plusieurs interfaces, simultanément, chacune des interfaces rattachées va recevoir un ensemble unique de préfixes de réseau de rattachement, et tous les préfixes alloués à une certaine interface d'un nœud mobile vont être gérés sous une session de mobilité. Par exemple, les préfixes de réseau de rattachement P1 et P2 alloués à l'interface I1 vont être gérés sous une session de mobilité, et les préfixes P3, P4, et P5 alloués à l'interface I2 du nœud mobile vont

être gérés sous une session de mobilité différente. De plus, dans certaines configurations, le préfixe alloué peut être d'une longueur de 128 bits.

Adresse de rattachement de nœud mobile (MN-HoA, *Mobile Node's Home Address*) : MN-HoA est une adresse tirée du préfixe de réseau de rattachement d'un nœud mobile. Le nœud mobile va être capable d'utiliser cette adresse tant qu'il est rattaché au réseau d'accès qui est dans la portée de ce domaine de mandataire IPv6 mobile. Si le nœud mobile utilise plus d'une adresse provenant de son ou ses préfixes de réseau de rattachement, chacune de ces adresses est appelée une adresse de rattachement du nœud mobile. À la différence de IPv6 mobile où l'agent de rattachement sait l'adresse de rattachement du nœud mobile, dans le protocole de mandataire IPv6 mobile, les entités de mobilité savent seulement le ou les préfixes de réseau de rattachement du nœud mobile et ne sont pas toujours informées de la ou les adresses exactes que le nœud mobile a configuré sur son interface à partir de son ou ses préfixes de réseau de rattachement. Cependant, dans certaines configurations et sur la base des modes de configuration d'adresse activés sur la liaison d'accès, les entités de mobilité dans le réseau peuvent être certaines de la ou des adresses exactes configurées par le nœud mobile.

Liaison de rattachement du nœud mobile : c'est la liaison sur laquelle le nœud mobile a obtenu sa configuration d'adresse de couche 3 pour l'interface rattachée après qu'il est passé dans ce domaine de mandataire IPv6 mobile. C'est la liaison qui suit conceptuellement le nœud mobile. Le réseau va s'assurer que le nœud mobile voit toujours cette liaison par rapport à la configuration de couche 3 du réseau, sur toute liaison d'accès à laquelle il se rattache dans ce domaine de mandataire IPv6 mobile.

Nœud mobile multi rattachements : un nœud mobile qui se connecte au même domaine de mandataire IPv6 mobile par plus d'une interface et utilise ces interfaces simultanément est appelé un nœud mobile multi ratttachements.

Identifiant de nœud mobile (MN-Identifiant) : identité d'un nœud mobile dans le domaine de mandataire IPv6 mobile. C'est l'identifiant stable d'un nœud mobile que les entités de mobilité dans un domaine de mandataire IPv6 mobile peuvent toujours acquérir et utiliser pour identifier de façon prévisible un nœud mobile. C'est normalement un identifiant comme un identifiant d'accès réseau (NAI, *Network Access Identifier*) [RFC4282] ou un autre identifiant comme une adresse de commande d'accès au support physique (MAC, *Media Access Control*).

Identifiant de couche de liaison de nœud mobile(MN-LL-Identifier, *Mobile Node Link-layer Identifier*) : identifiant de l'interface rattachée d'un nœud mobile. Pour les interfaces qui ont un identifiant de couche de liaison, cet identifiant peut être fondé sur lui. L'identifiant de couche de liaison, dans certains cas, est généré par le nœud mobile et porté à la passerelle d'accès mobile. Cet identifiant de l'interface rattachée doit être stable, vu par les passerelles d'accès mobile dans un certain domaine de mandataire IPv6 mobile. Dans d'autres cas, il pourrait n'y avoit aucun identifiant de couche de liaison associé à l'interface du nœud mobile. Une valeur d'identifiant de TOUT_ZÉRO n'est pas considérée être un identifiant valide et ne peut pas être utilisée comme identifiant d'interface.

Profil de politique : c'est un terme abstrait pour se référer à un ensemble de paramètres de configuration qui sont configurés pour un certain nœud mobile. Les entités de mobilité dans le domaine de mandataire IPv6 mobile exigent un accès à ces paramètres pour fournir la gestion de la mobilité à un certain nœud mobile. Les détails spécifiques de la façon dont les entités du réseau obtiennent ce profil de politique sortent du domaine d'application de ce document.

Mise à jour de lien de mandataire (PBU, *Proxy Binding Update*) : message de demande envoyé par une passerelle d'accès mobile à l'ancre de mobilité locale d'un nœud mobile pour établir un lien entre le ou les préfixes de réseau de rattachement du nœud mobile alloués à une certaine interface d'un nœud mobile et son adresse d'entretien actuelle (Proxy-CoA).

Accusé de réception de lien de mandataire (PBA, *Proxy Binding Acknowledge*) : message envoyé par l'ancre de mobilité locale en réponse à un message de mise à jour de lien de mandataire qu'elle a reçu d'une passerelle d'accès mobile.

Modèles de préfixe par nœud mobile et de préfixe partagé : le terme de modèle de préfixe par nœud mobile est utilisé pour se référer à un modèle d'adressage où il y a un unique préfixe réseau alloué pour chaque nœud. Le terme de modèle de préfixe partagé est utilisé pour se référer à un modèle d'adressage où le ou les préfixes sont partagés par plus d'un nœud. La présente spécification prend en charge le modèle de préfixe par nœud mobile et ne prend pas en charge le modèle de préfixe partagé.

Session de mobilité : dans le contexte de la spécification de mandataire IPv6 mobile, le terme de session de mobilité se réfère à la création ou l'existence de l'état associé au lien de mobilité du nœud mobile sur l'ancre de mobilité locale et sur la passerelle d'accès mobile qui le desservent.

DHCP : dans ce document, l'acronyme DHCP se réfère à DHCP pour IPv6, comme défini dans la [RFC3315].

TOUT_ZÉRO et NON_ZÉRO : champs de message de protocole initialisés avec la valeur 0 dans chaque octet du champ. Par exemple, un champ d'identifiant de couche de liaison de 8 octets avec la valeur réglée à 0 dans chacun des 8 octets, ou une adresse IPv6 avec la valeur 0 dans tous les 16 octets. À l'inverse, le terme NON_ZÉRO est utilisé pour se référer à toute valeur autre que TOUT_ZÉRO.

3. Vue d'ensemble du protocole de mandataire IPv6 mobile

La présente spécification décrit le protocole de gestion de la mobilité fondée sur le réseau. Il est appelé le protocole de mandataire IPv6 mobile et se fonde sur IPv6 mobile [RFC3775].

Le protocole de mandataire IPv6 mobile est destiné à fournir la prise en charge de la gestion de la mobilité IP fondée sur le réseau à un nœud mobile, sans exiger la participation du nœud mobile à la signalisation relative à la mobilité IP. Les entités de mobilité dans le réseau vont suivre les mouvements du nœud mobile et vont initier la signalisation de la mobilité et établir l'état d'acheminement requis.

Les entités fonctionnlles centrales dans l'infrastructure NETLMM sont l'ancre de mobilité locale (LMA) et la passerelle d'accès mobile (MAG). L'ancre de mobilité locale est chargée de maintenir l'état d'accessibilité du nœud mobile et est le point d'ancrage topologique pour le ou les préfixes de réseau de rattachement du nœud mobile. La passerelle d'accès mobile est l'entité qui effectue la gestion de la mobilité au nom d'un nœud mobile, et elle réside sur la liaison d'accès où le nœud mobile est ancré. La passerelle d'accès mobile est chargée de détecter les mouvements du nœud mobile de et vers la liaison d'accès et d'initier les enregistrements de liens à l'ancre de mobilité locale du nœud mobile. Il peut y avoit plusieurs ancres de mobilité locales dans un domaine de mandataire IPv6 mobile, chacune desservant un groupe différent de nœuds mobiles. L'architecture d'un domaine de mandataire IPv6 mobile est montrée à la Figure 1.

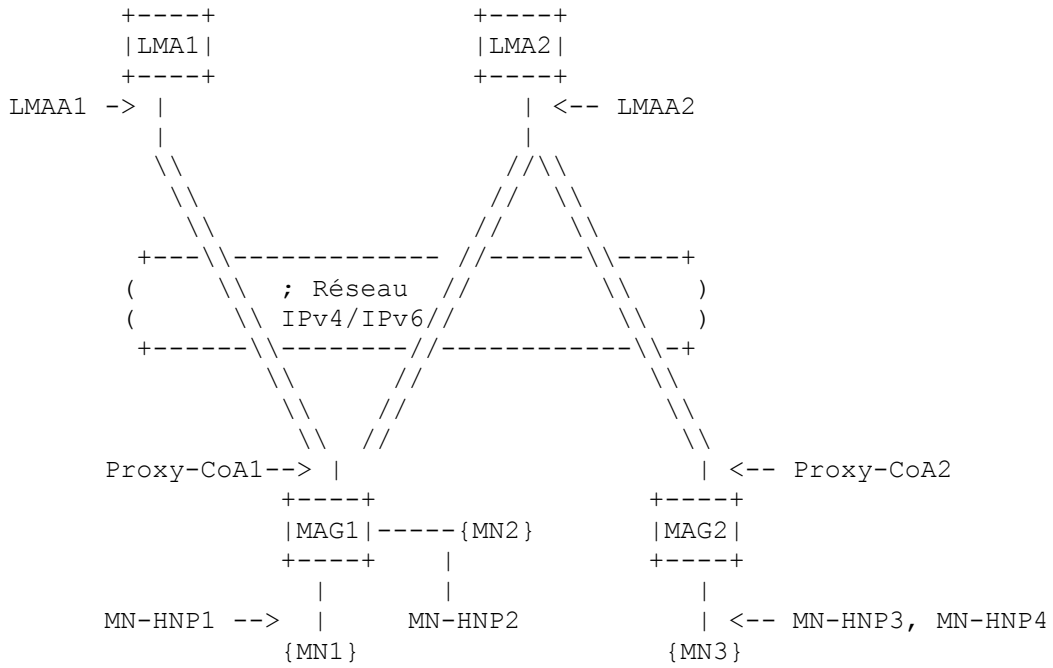


Figure 1 : Domaine de mandataire IPv6 mobile

Quand un nœud mobile entre dans un domaine de mandataire IPv6 mobile et se rattache à une liaison d'accès, la passerelle d'accès mobile sur cette liaison d'accès, après avoir identifié le nœud mobile et acquis son identité, va déterminer si le nœud mobile est autorisé pour le service de gestion de la mobilité fondée sur le réseau.

Si le réseau détermine que le nœud mobile est autorisé pour le service de mobilité fondée sur le réseau, le réseau va s'assurer que le nœud mobile en utilisant un des mécanismes de configuration d'adresse permis par le réseau va être capable d'obtenir la configuration d'adresse sur l'interface connectée et se déplace n'importe où dans ce domaine de mandataire IPv6 mobile. La configuration d'adresse obtenue inclut la ou les adresses provenant de son ou ses préfixes de réseau de rattachement, l'adresse de routeur par défaut sur la liaison, et les autres paramètres relatifs à la configuration. Du point de vue de chaque nœud mobile, le domaine de mandataire IPv6 mobile entier apparaît comme une seule liaison, le réseau

s'assure que le nœud mobile ne détecte aucun changement par rapport à son rattachement de couche 3 même après le changement de son point de rattachement dans le réseau.

Le nœud mobile peut être un nœud seulement IPv4, un nœud seulement IPv6, ou un nœud double pile (IPv4/v6). Sur la base des informations du profil de politique qui indique le type d'adresse ou les préfixes à allouer pour le nœud mobile dans le réseau, le nœud mobile va être capable d'obtenir une adresse IPv4, IPv6, ou double pile IPv4/IPv6 et passer n'importe où dans ce domaine de mandataire IPv6 mobile. Cependant, la présente spécification ne prend en charge que la mobilité d'adresse/préfixe IPv6 avec le réseau de transport IPv6. La prise en charge de l'adressage IPv4 ou un réseau de transport IPv4 est spécifiée dans la [RFC5844].

Si le nœud mobile se connecte au domaine de mandataire IPv6 mobile par plusieurs interfaces et sur plusieurs réseaux d'accès, le réseau va allouer un ensemble unique de préfixes de réseau de rattachement pour chacune des interfaces connectées. Le nœud mobile va être capable de configurer la ou les adresses sur ces interfaces à partir des préfixes respectifs de réseau de rattachement. Cependant, si le nœud mobile effectue un relais en déplaçant sa configuration d'adresse d'une interface à une autre, et si l'ancre de mobilité locale reçoit un conseil de relais de la passerelle d'accès mobile desservante sur la même, l'ancre de mobilité locale va allouer le ou les mêmes préfixes de réseau de rattachement qu'elle avait alloués précédemment avant le relais. Le nœud mobile va aussi être capable d'effectuer un relais en changeant son point de rattachement d'une passerelle d'accès mobile à une passerelle d'accès mobile différente en utilisant la même interface et va être capable de conserver la configuration d'adresse sur l'interface rattachée.

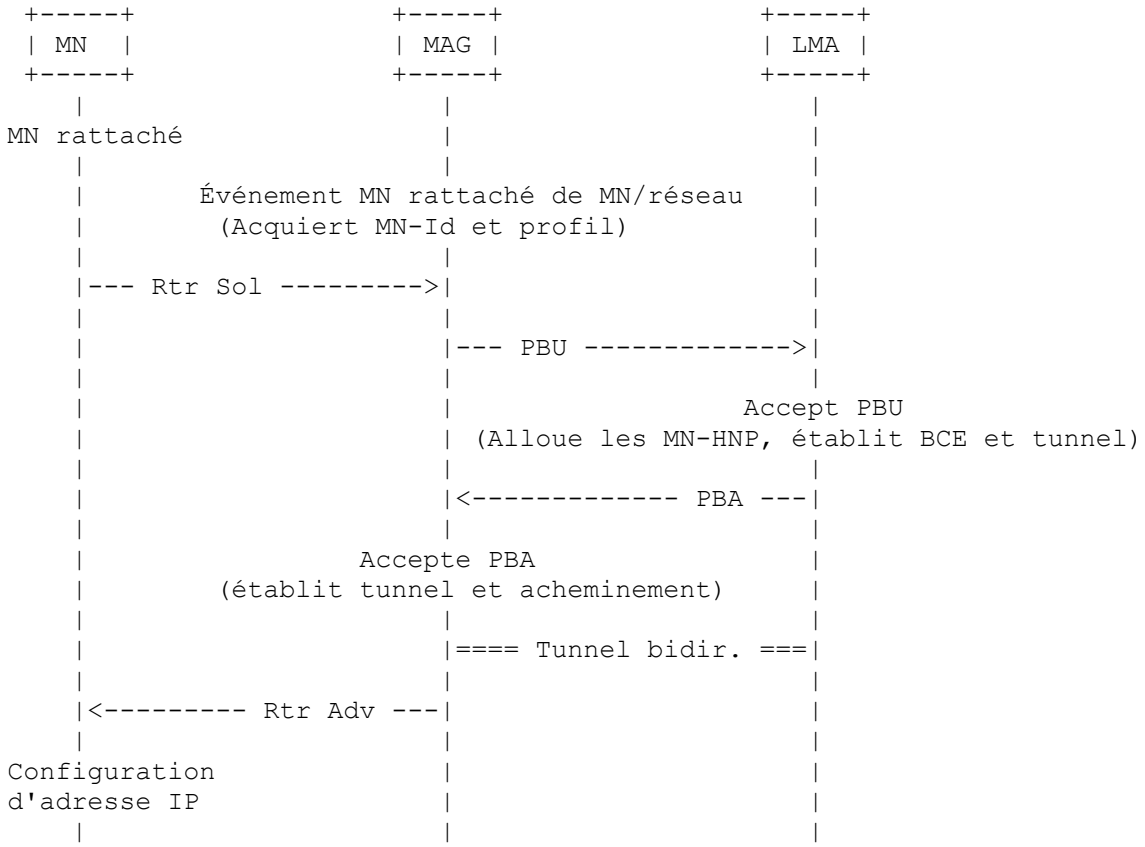


Figure 2 : Rattachement de nœud mobile - flux d'appels de signalisation

La Figure 2 montre le flux d'appels de signalisation quand le nœud mobile entre dans le domaine de mandataire IPv6 mobile. Le message Sollicitation de routeur provenant du nœud mobile peut arriver à tout moment après le rattachement du nœud mobile et n'a aucune relation d'ordre stricte avec les autres messages dans le flux d'appels.

Pour mettre à jour l'ancre de mobilité locale quant à la localisation actuelle du nœud mobile, la passerelle d'accès mobile envoie un message de mise à jour de lien de mandataire à l'ancre de mobilité locale du nœud mobile. Quand elle accepte ce message de mise à jour de lien de mandataire, l'ancre de mobilité locale envoie un message Accusé de réception de lien de mandataire incluant le ou les préfixes de réseau de rattachement du nœud mobile. Elle crée aussi l'entrée d'antémémoire de liens et établit son point d'extrémité de tunnel bidirectionnel pour la passerelle d'accès mobile.

La passerelle d'accès mobile, à réception du message Accusé de réception de lien de mandataire, établit son point d'extrémité de tunnel bidirectionnel à l'ancre de mobilité locale et établit aussi la transmission pour le trafic du nœud mobile. À ce point, la passerelle d'accès mobile a toutes les informations requises pour émuler la liaison de rattachement du nœud mobile. Elle envoie des messages Annonce de routeur au nœud mobile sur la liaison d'accès pour annoncer le ou les préfixes de réseau de rattachement du nœud mobile comme préfixes hébergés en liaison.

À réception de ces messages d'annonce de routeur sur la liaison d'accès, le nœud mobile tente de configurer son interface en utilisant des modes de configuration d'adresse à états pleins ou sans état, sur la base des modes permis sur cette liaison d'accès comme indiqué dans les messages Annonce de routeur. À la fin d'une procédure réussie de configuration d'adresse, le nœud mobile a une ou plusieurs adresses provenant de son ou ses préfixes de réseau de rattachement.

Aprés la configuration d'adresse, le nœud mobile a une ou plusieurs adresses valides provenant de son ou ses préfixes de réseau de rattachement au point de rattachement actuel. La passerelle d'accès mobile desservante et l'ancre de mobilité locale ont aussi des états d'acheminement appropriés pour traiter le trafic envoyé de et vers le nœud mobile en utilisant une ou plusieurs des adresses provenant de son ou ses préfixes de réseau de rattachement.

L'ancre de mobilité locale, étant le point d'ancrage topologique pour le ou les préfixes de réseau de rattachement du nœud mobile, reçoit tous les paquets qui sont envoyés au nœud mobile par tout nœud dans ou en dehors du domaine de mandataire IPv6 mobile. L'ancre de mobilité locale transmet ces paquets reçus à la passerelle d'accès mobile à travers le tunnel bidirectionnel. La passerelle d'accès mobile à l'autre extrémité du tunnel, après avoir reçu le paquet, supprime l'en-tête externe et transmet le paquet sur la liaison d'accès au nœud mobile. Cependant, dans certains cas, le trafic envoyé d'un nœud correspondant qui est connecté localement à la passerelle d'accès mobile ne peut pas être reçu par l'ancre de mobilité locale et peut être acheminé localement par la passerelle d'accès mobile (voir le paragraphe 6.10.3).

La passerelle d'accès mobile agit comme routeur par défaut sur la liaison point à point partagée avec le nœud mobile. Tout paquet que le nœud mobile envoie à tout nœud correspondant va être reçu par la passerelle d'accès mobile et va être envoyé à son ancre de mobilité locale à travers le tunnel bidirectionnel. L'ancre de mobilité locale à l'autre extrémité du tunnel, après avoir reçu le paquet, supprime l'en-tête externe et achemine le paquet à destination. Cependant, dans certains cas, le trafic envoyé à un nœud correspondant qui est connecté localement à la passerelle d'accès mobile peut être acheminé localement par la passerelle d'accès mobile (voir le paragraphe 6.10.3).

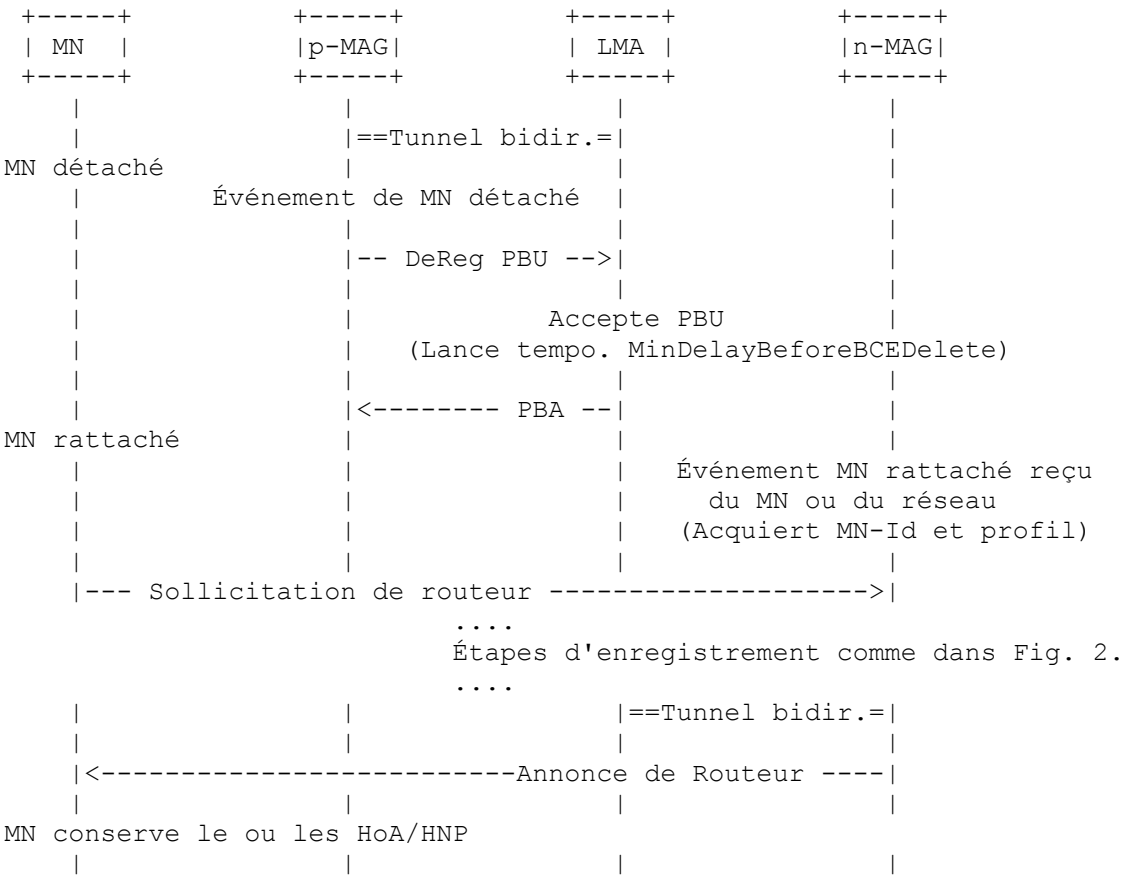


Figure 3 : Relais de nœud mobile - flux d'appels de signalisation

La Figure 3 montre le flux d'appels de signalisation pour le relais de nœud mobile de la passerelle d'accès mobile (p-MAG) précédemment rattachée à la passerelle d'accès mobile (n-MAG) nouvellement rattachée. Ce flux d'appels reflète seulement un ordre de messages spécifique ; il est possible que le message d'enregistrement provenant du n-MAG arrive avant que le message de désenregistrement de p-MAG arrive.

Après l'obtention de la configuration d'adresse initiale dans le domaine de mandataire IPv6 mobile, si le nœud mobile change son point de rattachement, la passerelle d'accès mobile sur la liaison précédente va détecter le détachement du nœud mobile de la liaison. Elle va le signaler à l'ancre de mobilité locale et va supprimer le lien et l'état d'acheminement pour ce nœud mobile. L'ancre de mobilité locale, à réception de cette demande, va identifier la session de mobilité correspondante pour qui la demande a été reçue, et accepte la demande, après quoi elle attend un certain temps pour pemettre à la passerelle d'accès mobile sur la nouvelle liaison de mettre à jour le lien. Cependant, si elle ne reçoit pas de message de mise à jour de lien de mandataire dans le délai imparti, elle va supprimer l'entrée d'antémémoire de lien.

La passerelle d'accès mobile sur la nouvelle liaison d'accès, quand elle détecte le nœud mobile sur sa liaison d'accès, va signaler à l'ancre de mobilité locale de mettre à jour l'état de lien. Après l'achèvement de la signalisation, la passerelle d'accès mobile desservante va envoyer les annonces de routeur contenant le ou les préfixes de réseau de rattachement du nœud mobile, et cela va assurer que le nœud mobile ne va détecter aucun changement par rapport au rattachement de couche 3 de son interface.

4. Sécurité du protocole de mandataire IPv6 mobile

Les messages de signalisation, Mise à jour de lien de mandataire et Accusé de réception de lien de mandataire, échangés entre la passerelle d'accès mobile et l'ancre de mobilité locale, DOIVENT être protégés en utilisant une ou des associations de sécurité de bout en bout offrant la protection de l'intégrité et l'authentification de l'origine des données.

La passerelle d'accès mobile et l'ancre de mobilité locale DOIVENT mettre en œuvre IPsec pour protéger les messages de signalisation de mandataire IPv6 mobile [RFC4301]. IPsec est un mécanisme de sécurité de mise en œuvre obligatoire. Cependant, des documents supplémentaires peuvent spécifier des mécanismes de remplacement et les entités de mobilité peuvent activer un mécanisme spécifique pour sécuriser les messages de signalisation de mandataire IPv6 mobile, sur la base d'une configuration statique ou après une négociation dynamique utilisant un protocole standard de négociation de sécurité. Comme dans IPv6 mobile [RFC3775], l'utilisation de IPsec pour protéger le trafic de données du nœud mobile est facultative.

L'encapsulation de charge utile de sécurité (ESP, *Encapsulating Security Payload*) IPsec [RFC4303] en mode transport avec protection obligatoire de l'intégrité DEVRAIT être utilisée pour protéger les messages de signalisation. La protection de la confidentialité de ces messages n'est pas exigée.

IPsec ESP [RFC4303] en mode tunnel PEUT être utilisé pour protéger le trafic de données tunnelé du nœud mobile, si la protection du trafic de données est demandée.

Le protocole d'échange de clé Internet version 2 (IKEv2, *Internet Key Exchange Protocol version 2*) [RFC4306] DEVRAIT être utilisé pour établir des associations de sécurité entre la passerelle d'accès mobile et l'ancre de mobilité locale pour protéger les messages de mise à jour de lien de mandataire et d'accusé de réception de lien de mandataire. La passerelle d'accès mobile et l'ancre de mobilité locale peuvent utiliser tout mécanisme d'authentification, comme spécifié dans la [RFC4306], pour l'authentification mutuelle.

La spécification IPv6 mobile [RFC3775] exige que l'agent de rattachement empêche un nœud mobile de créer des associations de sécurité ou de créer des entrées d'antémémoire de lien pour une adresse de rattachement d'un autre nœud mobile. Dans le protocole décrit dans ce document, le nœud mobile n'est pas impliqué dans la création d'associations de sécurité pour protéger les messages de signalisation ou dans l'envoi de mises à jour de lien. Donc, l'ancre de mobilité locale DOIT restreindre la création et la manipulation des liens de mandataire aux passerelles d'accès mobile et préfixes spécifiquement autorisés. L'ancre de mobilité locale DOIT être localement configurable pour autoriser de telles combinaisons spécifiques. Des mécanismes supplémentaires, comme un répertoire de politiques ou l'authentification, autorisation et comptabilité (AAA, *Authentication, Authorization, and Accounting*) peuvent être employés, mais cela sort du domaine d'application de la présente spécification.

À la différence de IPv6 mobile [RFC3775], ces messages de signalisation ne portent pas l'option Adresse de rattachement de destination ni l'en-tête Acheminement de type 2, et donc les entrées de politique et les sélecteurs d'association de sécurité restent les mêmes et n'exigent pas de considérations particulières relatives à IPsec.

4.1 Exemple d'entrées de la base de données d'autorisation d'homologue (PAD)

Ce paragraphe décrit les entrées de base de données d'autorisation d'homologue (PAD, *Peer Authorization Database*) [RFC4301] sur la passerelle d'accès mobile et l'ancre de mobilité locale. Les entrées de PAD sont seulement des exemples de configuration. Noter que le PAD est un concept logique et une mise en œuvre particulière de passerelle d'accès mobile ou d'ancre de mobilité locale peut mettre en œuvre le PAD d'une manière spécifique. L'état de PAD peut aussi être distribué sur diverses bases de donnnées d'une mise en œuvre spécifique.

Dans l'exemple montré ci-dessous, l'identité de l'ancre de mobilité locale est supposée être lma_identity_1 et l'identité de la passerelle d'accès mobile est supposé être mag_identity_1.

PAD de passerelle d'accès mobile :

- SI identité_distante = lma_identity_1
  Alors authentifier (secret/certificat/EAP partagé)
  et autoriser les CHILD_SA pour l'adresse distante lma_address_1

PAD d'ancre de mobilité locale :

- SI identité_distante = mag_identity_1
  Alors authentifier (secret/certificat/EAP partagé)
  et autoriser les CHILD_SA pour l'adresse distante mag_address_1

Figure 4 : Entrées de PAD

La liste des mécanismes d'authentification dans les exemples ci-dessus n'est pas exhaustive. Il pourrait y avoir d'autres accréditifs utilisés pour l'authentification mémorisés dans la PAD.

4.2 Exemple d'entrées de la base de données de politiques de sécurité (SPD)

Ce paragraphe décrit les entrées de politique de sécurité [RFC4301] sur la passerelle d'accès mobile et l'ancre de mobilité locale requises pour protéger les messages de signalisation de mandataire IPv6 mobile. Les entrées de SPD sont seulement des exemples de configurations. Une mise en œuvre particulière de passerelle d'accès mobile ou d'ancre de mobilité locale pourrait configurer des entrées de SPD différentes pour autant qu'elles fournissent la sécurité requise.

Dans l'exemple montré ci-dessous, l'identité de la passerelle d'accès mobile est supposée être mag_identity_1, l'adresse de la passerelle d'accès mobile est supposée être mag_adresse_1, et l'adresse de l'ancre de mobilité locale est supposée être lma_adresse_1. L'acronyme MH représente le numéro de protocole pour l'en-tête de mobilité (MH, *Mobility Header*) [RFC3775], tandis que les termes local_mh_type et distant_mh_type sont respectivement pour le type d'en-tête de mobilité locale et le type d'en-tête de mobilité distante.

SPD-S de passerelle d'accès mobile :

- Si adresse_locale = mag_address_1 &
  adresse_distante = lma_address_1 &
  proto = MH & (local_mh_type = BU | distant_mh_type = BA)
  Alors utiliser une SA en mode transport ESP
  Initier l'utilisation de IDi = mag_identity_1 pour l'adresse lma_address_1

SPD-S d'ancre de mobilité locale :

- Si adresse_locale = lma_adresse_1 &
  adresse_distante = mag_adresse_1 &
  proto = MH & (local_mh_type = BA | distant_mh_type = BU)
  Alors utiliser une SA en mode transport ESP

Figure 5 : Entrées de SPD

5. Fonctionnement de l'ancre de mobilité locale

L'ancre de mobilité locale DOIT prendre en charge la fonction d'agent de rattachement comme défini dans la [RFC3775] et les extensions définies dans la présente spécification. Un agent de rattachement avec ces modifications et les capacités améliorées pour la prise en charge du protocole de mandataire IPv6 mobile est appelé une ancre de mobilité locale.

Cette Section décrit les détails du fonctionnement de l'ancre de mobilité locale.

5.1 Extensions à la structure de données d'entrée d'antémémoire de liens

Chaque ancre de mobilité locale DOIT tenir une entrée d'antémémoire de liens pour chaque nœud mobile enregistré actuellement. Une entrée d'antémémoire de liens est une structure de données conceptuelle, décrite au paragraphe 9.1 de la [RFC3775].

Pour prendre en charge la présente spécification, la structure de données Entrée d'antémémoire de liens doit être étendue avec les champs supplémentaires suivants.

- Un fanion indiquant si cette entrée d'antémémoire de liens est ou non créée à cause d'un enregistrement de mandataire. Ce fanion est réglé à la valeur 1 pour les entrées d'antémémoire de liens qui sont des enregistrements de mandataire et est réglé à la valeur 0 pour toutes les autres entrées.

- l'identifiant du nœud mobile enregistré, MN-Identifiant. Cet identifiant est obtenu de l'option Identifiant de nœud mobile [RFC4283] présente dans le message Mise à jour de lien de mandataire reçu.

- L'identifiant de couche de liaison de l'interface connectée du nœud mobile sur la liaison d'accès. Cet identifiant peut être acquis de l'option Identifiant de couche de liaison de nœud mobile, présente dans le message Mise à jour de lien de mandataire reçu. Si l'option n'est pas présente dans la demande, ce champ de longueur variable DOIT être réglé à deux (octets) et DOIT être initialisé à une valeur de TOUT_ZÉRO.

- L'adresse de liaison locale de la passerelle d'accès mobile sur la liaison point à point partagé avec le nœud mobile. Elle est générée par l'ancre de mobilité locale après l'acceptation du message initial Mise à jour de lien de mandataire.

- Une liste des préfixes de réseau de rattachement IPv6 alloués à l'interface connectée du nœud mobile. Le ou les préfixes de réseau de rattachement peuvent avoir été configurés statiquement dans le profil de politique du nœud mobile, ou ils peuvent avoir été alloués de façon dynamique par l'ancre de mobilité locale. Chacune de ces entrées de préfixe va aussi inclure la longueur de préfixe correspondante.

- L'identifiant d'interface de tunnel (tunnel-si-id) du tunnel bidirectionnel entre l'ancre de mobilité locale et la passerelle d'accès mobile où le nœud mobile est actuellement ancré. Ceci est interne à l'ancre de mobilité locale. L'identifiant d'interface de tunnel est acquis durant la création du tunnel.

- Le type de technologie d'accès, par laquelle le nœud mobile est actuellement rattaché. Ceci est obtenu de l'option Type de technologie d'accès, présente dans le message Mise à jour de lien de mandataire.

- La valeur d'horodatage de 64 bits du plus récent message accepté de mise à jour de lien de mandataire envoyé pour ce nœud mobile. C'est l'heure, à l'ancre de mobilité locale, où le message a été reçu. Si l'option Horodatage n'est pas présente dans le message Mise à jour de lien de mandataire (c'est-à-dire, quand le schéma fondé sur le numéro de séquence est utilisé) la valeur DOIT être réglée à TOUT_ZÉRO.

Normalement, tout préfixe de réseau de rattachement du nœud mobile provenant de sa session de mobilité peut être utilisé comme clé pour localiser son entrée d'antémémoire de liens dans tous les cas sauf quand il y a eu un relais de la session du nœud mobile à une nouvelle passerelle d'accès mobile, et que la passerelle d'accès mobile n'est pas informée du ou des préfixes de réseau de rattachement alloués à cette session de mobilité. Dans ces cas de relais, l'entrée d'antémémoire de liens peut être localisée sous les considérations spécifiées au paragraphe 5.4.1.

5.2 Modèles de préfixes de réseau de rattachement pris en charge

La présente spécification prend en charge le modèle de préfixe par nœud mobile et ne prend pas en charge le modèle de préfixe partagé. Selon le modèle de préfixe par nœud mobile, le ou les préfixes de réseau de rattachement alloués à un nœud mobile sont pour l'usage exclusif de ce nœud mobile et aucun autre nœud ne partage une adresse provenant de ce

préfixe (autres que l'adresse d'envoi à la cantonade de routeur de sous réseau [RFC4291] utilisée par la passerelle d'accès mobile qui héberge ce préfixe sur cette liaison).

Il peut y avoir plus d'un préfixe alloué à une certaine interface du nœud mobile ; tous ces préfixes alloués DOIVENT être uniques sur ce nœud mobile, et tous font partie d'exactement une session de mobilité. Si le nœud mobile se rattache simultanément au domaine de mandataire IPv6 mobile par plusieurs interfaces, chacune des interfaces rattachée DOIT avoir alloués un ou plusieurs préfixes uniques. Les préfixes qui ne sont pas alloués à la même interface NE DOIVENT PAS être gérés sous la même session de mobilité.

Le ou les préfixes de réseau de rattachement du nœud mobile alloués à une certaine interface d'un nœud mobile (partie d'une session de mobilité) vont être hébergés sur la liaison d'accès où le nœud mobile est rattaché (en utilisant cette interface). L'ancre de mobilité locale n'est pas obligée d'effectuer d'opération de découverte de voisin (ND, *Neighbor Discovery*) mandataire [RFC4861] pour défendre la ou les adresses de rattachement du nœud mobile, car les préfixes ne sont pas hébergés localement sur l'ancre de mobilité locale. Cependant, du point de vue de l'acheminement, le ou les préfixes de réseau de rattachement sont topologiquement ancrés sur l'ancre de mobilité locale.

5.3 Considérations de signalisation

Ce paragraphe donne les règles de traitement des messages de signalisation. Les règles de traitement spécifiées dans ce paragraphe et les autres paragraphes en relation s'enchaînent dans un ordre spécifique. Quand on applique ces considérations au traitement des messages de signalisation, l'ordre spécifié DOIT être conservé.

5.3.1 Traitement des mises à jour de lien de mandataire

1. Le message de mise à jour de lien de mandataire reçu (un message Mise à jour de lien avec le fanion (P) réglé à la valeur de 1, format spécifié au paragraphe 8.1) DOIT être authentifié comme décrit à la Section 4. Quand IPsec est utilisé pour l'authentification de message, l'indice de paramètre de sécurité (SPI, *Security Parameter Index*) dans l'en-tête IPsec [RFC4306] du paquet reçu est nécessaire pour la localisation de l'association de sécurité, pour authentifier le message de mise à jour de lien de mandataire.

2. L'ancre de mobilité locale DOIT respecter les règles décrites au paragraphe 9.2 de la [RFC3775] lors du traitement de l'en-tête de mobilité dans le message Mise à jour de lien de mandataire reçu.

3. L'ancre de mobilité locale DOIT ignorer la vérification, spécifiée au paragraphe 10.3.1 de la [RFC3775], relative à la présence de l'option Adresse de rattachement de destination dans le message Mise à jour de lien de mandataire.

4. L'ancre de mobilité locale DOIT identifier le nœud mobile à partir de l'identifiant présent dans l'option Identifiant de nœud mobile [RFC4283] du message Mise à jour de lien de mandataire. Si l'option Identifiant de nœud mobile n'est pas présente dans le message Mise à jour de lien de mandataire, l'ancre de mobilité locale DOIT rejeter la demande et envoyer un message Accusé de réception de lien de mandataire avec le champ État réglé à MISSING_MN_IDENTIFIER_OPTION *(option Identifiant de nœud mobile manquante)* et l'identifiant dans l'option Identifiant de nœud mobile portée dans le message DOIT être réglée à un identifiant de longueur zéro.

5. L'ancre de mobilité locale DOIT appliquer les vérifications de politique requises, comme expliqué à la Section 4, pour vérifier que l'envoyeur est une passerelle d'accès mobile de confiance autorisée à envoyer des messages de mise à jour de lien de mandataire au nom de ce nœud mobile.

6. Si l'ancre de mobilité locale détermine que le nœud demandeur n'est pas autorisé à envoyer de message de mise à jour de lien de mandataire pour le nœud mobile identifié, elle DOIT rejeter la demande et envoyer un message Accusé de réception de lien de mandataire avec le champ État réglé à MAG_NOT_AUTHORIZED_FOR_PROXY_REG *(non autorisé à envoyer des mises à jour de lien de mandataire)*.

7. Si l'ancre de mobilité locale ne peut pas identifier le nœud mobile sur la base de l'identifiant présent dans l'option Identifiant de nœud mobile [RFC4283] du message Mise à jour de lien de mandataire, elle DOIT rejeter la demande et envoyer un message Accusé de réception de lien de mandataire avec le champ État réglé à NOT_LMA_FOR_THIS_MOBILE_NODE *(n'est pas ancre de mobilité locale pour ce nœud mobile)*.

8. Si l'ancre de mobilité locale détermine que le nœud mobile n'est pas autorisé pour le service de gestion de mobilité fondée sur le réseau, elle DOIT rejeter la demande et envoyer un message Accusé de réception de lien de mandataire avec le champ État réglé à PROXY_REG_NOT_ENABLED *(enregistrement de mandataire non activé)*.

9. L'ancre de mobilité locale DOIT appliquer les considérations spécifiées au paragraphe 5.5 pour traiter le champ Numéro de séquence et l'option Horodatage (si elle est présente) dans le message Mise à jour de lien de mandataire.

10. Si il n'y a pas d'option Préfixe de réseau de rattachement présente dans le message Mise à jour de lien de mandataire, l'ancre de mobilité locale DOIT rejeter la demande et envoyer un message Accusé de réception de lien de mandataire avec le champ État réglé à MISSING_HOME_NETWORK_PREFIX_OPTION *(option Préfixe de réseau de rattachement manquante)*.

11. Si l'option Indicateur de relais n'est pas présente dans le message Mise à jour de lien de mandataire, l'ancre de mobilité locale DOIT rejeter la demande et envoyer un message Accusé de réception de lien de mandataire avec le champ État réglé à MISSING_HANDOFF_INDICATOR_OPTION *(option Indicateur de relais manquante)*.

12. Si l'option Type de technologie d'accès n'est pas présente dans le message Mise à jour de lien de mandataire, l'ancre de mobilité locale DOIT rejeter la demande et envoyer un message Accusé de réception de lien de mandataire avec le champ État réglé à MISSING_ACCESS_TECH_TYPE_OPTION *(option Type de technologie d'accès manquante)*.

13. Les considérations spécifiées au paragraphe 5.4.1 DOIVENT être appliquées pour effectuer l'essai d'existence de l'entrée d'antémémoire de liens. Si les vérifications spécifiées au paragraphe 5.4.1 résultent en l'association du message Mise à jour de lien de mandataire reçu à une nouvelle demande de création de session de mobilité, les considérations du paragraphe 5.3.2 (Enregistrement de lien initial - nouvelle session de mobilité) DOIVENT être appliquées. Si ces vérifications résultent en l'association de la demande à une session de mobilité existante, les vérifications suivantes déterminent le prochain ensemble de règles de traitement qui doivent être appliquées.
    * Si le message Mise à jour de lien de mandataire reçu a la valeur de durée de vie de zéro, les considérations du paragraphe 5.3.5 (Désenregistrement de lien) DOIVENT être appliquées.
    * Si la Proxy-CoA dans l'entrée d'antémémoire de liens correspond à l'adresse de source de la demande (ou à l'adresse dans l'option Autre adresse d'entretien, si l'option est présente) les considérations du paragraphe 5.3.3 (Extension de durée de vie de lien - pas de relais) DOIVENT être appliquées.
    * Pour tous les autres cas, les considérations du paragraphe 5.3.4 (Extension de durée de vie de lien - après relais) DOIVENT être appliquées.

14. Lors de l'envoi du message Accusé de réception de lien de mandataire avec toute valeur du champ État, le message DOIT être construit comme spécifié au paragraphe 5.3.6.

5.3.2 Enregistrement de lien initial (nouvelle session de mobilité)

1. Si il y a au moins une instance de l'option Préfixe de réseau de rattachement présente dans le message de mise à jour de lien de mandataire avec la valeur de préfixe réglée à TOUT_ZÉRO, l'ancre de mobilité locale DOIT allouer un ou plusieurs préfixes de réseau de rattachement au nœud mobile et les allouer à la nouvelle session de mobilité créée pour le nœud mobile. L'ancre de mobilité locale DOIT s'assurer que le ou les préfixes alloués ne sont pas utilisés par un autre nœud ou session de mobilité. La décision de combien de préfixes sont alloués pour l'interface rattachée peut se fonder sur une politique globale ou sur une politique spécifique de ce nœud mobile. Cependant, quand l'autoconfiguration d'adresse à états pleins utilisant DHCP est prise en charge sur la liaison, les considérations du paragraphe 6.11 DOIVENT être appliquées pour l'allocation de préfixe.

2. Si l'ancre de mobilité locale n'est pas capable d'allouer de préfixe de réseau de rattachement au nœud mobile, elle DOIT rejeter la demande et envoyer un message Accusé de réception de lien de mandataire avec le champ État réglé à 130 (ressources insuffisantes).

3. Si il y a une ou plusieurs options Préfixe de réseau de rattachement présentes dans le message de mise à jour de lien de mandataire (avec chaque préfixe réglé à une valeur NON_ZÉRO) l'ancre de mobilité locale, avant d'accepter cette demande, DOIT s'assurer que chaque préfixe est possédé par l'ancre de mobilité locale, et de plus que le nœud mobile est autorisé à utiliser ces préfixes. Si le nœud mobile n'est pas autorisé à utiliser un ou plusieurs de ces préfixes, l'ancre de mobilité locale DOIT rejeter la demande et envoyer un message Accusé de réception de lien de mandataire avec le champ État réglé à NOT_AUTHORIZED_FOR_HOME_NETWORK_PREFIX *(nœud mobile non autorisé pour un ou plusieurs des préfixes de réseau de rattachement demandés)*.

4. Lorsque elle accepte la demande, l'ancre de mobilité locale DOIT créer une entrée d'antémémoire de liens pour le nœud mobile. Elle doit régler les champs dans l'entrée d'antémémoire de liens aux valeurs acceptées pour cet enregistrement.

5. Si il n'existe pas de tunnel bidirectionnel pour la passerelle d'accès mobile qui a envoyé la demande, l'ancre de mobilité locale DOIT établir un tunnel bidirectionnel à cette passerelle d'accès mobile. Les considérations du paragrahe 5.6.1 DOIVENT être appliquées pour gérer le tunnel bidirectionnel créé dynamiquement.

6. L'ancre de mobilité locale DOIT créer un ou des chemins de préfixe sur le tunnel à la passerelle d'accès mobile pour transmettre tout trafic reçu pour le ou les préfixes de réseau de rattachement du nœud mobile associés à cette session de mobilité. Le tunnel créé et l'état d'acheminement DOIVENT résulter en le comportement de tranmission sur l'ancre de mobilité locale spécifié au paragraphe 5.6.2.

7. L'ancre de mobilité locale DOIT envoyer le message Accusé de réception de lien de mandataire avec le champ État réglé à 0 (mise à jour de lien de mandataire acceptée). Le message DOIT être construit comme spécifié au paragraphe 5.3.6.

5.3.3 Extension de durée de vie de lien (pas de relais)

1. Lorsque elle accepte le message de mise à jour de lien de mandataire pour étendre la durée de vie du lien, reçu de la même passerelle d'accès mobile (si la Proxy-CoA dans l'entrée d'antémémoire de liens est la même que la Proxy-CoA dans la demande) que la dernière mise à jour le lien, l'ancre de mobilité locale DOIT mettre à jour l'entrée d'antémémoire de liens avec les valeurs d'enregistrement acceptées.

2. L'ancre de mobilité locale DOIT envoyer le message Accusé de réception de lien de mandataire avec le champ État réglé à 0 (mise à jour de lien de mandataire acceptée). Le message DOIT être construit comme spécifié au paragraphe 5.3.6.

5.3.4. Extension de durée de vie de lien (après relais)

1. Lorsque elle accepte le message de mise à jour de lien de mandataire pour étendre la durée de vie du lien, reçu d'une nouvelle passerelle d'accès mobile (si la Proxy-CoA dans l'entrée d'antémémoire de liens ne correspond pas à la Proxy-CoA dans la demande) où la session de mobilité du nœud mobile est relayée, l'ancre de mobilité locale DOIT mettre à jour l'entrée d'antémémoire de liens avec les valeurs d'enregistrement acceptées.

2. L'ancre de mobilité locale DOIT supprimer le ou les chemins créés précédemment pour le ou les préfixes de réseau de rattachement du nœud mobile associés à cette session de mobilité. De plus, si il n'y a pas d'autre nœud mobile qui partage le tunnel bidirectionnel créé dynamiquement avec la précédente passerelle d'accès mobile, le tunnel DEVRAIT être supprimé, en appliquant les considérations du paragraphe 5.6.1 (si le tunnel a été créé dynamiquement et n'est pas un tunnel fixe pré-établi).

3. Si il n'existe pas de tunnel bidirectionnel pour la passerelle d'accès mobile qui a envoyé la demande, l'ancre de mobilité locale DOIT établir un tunnel bidirectionnel à cette passerelle d'accès mobile. Les considerations du paragraphe 5.6.1 DOIVENT être appliquées pour gérer le tunnel bidirectionnel créé dynamiquement.

4. L'ancre de mobilité locale DOIT créer un ou des chemins de préfixe sur le tunnel à la passerelle d'accès mobile pour transmettre tout trafic reçu pour le ou les préfixes de réseau de rattachement du nœud mobile associés à cette session de mobilité. Le tunnel et l'état d'acheminement créés DOIVENT résulter en le comportement de transmission sur l'ancre de mobilité locale spécifié au paragraphe 5.6.2.

5. L'ancre de mobilité locale DOIT envoyer le message Accusé de réception de lien de mandataire avec le champ État réglé à 0 (mise à jour de lien de mandataire acceptée). Le message DOIT être construit comme spécifié au paragraphe 5.3.6.

5.3.5 Désenregistrement de lien

1. Si le message Mise à jour de lien de mandataire reçu avec la valeur de durée de vie de zéro, a une adresse de source dans l'en-tête IPv6 (ou l'adresse dans l'option Autre adresse d'entretien, si l'option est présente) différente de ce qui est présent dans le champ Adresse d'entretien de mandataire dans l'entrée d'antémémoire de liens, l'ancre de mobilité locale DOIT ignorer la demande.

2. Lorsque elle accepte le message de mise à jour de lien de mandataire, avec la valeur de durée de vie de zéro, l'ancre de mobilité locale DOIT attendre pendant MinDelayBeforeBCEDelete *(délai minimum avant suppression d'entrée d'antémémoire de lien)* avant de supprimer l'entrée d'antémémoire de liens (BCE, *Binding Cache Entry*). Cependant,

elle DOIT envoyer le message Accusé de réception de lien de mandataire avec le champ État réglé à 0 (mise à jour de lien de mandataire acceptée). Le message DOIT être construit comme spécifié au paragraphe 5.3.6.

* Durant cette période d'attente, l'ancre de mobilité locale DEVRAIT éliminer le trafic de données du nœud mobile.
* Durant cette période d'attente, si l'ancre de mobilité locale reçoit un message valide de mise à jour de lien de mandataire pour la même session de mobilité avec la valeur de durée de vie supérieure à zero, et si cette demande est acceptée, alors l'entrée d'antémémoire de liens NE DOIT PAS être supprimée, mais doit être mise à jour avec les valeurs d'enregistrement qui viennent d'être acceptées, et la période d'attente devrait être terminée.
* À la fin de cette période d'attente, si l'ancre de mobilité locale n'a pas reçu de message de mise à jour de lien de mandataire valide pour cette session de mobilité, elle DOIT alors supprimer l'entrée d'antémémoire de liens et supprimer l'état d'acheminement créé pour cette session de mobilité. L'ancre de mobilité locale peut éventuellement réallouer le ou les préfixes associés à cette session de mobilité aux autres nœuds mobiles.

5.3.6 Construction du message d'accusé de réception de lien de mandataire

o L'ancre de mobilité locale, quand elle envoie le message Accusé de réception de lien de mandataire à la passerelle d'accès mobile, DOIT construire le message comme spécifié ci-dessous :

```
En-tête IPv6 (src=LMAA, dst=Proxy-CoA)
  En-tête de mobilité
      - BA                                  /* Le fanion P doit être réglé à la valeur 1 */
    Options de mobilité
      - option Identifiant de nœud mobile                          (obligatoire)
      - option Préfixe de réseau de rattachement                   (obligatoire)
      - option Indicateur de relais                                (obligatoire)
      - option Type de technologie d'accès                         (obligatoire)
      - option Horodatage                                          (facultatif)
      - option Identifiant de couche de liaison de nœud mobile     (facultatif)
      - option Adresse de liaison locale                           (facultatif)
```

Figure 6 : Format du message d'accusé de réception de lien de mandataire

o Le champ Adresse de source dans l'en-tête IPv6 du message DOIT être réglé à l'adresse de destination du message de mise à jour de lien de mandataire reçu.

o Le champ Adresse de destination dans l'en-tête IPv6 du message DOIT être réglé à l'adresse de source du message de mise à jour de lien de mandataire reçu. Quand il n'y a pas d'option Autre adresse d'entretien présente dans la demande, l'adresse de destination est la même que Proxy-CoA ; autrement, l'adresse peut n'être pas la même que Proxy-CoA.

o L'option Identifiant de nœud mobile [RFC4283] DOIT être présente. Le champ Identifiant dans l'option DOIT être copié de l'option Identifiant de nœud mobile dans le message Mise à jour de lien de mandataire reçu. Si l'option n'était pas présente dans la demande, l'identifiant dans l'option DOIT être réglé à un identifiant de longueur zéro.

o Au moins une option Préfixe de réseau de rattachement DOIT être présente.
  * Si le champ État est réglé à une valeur supérieure ou égale à 128, c'est-à-dire, si la mise à jour de lien de mandataire est rejetée, toutes les options Préfixe de réseau de rattachement qui étaient présentes dans la demande (avec leurs valeurs de préfixe) DOIVENT être présentes dans la réponse. Mais, si il n'y avait pas d'option Préfixe de réseau de rattachement présente dans la demande, il DOIT alors y avoir seulement une option Préfixe de réseau de rattachement avec la valeur de l'option réglée à TOUT_ZÉRO.
  * Pour tous les autres cas, il DOIT y avoir une option Préfixe de réseau de rattachement pour chaque préfixe de réseau de rattachement alloué (pour cette session de mobilité) et avec la valeur de préfixe dans l'option réglée à la valeur de préfixe allouée.

o L'option Indicateur de relais DOIT être présente. Le champ Indicateur de relais dans l'option DOIT être copié de l'option Indicateur de relais dans le message de mise à jour de lien de mandataire rmçu. Si l'option n'était pas présente dans la demande, la valeur dans l'option DOIT être réglée à zéro.

o L'option Type de technologie d'accès DOIT être présente. Le champ Type de technologie d'accès dans l'option DOIT être copié de l'option Type de technologie d'accès dans le message de mise à jour de lien de mandataire reçu. Si l'option n'était pas présente dans la demande, la valeur dans l'option DOIT être réglée à zéro.

- L'option Horodatage DOIT être présente seulement si la même option était présente dans le message de mise à jour de lien de mandataire reçu et NE DOIT PAS être présente autrement. Les considérations du paragraphe 5.5 doivent être appliquées pour construire l'option Horodatage.

- L'option Identifiant de couche de liaison de nœud mobile DOIT être présente seulement si la même option était présente dans le message de mise à jour de lien de mandataire reçu et NE DOIT PAS être présente autrement. La valeur de l'identifiant de couche de liaison DOIT être copiée de l'option Identifiant de couche de liaison de nœud mobile présente dans le message de mise à jour de lien de mandataire reçu.

- L'option Adresse de liaison locale DOIT être présente seulement si la même option était présente dans le message de mise à jour de lien de mandataire reçu et NE DOIT PAS être présente autrement. Si le champ État dans la réponse est réglé à une valeur supérieure ou égale à 128, c'est-à-dire, si la mise à jour de lien de mandataire est rejetée, alors l'adresse de liaison locale provenant de la demande DOIT être copiée dans l'option Adresse de liaison locale de la réponse, autrement, les considérations suivantes s'appliquent :
  * Si le message de mise à jour de lien de mandataire reçu a l'option Adresse de liaison locale avec la valeur de TOUT_ZÉRO et si il existe une entrée d'antémémoire de liens associée à cette demande, alors l'adresse de liaison locale provenant de l'entrée d'antémémoire de liens DOIT être copiée dans l'option Adresse de liaison locale dans la réponse.
  * Si le message de mise à jour de lien de mandataire reçu a l'option Adresse de liaison locale avec la valeur de TOUT_ZÉRO et si il n'existe pas d'entrée d'antémémoire de liens associée à cette demande, alors l'ancre de mobilité locale DOIT générer l'adresse de liaison locale que la passerelle d'accès mobile peut utiliser sur la liaison point à point partagée avec le nœud mobile. Cette adresse générée DOIT être copiée dans l'option Adresse de liaison locale de la réponse. La même adresse DOIT aussi être copiée dans le champ Adresse de liaison locale de l'entrée d'antémémoire de liens créée pour cette session de mobilité.
  * Si le message de mise à jour de lien de mandataire reçu a l'option Adresse de liaison locale avec une valeur NON_ZÉRO, alors l'adresse de liaison locale provenant de la demande DOIT être copiée dans l'option Adresse de liaison locale de la réponse. La même adresse DOIT aussi être copiée dans le champ Adresse de liaison locale de l'entrée d'antémémoire de liens associée à cette demande (après la création de l'entrée d'antémémoire de liens, si il n'en existe pas déjà une).

- Si IPsec est utilisé pour protéger les messages de signalisation, le message DOIT être protégé en utilisant l'association de sécurité existante entre l'ancre de mobilité locale et la passerelle d'accès mobile.

- À la différence de IPv6 mobile [RFC3775], l'en-tête d'acheminement de type 2 NE DOIT PAS être présent dans l'en-tête IPv6 du paquet.

5.4 Prise en charge du multi rattachement

La présente spécification permet aux nœuds mobiles de se connecter à un domaine de mandataire IPv6 mobile à travers plusieurs interfaces pour un accès simultané. Les aspects clés de la prise en charge du multi-rattachements sont :

- Quand un nœud mobile se connecte à un domaine de mandataire IPv6 mobile à travers plusieurs interfaces pour un accès simultané, l'ancre de mobilité locale DOIT allouer une session de mobilité pour chaque interface rattachée. Chaque session de mobilité devrait être gérée sous une entrée d'antémémoire de liens séparée et avec sa propre durée de vie.

- L'ancre de mobilité locale PEUT allouer plus d'un préfixe de réseau de rattachement pour une certaine interface du nœud mobile. Cependant, tous les préfixes associés à une certaine interface DOIVENT être gérés au titre d'une session de mobilité, associée à cette interface.

- L'ancre de mobilité locale DOIT permettre un relais entre deux différentes interfaces d'un nœud mobile. Dans ce scénario, tous les préfixes de réseau de rattachement associés à une interface (faisant partie d'une session de mobilité) vont être associés à une interface différente du nœud mobile. La décision de quand créer une nouvelle session de mobilité et quand mettre à jour une session de mobilité existante DOIT être fondée sur le conseil de transfert présent dans le message de mise à jour de lien de mandataire et les considérations specifiées dans ce paragraphe.

5.4.1 Considérations sur la recherche d'entrée d'antémémoire de lien

Il peut y avoir plusieurs entrées d'antémémoire de liens pour un certain nœud mobile. Quand on fait une recherche d'entrée d'antémémoire de liens pour un nœud mobile pour traiter un message reçu de mise à jour de lien de mandataire, l'ancre de

mobilité locale DOIT appliquer les considérations de multi rattachements suivantes (dans l'ordre spécifié ci-dessous, en commençant par le paragraphe 5.4.1.1). Ces règles sont couplées avec les règles de traitement spécifiées au paragraphe 5.3.

5.4.1.1 Option Préfixe de réseau de rattachement (valeur NON ZÉRO) présente dans la demande

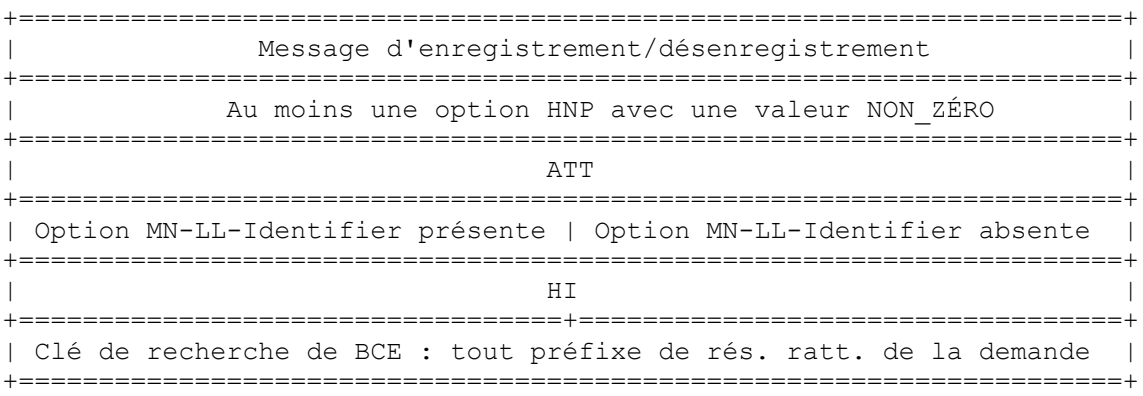


Figure 7 : Recherche d'entrée d'antémémoire de liens (BCE) en utilisant un préfixe de réseau de rattachement

Si il y a au moins une option Préfixe de réseau de rattachement présente dans la demande avec une valeur de préfixe NON_ZÉRO et sans considération de la présence de l'option Identifiant de couche de liaison de nœud mobile dans la demande, les considérations suivantes DOIVENT être appliquées. Si il y a plus d'une instance de l'option Préfixe de réseau de rattachement, toute option Préfixe de réseau de rattachement présente dans la demande (avec une valeur de préfixe NON_ZÉRO) peut être utilisée pour localiser l'entrée d'antémémoire de liens.

1. L'ancre de mobilité locale DOIT vérifier si il existe une entrée d'antémémoire de liens avec un de ses préfixes de réseau de rattachement qui correspond à la valeur de préfixe d'une des options Préfixe de réseau de rattachement du message reçu de mise à jour de lien de mandataire.

2. Si il n'existe pas d'entrée d'antémémoire de liens (avec un de ses préfixes de réseau de rattachement dans l'entrée d'antémémoire de liens correspondant à la valeur de préfixe dans une des options Préfixe de réseau de rattachement du message de mise à jour de lien de mandataire reçu) la demande DOIT être considérée comme une demande de création d'une nouvelle session de mobilité.

3. Si il existe une entrée d'antémémoire de liens (avec un de ses préfixes de réseau de rattachement dans l'entrée d'antémémoire de liens correspondant à la valeur de préfixe dans une des options Préfixe de réseau de rattachement du message Mise à jour de lien de mandataire reçu) mais si l'identifant de nœud mobile dans l'entrée ne correspond pas à l'identifiant de nœud mobile dans l'option Identifiant de nœud mobile du message Mise à jour de lien de mandataire reçu, l'ancre de mobilité locale DOIT rejeter la demande avec la valeur de champ État réglée à NOT_AUTHORIZED_FOR_HOME_NETWORK_PREFIX *(nœud mobile non autorisé pour un ou plusieurs des préfixes de réseau de rattachement demandés)*.

4. Si il existe une entrée d'antémémoire de liens (identifiant de nœud mobile corrrespondant et un de ses préfixes de réseau de rattachement dans l'entrée d'antémémoire de liens correspondant à la valeur de préfixe dans une des options Préfixe de réseau de rattachement du message Mise à jour de lien de mandataire reçu) mais si tous les prefixes dans la demande ne correspondent pas à tous les préfixes dans l'entrée d'antémémoire de liens, ou si leur nombre ne correspond pas, alors l'ancre de mobilité locale DOIT rejeter la demande avec la valeur du champ État réglée à BCE_PBU_PREFIX_SET_DO_NOT_MATCH *(tous les préfixes de réseau de rattachement mentonnés dans la BCE ne correspondent pas à tous les préfixes de la PBU reçue)*.

5. Si il existe une entrée d'antémémoire de liens (identifiant de nœud mobile corrrespondant et tous les préfixes de réseau de rattachement dans l'entrée d'antémémoire de liens correspondants à tous les préfixes de réseau de rattachement dans le message de mise à jour de lien de mandataire reçu) et si une ou plusieurs des conditions déclarées ci-dessous sont vraies, la demande DOIT être considérée comme une demande de mise à jour de cette entrée d'antémémoire de liens.
   * Si une option Identifiant de couche de liaison de nœud mobile est présente dans la demande et si l'identifiant de couche de liaison dans l'option correspond à l'identifiant de couche de liaison de l'entrée d'antémémoire de liens et si le type de technologie d'accès dans l'option Type de technologie d'accès présente dans la demande correspond au type de technologie d'accès dans l'entrée d'antémémoire de liens.
   * Si le champ Indicateur de relais dans l'option Indicateur de relais présente dans la demande est réglé à la valeur 2 (relais entre deux interfaces différentes du nœud mobile).

* Si il n'y a pas d'option Identifiant de couche de liaison de nœud mobile présente dans la demande, la valeur d'identifiant de couche de liaison dans l'entrée d'antémémoire de liens est réglée à TOUT_ZÉRO, le champ Type de technologie d'accès dans l'option Type de technologie d'accès présente dans la demande correspond au type de technologie d'accès dans l'entrée d'antémémoire de liens, et si le champ Indicateur de relais dans l'option Indicateur de relais présente dans la demande est réglé à la valeur de 3 (relais entre passerelles d'accès mobile pour la même interface).
* Si la Proxy-CoA dans l'entrée d'antémémoire de liens correspond à l'adresse de source de la demande (ou à l'adresse dans l'option Autre adresse d'entretien, si l'option est présente) et si le champ Type de technologie d'accès dans l'option Type de technologie d'accès présente dans la demande correspond au type de technologie dans l'entrée d'antémémoire de liens.

6. Pour tous les autres cas, le message DOIT être considéré comme une demande de création d'une nouvelle session de mobilité. Cependant, si le message reçu de mise à jour de lien de mandataire a la valeur de durée de vie de zéro et si la demande ne peut pas être associée à une session de mobilité existante, le message DOIT être ignoré en silence.

5.4.1.2 Option Identifiant de couche de liaison de nœud mobile présente dans la demande

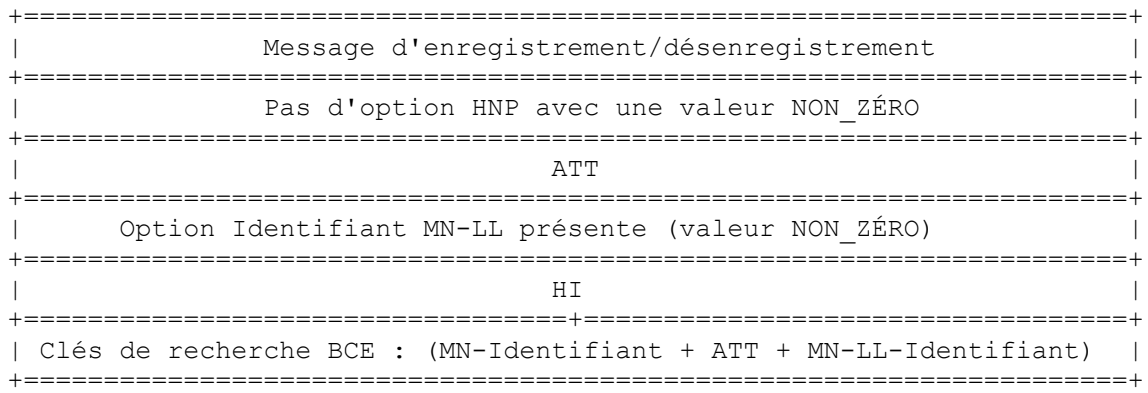


Figure 8 : Recherche de BCE en utilisant un identifiant de couche de liaison

Si il n'y a pas d'option Préfixe de réseau de rattachement présente dans la demande avec une valeur de préfixe NON_ZERO, mais si il y a une option Identifiant de couche de liaison de nœud mobile présente dans la demande, alors les considérations suivantes DOIVENT être appliquées pour localiser l'entrée d'antémémoire de liens.

1. L'ancre de mobilité locale DOIT vérifier si il existe une entrée d'antémémoire de liens, avec l'identifiant de nœud mobile correspondant à l'identifiant de l'option Identifiant de nœud mobile reçue, le type de technologie d'accès correspondant à la valeur de l'option Type de technologie d'accès reçue, et la valeur d'identifiant de couche de liaison correspondant à l'identifiant dans l'option Identifiant de couche de liaison de nœud mobile reçue.

2. Si il existe une entrée d'antémémoire de liens (correspondant à MN-Identifiant, type de technologie d'accès (ATT, *Access Technology Type*), et MN-LL-Identifiant) la demande DOIT être considérée comme une demande de mise à jour de cette entrée d'antémémoire de liens.

3. Si il n'existe pas d'entrée d'antémémoire de liens (correspondant à MN-Identifiant, ATT, et MN-LL-Identifiant) et si le champ Indicateur de relais dans l'option Indicateur de relais présente dans la demande est réglé à une valeur de 2 (relais entre deux interfaces différentes du nœud mobile). L'ancre de mobilité locale DOIT appliquer les considérations supplémentaires suivantes :
   * L'ancre de mobilité locale DOIT vérifier si il existe une et seulement une entrée d'antémémoire de liens avec l'identifiant de nœud mobile correspondant à l'identifiant de l'option Identifiant de nœud mobile présente dans la demande et pour toute valeur d'identifiant de couche de liaison. Si il existe seulement une telle entrée (correspondant à l'identifiant de nœud mobile) la demande DOIT être considérée comme une demande de mise à jour de cette entrée d'antémémoire de liens.

4. Si il n'existe pas d'entrée d'antémémoire de liens (correspondant à MN-Identifiant, ATT, et MN-LL-Identifiant) et si le champ Indicateur de relais dans l'option Indicateur de relais présente dans la demande est réglé à une valeur de 4 (État de relais inconu) l'ancre de mobilité locale DOIT appliquer les considérations supplémentaires suivantes.
   * L'ancre de mobilité locale DOIT vérifier si il existe une et seulement une entrée d'antémémoire de liens avec l'identifiant de nœud mobile correspondant à l'identifiant dans l'option Identifiant de nœud mobile présente dans la demande et pour toute valeur d'identifiant de couche de liaison. Si il existe seulement une telle entrée (correspondant

à l'identifiant de nœud mobile) l'ancre de mobilité locale DEVRAIT attentre jusqu'à ce que l'entrée d'antémémoire de liens existante soit désenregistrée par la passerelle d'accès mobile desservante précédente, avant que la demande puisse être considérée comme une demande de mise à jour de cette entrée d'antémémoire de liens. Cependant, si il n'y a pas de message de désenregistrement reçu dans le délai MaxDelayBeforeNewBCEAssign, l'ancre de mobilité locale, quand elle accepte la demande, DOIT considérer la demande comme une demande de création d'une nouvelle session de mobilité. L'ancre de mobilité locale PEUT aussi choisir de créer une nouvelle session de mobilité sans attendre un message de désenregistrement, et cela devrait être configurable sur l'ancre de mobilité locale.

5. Pour tous les autres cas, le message DOIT être considéré comme une demande de création d'une nouvelle session de mobilité. Cependant, si le message de mise à jour de lien de mandataire reçu a la valeur de durée de vie de zéro et si la demande ne peut pas être associée à une session de mobilité existante, le message DOIT être ignoré en silence.

5.4.1.3 Option Identifiant de couche de liaison de nœud mobile non présente dans la demande

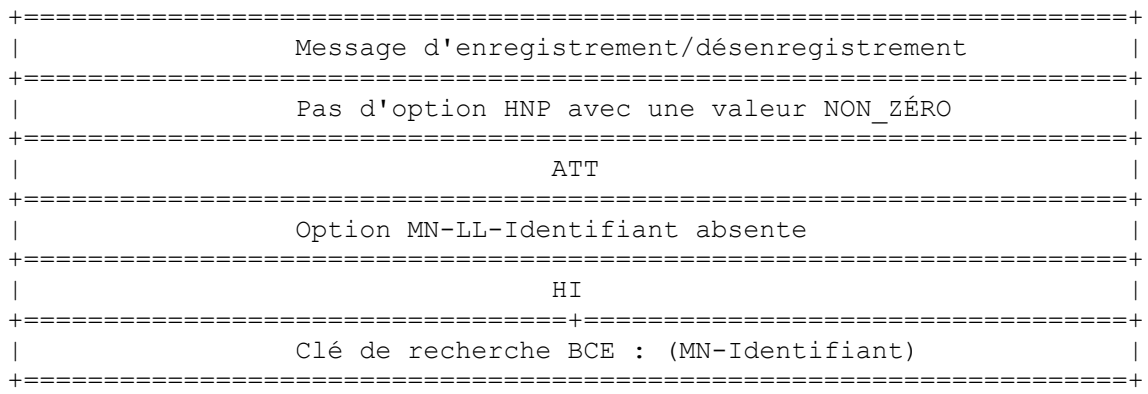


Figure 9 : Recherche de BCE utilisant un identifiant de nœud mobile

Si il n'y a pas d'option Préfixe de réseau de rattachement présente dans la demande avec une valeur de préfixe NON_ZÉRO et si il n'y a pas non plus d'option Identifiant de couche de liaison de nœud mobile présente dans la demande, alors les considérations suivantes DOIVENT être appliquées pour locakiser l'entrée d'antémémoire de liens.

1. L'ancre de mobilité locale DOIT vérifier si il existe une et seulement une entrée d'antémémoire de liens avec l'identifiant de nœud mobile correspondant à l'identifiant de l'option Identifiant de nœud mobile présente dans la demande.

2. Si il existe seulement une telle entrée (correspondant à l'identifiant de MN) et si le champ Indicateur de relais dans l'option Indicateur de relais présente dans la demande est réglé à une valeur de 2 (relais entre deux interfaces différentes du nœud mobile) ou est réglé à une valeur de 3 (relais entre passerelles d'accès mobile pour la même interface) alors la demande DOIT être considérée comme une demande de mise à jour de cette entrée d'antémémoire de liens.

3. Si il existe seulement une entrée (correspondant à l'identifiant de MN) et si le champ Indicateur de relais dans l'option Indicateur de relais présente dans la demande est réglé à une valeur de 4 (état de relais inconnu) l'ancre de mobilité locale DEVRAIT attendre jusqu'à ce que l'entrée d'antémémoire de liens existante soit désenregistrée par la passerelle d'accès mobile antérieurement desservante avant que la demande puisse être considérée comme une demande de mise à jour de cette entrée d'antémémoire de liens. Cependant, si il n'y a pas de message de désenregistrement reçu dans le délai MaxDelayBeforeNewBCEAssign *(délai maximum avant l'allocation d'une nouvelle BCE)* l'ancre de mobilité locale, quand elle accepte la demande, DOIT considérer la demande comme une demande de création d'une nouvelle session de mobilité. L'ancre de mobilité locale PEUT aussi choisir de créer une nouvelle session de mobilité sans attendre un message de désenregistrement, et cela devrait être configurable sur l'ancre de mobilité locale.

4. Pour tous les autres cas, le message DOIT être considéré comme une demande de création d'une nouvelle session de mobilité. Cependant, si le message de mise à jour de lien de mandataire reçu a la valeur de durée de vie de zéro et si la demande ne peut pas être associée à une session de mobilité existante, le message DOIT être ignoré en silence.

5.5 Option Horodatage pour rangement des messages

IPv6 mobile [RFC3775] utilise le champ Numéro de séquence dans les messages d'enregistrement de lien comme moyen pour que l'agent de rattachement traite les mises à jour de lien dans l'ordre où elles ont été envoyées par un nœud mobile. L'agent de rattachement et le nœud mobile sont obligés de gérer ce compteur sur la durée de vie d'un lien. Cependant, dans

le mandataire IPv6 mobile, comme le nœud mobile passe d'une passerelle d'accès mobile à une autre et en l'absence de mécanismes comme un transfert de contexte entre les passerelles d'accès mobile, la passerelle d'accès mobile desservante ne va pas être capable de déterminer le numéro de séquence qu'elle a besoin d'utiliser dans les messages de signalisation. Donc, le schéma de numéro de séquence, comme spécifié dans la [RFC3775], va être insuffisant pour le mandataire IPv6 mobile.

Si l'ancre de mobilité locale ne peut pas déterminer l'ordre d'envoi des messages de mise à jour de lien de mandataire reçus, elle peut éventuellement traiter un plus ancien message envoyé par une passerelle d'accès mobile où le nœud mobile était précédemment ancré, mais livré déclassé, d'où résulterait une mise à jour incorrecte de l'entrée d'antémémoire de liens du nœud mobile et créerait un état d'acheminement pour le tunnelage du trafic du nœud mobile à la passerelle d'accès mobile précédente.

Pour résoudre ce problème, la présente spécification adopte deux solutions alternatives. Une se fonde sur les horodatages, et l'autre sur les numéros de séquence, comme défini dans la [RFC3775].

Le principe de base derrière l'utilisation des horodatages dans les messages d'enregistrement de lien est que le nœud qui génère le message insère l'heure actuelle, et le nœud qui reçoit le message vérifie que cet horodatage est supérieur à tous les horodatages précédemment acceptés. La solution fondée sur l'horodatage peut être utilisée quand les passerelles d'accès mobile qui desservent un domaine de mandataire IPv6 mobile n'ont pas la capacité d'obtenir le dernier numéro de séquence qui a été envoyé dans un message de mise à jour de lien de mandataire pour mettre à jour le lien d'un certain nœud mobile.

La dérive d'horloge réduit l'efficacité du mécanisme d'horodatage. Le temps exigé pour la reconnexion est la somme du temps nécessaire pour que le nœud mobile se tranfère entre deux passerelles d'accès mobile et du temps nécessaire pour que la passerelle d'accès mobile desservante détecte le nœud mobile sur sa liaison d'accès et construise le message de mise à jour de lien de mandataire. Si la dérive d'horloge sur l'une des deux passerelles d'accès mobile voisines (par rapport à la source de temps commune utilisée pour la synchronisation d'horloges) est de plus de la moitié de ce temps de reconnexion, la solution d'horodatage ne va pas fonctionner de façon prévisible dans tous les cas et donc NE DEVRAIT PAS être utilisée.

Comme solution de remplacement à l'approche de l'hordatage, la spécification permet aussi l'utilisation du schéma fondé sur le numéro de séquence, comme spécifié dans la [RFC3775]. Cependant, pour que ce schéma fonctionne, la passerelle d'accès mobile desservante dans un domaine de mandataire IPv6 mobile DOIT avoir la capacité d'obtenir le dernier numéro de séquence envoyé dans un message d'enregistrement de lien pour cette session de mobilité. Le numéro de séquence DOIT être tenu sur la base de la session de mobilité d'un nœud mobile et DOIT être disponible à la passerelle d'accès mobile desservante. Cela peut être réalisé en utilisant des schémas de transfert de contexte ou en conservant le numéro de séquence dans un magasin de politiques. Cependant, les détails spécifiques de la façon dont le numéro de séquence du nœud mobile est rendu disponible à la passerelle d'accès mobile desservante avant d'envoyer le message de mise à jour de lien de mandataire sort du domaine d'application de ce document.

Utilisation de l'approche de l'hordatage :

1. Une mise en œuvre d'ancre de mobilité locale DOIT prendre en charge l'option Horodatage. Si l'option Horodatage est présente dans le message de mise à jour de lien de mandataire reçu, alors l'ancre de mobilité locale DOIT inclure une option Horodatage valide dans le message Accusé de réception de lien de mandataire qu'elle envoie à la passerelle d'accès mobile.

2. Toutes les entités de mobilité dans un domaine de mandataire IPv6 mobile qui échangent des messages d'enregistrement de lien en utilisant l'option Horodatage DOIVENT avoir des horloges adéquatement synchronisées. C'est l'exigence essentielle pour que cette solution fonctionne. Si cette exigence n'est pas satisfaite, la solution ne va pas fonctionner de façon prévisible dans tous les cas.

3. Les entités de mobilité dans un domaine de mandataire IPv6 mobile DEVRAIENT synchroniser leurs horloges avec une source horaire commune. Pour synchroniser les horloges, les nœuds PEUVENT utiliser le protocole de l'heure du réseau [RFC4330]. Des déploiements PEUVENT aussi adopter d'autres approches convenables pour ce déploiement spécifique. Autrement, si il y a un horodatage généré par un nœud mobile qui augmente à chaque rattachement à la liaison d'accès et si cet horodatage est disponible à la passerelle d'accès mobile (par exemple, l'option Horodatage dans les messages SEND [RFC3971] qu'envoie le nœud mobile) la passerelle d'accès mobile peut utiliser cet horodatage ou le numéro de séquence dans les messages de mise à jour de lien de mandataire et n'a pas à dépendre d'une source d'horloge externe. Cependant, les détails spécifiques de la façon de réaliser cela sortent du domaine d'application de ce document.

4. Quand elles génèrent la valeur d'horodatage pour construire l'option Horodatage, les entités de mobilité DOIVENT s'assurer que l'horodatage généré est le temps écoulé depuis la même époque de référence, comme spécifié dans le format pour l'option Horodatage (paragraphe 8.8).

5. Si l'option Horodatage est présente dans le message de mise à jour de lien de mandataire reçu, l'ancre de mobilité locale DOIT ignorer le champ Numéro de séquence du message. Cependant, elle DOIT copier le numéro de séquence du message de mise à jour de lien de mandataire reçu dans le message Accusé de réception de lien de mandataire.

6. À réception d'un message de mise à jour de lien de mandataire avec l'option Horodatage, l'ancre de mobilité locale DOIT vérifier la validité du champ d'horodatage. Pour qu'il soit considéré comme valide, ce qui suit DOIT être vrai :
   * La valeur d'horodatage contenue dans l'option Horodatage DOIT être assez proche (dans l'intervalle de différence de TimestampValidityWindow *(fenêtre de validité d'horodatage)*) de l'heure de l'horloge de l'ancre de mobilité locale. Cependant, si le fanion MobileNodeGeneratedTimestampInUse *(utilisation de l'horodatage généré par le nœud mobile)* est réglé à une valeur de 1, l'ancre de mobilité locale DOIT ignorer cette vérification et effectuer seulement la vérification suivante.
   * L'horodatage DOIT être supérieur à tous les horodatages acceptés précédemment dans les messages de mise à jour de lien de mandataire envoyés pour ce nœud mobile.

7. Si la valeur d'horodatage dans la mise à jour de lien de mandataire reçue est valide (comme spécifié dans les considérations ci-dessus) ou si le fanion MobileNodeGeneratedTimestampInUse est réglé à la valeur de 1, l'ancre de mobilité locale DOIT retournr la même valeur d'horodatage dans l'option Horodatage incluse dans le message Accusé de réception de lien de mandataire que celle envoyée à la passerelle d'accès mobile.

8. Si la valeur d'horodatage dans la mise à jour de lien de mandataire reçue est inférieure à l'horodatage précédemment accepté dans les messages de mise à jour de lien de mandataire envoyés pour ce lien de mobilité, l'ancre de mobilité locale DOIT rejeter le message de mise à jour de lien de mandataire et envoyer un message Accusé de réception de lien de mandataire avec le champ État réglé à TIMESTAMP_LOWER_THAN_PREV_ACCEPTED *(horodatage inférieur à celui accepté précédemment)*. Le message DOIT aussi inclure l'option Horodatage avec la valeur réglée à l'heure actuelle sur l'ancre de mobilité locale.

9. Si la valeur d'horodatage dans la mise à jour de lien de mandataire reçue n'est pas valide (comme spécifié dans les considérations ci-dessus) l'ancre de mobilité locale DOIT rejeter la mise à jour de lien de mandataire et envoyer un message Accusé de réception de lien de mandataire avec le champ État réglé à TIMESTAMP_MISMATCH *(discordance d'hordatage)*. Le message DOIT aussi inclure l'option Horodatage avec la valeur réglée à l'heure actuelle sur l'ancre de mobilité locale.

Utilisation de l'approche du numéro de séquence :

1. Si l'option Horodatage n'est pas présente dans le message de mise à jour de lien de mandataire reçu, l'ancre de mobilité locale DOIT revenir au schéma fondé sur le numéro de séquence. Elle DOIT traiter le champ Numéro de séquence comme spécifié dans la [RFC3775]. Aussi, elle NE DOIT PAS inclure l'option Horodatage dans les messages Accusé de réception de lien de mandataire qu'elle envoie à la passerelle d'accès mobile.

2. Une mise en œuvre DOIT prendre en charge le schéma fondé sur le numéro de séquence, comme spécifié dans la [RFC3775].

3. L'approche fondée sur le numéro de séquence ne peut être utilisée que quand il y a un mécanisme (comme la procédure de transfert de contexte entre passerelles d'accès mobile) qui permet à la passerelle d'accès mobile desservante d'obtenir le dernier numéro de séquence envoyé dans un message de mise à jour de lien de mandataire pour mettre à jour le lien du nœud mobile concerné.

5.6 Considérations d'acheminement

5.6.1 Gestion de tunnel bidirectionnel

Le tunnel bidirectionnel DOIT être utilisé pour acheminer le trafic de données du nœud mobile entre la passerelle d'accès mobile et l'ancre de mobilité locale. Un tunnel cache la topologie et permet au nœud mobile d'utiliser la ou les adresses provenant de son ou ses préfixes de réseau de rattachement de toute liaison d'accès dans ce domaine de mandataire IPv6 mobile. Un tunnel peut être créé de façon dynamique quand nécessaire et supprimé quand il n'est plus utile. Cependant, les mises en œuvre PEUVENT choisir d'utiliser des tunnels statiques pré-établis au lieu de les créer et supprimer dynamiquement selon leurs besoins. Les considérations suivantes DOIVENT être appliquées quand on utilise des tunnels créés dynamiquement.

- Un tunnel bidirectionnel DOIT être établi entre l'ancre de mobilité locale et la passerelle d'accès mobile et l'ancre de mobilité locale avec encapsulation IPv6 dans IPv6, comme décrit dans la [RFC2473]. Les points d'extrémité de tunnel sont la Proxy-CoA et la LMAA. Cependant, quand on utilise le transport IPv4, les points d'extrémité du tunnel sont IPv4-LMAA et IPv4-Proxy-CoA avec le mode d'encapsulation spécifié dans la [RFC5844].

- Les mises en œuvre PEUVENT utiliser un temporisateur logiciel pour gérer la durée de vie du tunnel et un compteur pour tenir le compte de tous les nœuds mobiles qui partagent le tunnel. La valeur du temporisateur peut être réglée à la durée de vie acceptée du lien et peut être mise à jour après chaque réenregistrement périodique pour étendre la durée de vie. Si le tunnel est partagé par plusieurs nœuds mobiles, la durée de vie du tunnel doit être réglée à la plus longue durée de vie de lien qui est accordée à tout nœud mobile qui partage ce tunnel.

- Le tunnel DEVRAIT être supprimé quand soit la durée de vie du tunnel arrive à expiration, soit quand il n'y a plus de nœud mobile qui partage le tunnel.

5.6.2 Considérations de transmission

Interception des paquets envoyés au réseau de rattachement du nœud mobile :

- Quand l'ancre de mobilité locale dessert un nœud mobile, elle DOIT être capable de recevoir les paquets qui sont envoyés au réseau de rattachement du nœud mobile. Afin qu'elle reçoive ces paquets, elle DOIT annoncer un chemin connecté dans l'infrastructure d'acheminement pour le ou les préfixes de réseau de rattachement du nœud mobile ou pour un préfixe agrégé d'une plus grande portée. Cela permet essentiellement aux routeurs IPv6 dans ce réseau de détecter l'ancre de mobilité locale comme routeur de dernier bond pour le ou les préfixes de réseau de rattachement du nœud mobile.

Transmission des pacquets au nœud mobile :

À réception d'un paquet d'un nœud correspondant avec l'adresse de destination correspondant au ou aux préfixes de réseau de rattachement d'un nœud mobile, l'ancre de mobilité locale DOIT transmettre le paquet à travers le tunnel bidirectionnel établi pour ce nœud mobile.

- Le format du paquet tunnelé est montré ci-dessous. Les considérations de la [RFC2473] DOIVENT être appliquées pour l'encapsulation IPv6. Cependant, quand le transport IPv4 est utilisé, le format du paquet est comme décrit dans la [RFC5844].

```
en-tête IPv6 (src= LMAA, dst= Proxy-CoA      /* en-tête de tunnel */
  en-tête IPv6 (src= CN, dst= MN-HOA)        /* en-tête de paquet */
     protocoles de couche supérieure         /* contenu de paquet*/
```

Figure 10 : Paquet tunnelé de LMA à MAG

- Le format du paquet tunnelé est montré ci-dessous, quand la protection de la charge utile avec IPsec est activée pour le trafic de données du nœud mobile. Cependant, quand le transport IPv4 est utilisé, le format du paquet est comme décrit dans la [RFC5844].

```
en-tête IPv6 (src= LMAA, dst= Proxy-CoA      /* en-tête de tunnel */
  en-tête ESP en mode tunnel                 /* en-tête ESP */
    en-tête IPv6 (src= CN, dst= MN-HoA )     /* en-tête de paquet */
      protocoles de couche supérieure        /* contenu de paquet*/
```

Figure 11 : Paquet tunnelé du LMA au MAG avec protection de la charge utile

Transmission des paquets envoyés par le nœud mobile :

- Tous les paquets sur le tunnel inverse que l'ancre de mobilité locale a reçus de la passerelle d'accès mobile, après suppression de l'en-tête de tunnel DOIVENT être acheminés à la destination spécifiée dans l'en-tête interne du paquet. Ces paquets acheminés vont avoir le champ Adresse de source réglé à l'adresse de rattachement du nœud mobile. Les considérations de la [RFC2473] DOIVENT être appliquées pour la désencapsulation IPv6.

5.6.3 Considérations de notification explicite d'encombrement (ECN) pour les tunnels de mandataire IPv6 mobile

Ce paragraphe décrit comment les informations d'ECN doivent être traitées par les agents de mobilité à l'entrée du tunnel et aux points de sortie. Les considerations d'ECN pour les tunnels IP sont spécifiées dans la [RFC3168], et les mêmes considérations s'appliquent aux tunnels de mandataire IPv6 mobile (en utilisant le mode d'encapsulation IPv6 dans IPv6). Pécisément, l'option de pleine fonctionnalité DOIT être prise en charge. Les considérations d'ECN pertinentes provenant de la [RFC3168] sont résumées ici.

Considérations d'encapsulation : si le champ Notification explicite d'encombrement (ECN) dans l'en-tête interne est réglé à ECT(0) ou ECT(1), où ECT signifie "transport à capacité ECN" (ECT, *ECN-Capable Transport*) le champ ECN provenant de l'en-tête interne DOIT être copié sur l'en-tête externe. De plus, quand la protection de la charge utile avec IPsec est activée pour le trafic de données du nœud mobile, les considérations d'ECN de la [RFC4301] DOIVENT être appliquées.

Considérations de désencapsulation : si le champ Notification explicite d'encombrement (ECN) dans l'en-tête interne est réglé à ECT(0) ou ECT(1), et si le champ ECN dans l'en-tête externe est réglé à "Encombrement rencontré" (CE, *Congestion Experienced*) alors le champ ECN dans l'en-tête interne DOIT être réglé à CE. Autrement, le champ ECN dans l'en-tête interne NE DOIT PAS être modifié. De plus, quand la protection de la charge utile avec IPsec est activée pour le trafic de données du nœud mobile, les considérations d'ECN de la [RFC4301] DOIVENT être appliquées.

5.7 Découverte d'adresse d'ancre de mobilité locale

La découverte dynamique d'adresse d'agent de rattachement (DHAAD, *Dynamic Home Agent Address Discovery*) expliquée au paragraphe 10.5 de la [RFC3775], permet à un nœud mobile de découvrir tous les agents de rattachement sur sa liaison de rattachement en envoyant un message ICMP de demande de découverte d'adresse d'agent de rattachement à l'adresse d'envoi à la cantonade d'agent de rattachementt IPv6, déduite de son préfixe de réseau de rattachement.

Le message DHAAD dans sa forme actuelle ne peut pas être utilisé par le mandataire IPv6 mobile pour découvrir l'adresse de l'ancre de mobilité locale du nœud mobile. Dans le protocole de mandataire IPv6 mobile, l'ancre de mobilité locale ne va pas être capable de recevoir de messages envoyés à l'adresse d'envoi à la cantonade de l'agent de rattachement IPv6 mobile correspondant au ou aux préfixes de réseau de rattachement du nœud mobile, car les préfixes ne sont pas hébergés sur ces interfaces. De plus, la passerelle d'accès mobile ne va pas être capable de localiser de façon prévisible l'ancre de mobilité locale qui a l'entrée d'antémémoire de lien du nœud mobile. Donc, la présente spécification ne prend pas en charge le protocole de découverte dynamique d'adresse d'agent de rattachement.

Dans le protocole de mandataire IPv6 mobile, l'adresse de l'ancre de mobilité locale configurée pour desservir un nœud mobile peut être découverte par l'entité de passerelle d'accès de mobilité via d'autres moyens. La LMA à allouer à un nœud mobile peut être une entrée configurée dans le profil de politique du nœud mobile, ou elle peut être obtenue par des mécanismes qui sortent du domaine d'application de ce document.

5.8 Considérations de découverte de préfixe mobile

La présente spécification ne prend pas en charge la découverte de préfixe mobile. Le mécanisme de découverte de préfixe mobile comme spécifié dans la [RFC3775] n'est pas applicable au mandataire IPv6 mobile.

5.9 Considérations d'optimisation de chemin

L'optimisation de chemin dans IPv6 mobile, comme définie dans la [RFC3775], permet à un nœud mobile de communiquer avec un nœud correspondant en utilisant directement son adresse d'entretien et de plus la procédure d'acheminement de retour permet au nœud correspondant d'avoir une confiance raisonnable que le nœud mobile est accessible à ses deux adresses de rattachement et d'entretien.

La présente spécification ne prend pas en charge l'optimisation de chemin spécifiée dans IPv6 mobile [RFC3775]. Cependant, la présente spécification prend bien en charge une autre forme d'optimisation de chemin, spécifiée au paragraphe 6.10.3.

6. Fonctionnement de passerelle d'accès mobile

Le protocole de mandataire IPv6 mobile décrit dans le présent document introduit une nouvelle entité fonctionnelle, la passerelle d'accès mobile (MAG). La passerelle d'accès mobile est l'entité qui est chargée de détecter les mouvements du

nœud mobile vers et depuis la liaison d'accès et d'envoyer les messages de mise à jour de lien de mandataire à l'ancre de mobilité locale. Par essence, la passerelle d'accès mobile effectue la gestion de mobilité au nom du nœud mobile.

La passerelle d'accès mobile est une fonction qui est normalement assurée par un routeur d'accès. Cependant, des mises en œuvre PEUVENT choisir de partager cette fonction entre plusieurs systèmes. Les spécificités de cette réalisation ou des interactions de signalisation entre ces entités fonctionnelles sortent du domaine d'application de ce document.

La passerelle d'accès mobile a les rôles fonctionnels clés suivants :
- o Elle est chargée de détecter les mouvements du nœud mobile sur la liaison d'accès et d'initier la signalisation de mobilité avec l'ancre de mobilité locale du nœud mobile.
- o Émulation de la liaison de rattachement du nœud mobile sur la liaison d'accès en envoyant des messages Annonce de routeur contenant le ou les préfixes de réseau de rattachement du nœud mobile, chaque préfixe porté utilisant l'option Informations de préfixe [RFC4861].
- o Chargée d'établir la transmission pour permettre au nœud mobile de configurer une ou plusieurs adresses à partir de son ou ses préfixes de réseau de rattachement et de les utiliser à partir de la liaison d'accès rattachée.

6.1 Extensions à la structure de données d'entrée de liste de mise à jour de lien

Chaque passerelle d'accès mobile DOIT tenir une liste des mises à jour de lien. Chaque entrée dans la liste des mises à jour de lien représente un lien de mobilité d'un nœud mobile avec son ancre de mobilité locale. La liste des mises à jour de lien est une structure de données conceptuelle, décrite au paragraphe 11.1 de la [RFC3775].

Pour prendre en charge la présente spécification, la structure de données conceptuelle d'entrée de liste de mises à jour de lien doit être étendue avec les champs supplémentaires suivants.

- o L'identifiant du nœud mobile rattaché, MN-Identifiant. Cet identifiant est acquis durant le rattachement du nœud mobile à la liaison d'accès par des mécanismes qui sortent du domaine d'application de ce document.

- o L'identifiant de couche de liaison de l'interface connectée du nœud mobile. Il peut être acquis des messages de sollicitation de routeur reçus du nœud mobile ou durant le rattachement du nœud mobile au réseau d'accès. C'est normalement un identifiant de couche de liaison porté par le nœud mobile ; cependant, les détails spécifiques de la façon de le porter sortent du domaine d'application de la présente spécification. Si cet identifiant n'est pas disponible, ce champ de longueur variable DOIT être réglé à deux (octets) et DOIT être initialisé à la valeur de TOUT_ZÉRO.

- o Une liste de préfixes IPv6 de réseau de rattachement alloués à l'interface connectée du nœud mobile. Le ou les préfixes de réseau de rattachement peuvent avoir été configurés statiquement dans le profil de politique du nœud mobile, ou peuvent avoir été alloués dynamiquement par l'ancre de mobilité locale. Chacune de ces entrées de préfixe va aussi inclure la longueur de préfixe correspondante.

- o L'adresse de liaison locale de la passerelle d'accès mobile sur la liaison d'accès partagée avec le nœud mobile.

- o L'adresse IPv6 de l'ancre de mobilité locale qui dessert le nœud mobile rattaché. Cette adresse est acquise du profil de politique du nœud mobile ou par d'autres moyens.

- o L'identifiant d'interface (si-id) de la liaison point à point entre le nœud mobile et la passerelle d'accès mobile. Ceci est interne à la passerelle d'accès mobile et est utilisé pour associer le tunnel de mandataire IPv6 mobile à la liaison d'accès où le nœud mobile est rattaché.

- o L'identifiant d'interface de tunnel (tunnel-si-id) du tunnel bidirectionnel entre l'ancre de mobilité locale du nœud mobile et la passerelle d'accès mobile. Ceci est interne à la passerelle d'accès mobile. L'identifiant d'interface de tunnel est acquis durant la création du tunnel.

6.2 Profil de politique de nœud mobile

Le profil de politique d'un nœud mobile contient les paramètres de fonctionnement essentiels pour que les entités du réseau gèrent le service de mobilité du nœud mobile. Ces profils de politique sont mémorisés dans un magasin local ou distant de politiques. La passerelle d'accès mobile et l'ancre de mobilité locale DOIVENT être capables d'obtenir le profil de politique d'un nœud mobile. Le profil de politique PEUT aussi être traité sur une passerelle d'accès mobile desservante au titre d'une procédure de transfert de contexte durant un relais ou la passerelle d'accès mobile desservante PEUT être capable de générer dynamiquement ce profil. Les détails exacts de la façon de réaliser cela sortent du domaine d'application de ce

document. Cependant, la présente spécification exige qu'une passerelle d'accès mobile desservant un nœud mobile DOIT avoir accès à son profil de politique.

Les champs suivants sont obligatoires dans le profil de politique :
- o L'identifiant du nœud mobile (MN-Identifiant)
- o L'adresse IPv6 de l'ancre de mobilité locale (LMAA)

Les champs suivants sont facultatifs dans le profil de politique :
- o Le ou les préfixes IPv6 de réseau de rattachement du nœud mobile alloués à l'interface connectée du nœud mobile. Ces préfixes doivent être tenus par interface. Il peut y avoir plusieurs entrées uniques pour chaque interface du nœud mobile. Les détails spécifiques de la façon dont le réseau maintient cette association entre l'ensemble de préfixes et les interfaces, spécialement durant le relais de la session de mobilité entre interfaces, sortent du domaine de ce document.
- o La durée de vie du préfixe IPv6 du réseau de rattachement du nœud mobile. Cette durée de vie va être la même pour tous les préfixes hébergés sur la liaison, car ils font tous partie d'une session de mobilité. Cette valeur peut aussi être la même pour toutes les sessions de mobilité du nœud mobile.
- o Les procédures de configuration d'adresse prises en charge (à état pleins, sans état, ou les deux) pour le nœud mobile dans le domaine de mandataire IPv6 mobile

6.3 Types de liaisons d'accès prises en charge

La présente spécification ne prend en charge que les types de liaison d'accès en point à point, et donc, elle suppose que le nœud mobile et la passerelle d'accès mobile sont les deux seuls nœuds sur la liaison d'accès. La liaison est supposée avoir la capacité de diffusion groupée.

Ce protocole peut aussi être utilisé sur d'autres types de liaisons, pour autant que la liaison soit configurée d'une façon telle qu'elle émule la livraison point à point entre le nœud mobile et la passerelle d'accès mobile pour tout le trafic de protocole.

Il est aussi nécessaire d'être capable d'identifier les nœuds mobiles qui se rattachent à la liaison. Les exigences qui s'y rapportent sont traitées au paragraphe 6.6.

Finalement, bien que la présente spécification puisse opérer sans indication de couche de liaison sur le rattachement et le détachement du nœud à la liaison, l'existence de telles indications du côté réseau ou du côté nœud mobile améliore les performances résultantes.

6.4 Modes de configuration d'adresse pris en charge

Un nœud mobile dans le domaine de mandataire IPv6 mobile peut configurer une ou plusieurs adresses IPv6 mondiales sur son interface (en utilisant les procédures d'autoconfiguration d'adresse sans état, à états pleins ou la configuration d'adresse manuelle) à partir du ou des préfixes hébergés sur cette liaison. Les messages Annonce de routeur envoyés sur la liaison d'accès spécifient les méthodes de configuration d'adresse permises sur cette liaison d'accès pour ce nœud mobile. Cependant, les fanions annoncés, par rapport à la configuration d'adresse, vont être cohérents pour un nœud mobile, sur toute liaison d'accès dans ce domaine de mandataire IPv6 mobile. Normalement, ces réglages de configuration vont se fonder sur la politique au niveau du domaine ou sur une politique spécifique de chaque nœud mobile.

Quand l'autoconfiguration d'adresse sans état est prise en charge sur la liaison d'accès, le nœud mobile peut générer une ou plusieurs adresses IPv6 à partir du ou des préfixes hébergés par les mécanismes IPv6 standard comme l'autoconfiguration sans état de la [RFC4862] ou les extensions de confidentialité de la [RFC4941].

Quand l'autoconfiguration d'adresse à états pleins est prise en charge sur la liaison, le nœud mobile peut obtenir la configuration d'adresse du serveur DHCP situé dans le domaine de mandataire IPv6 mobile, par les mécanismes DHCP standard, comme spécifié dans la [RFC3315]. La ou les adresses obtenues vont être de son ou ses préfixes de réseau de rattachement. Le paragraphe 6.11 spécifie les détails de la façon dont cette configuration peut être réalisée.

De plus, d'autres mécanismes de configuration d'adresse spécifiques de la liaison d'accès entre le nœud mobile et la passerelle d'accès mobile peuvent aussi être utilisés pour livrer la configuration d'adresse au nœud mobile. La présente spécification ne modifie pas le comportement des mécanismes standard de configuration d'adresse IPv6.

6.5 Authentification d'accès et identification de nœud mobile

Quand un nœud mobile se rattache à une liaison d'accès connectée à la passerelle d'accès mobile, les protocoles de sécurité d'accès déployés sur cette liaison DEVRAIENT s'assurer que le service de gestion de la mobilité fondée sur le réseau est

offert seulement après l'authentification et l'autorisation du nœud mobile pour ce service. La spécification exacte de la façon dont c'est réalisé ou les interactions entre la passerelle d'accès mobile et le service de sécurité d'accès sortent du domaine d'application du présent document. La présente spécification fait l'hypothèse qu'un certain niveau de confiance est établi entre le nœud mobile et la passerelle d'accès mobile avant que le protocole commence à fonctionner.

6.6 Acquisition d'identifiant de nœud mobile

Toutes les entités du réseau dans un domaine de mandataire IPv6 mobile DOIVENT être capables d'identifier un nœud mobile, en utilisant son identifiant de nœud mobile. Cet identifiant DOIT être stable et unique à travers le domaine de mandataire IPv6 mobile. Les entités de mobilité dans le domaine de mandataire IPv6 mobile DOIVENT être capables d'utiliser cet identifiant dans les messages de signalisation et d'identifier sans ambiguïté un certain nœud mobile. Les considérations suivantes se rapportent à cet identifiant de nœud mobile.

- Le MN-Identifiant est normalement obtenu au titre de l'authentification d'accès ou d'un événement notifié de rattachement au réseau. Dans les cas où l'identifiant d'utilisateur authentifié durant l'authentification d'accès identifie de façon univoque un nœud mobile, le MN-Identifiant PEUT être le même que l'identifiant d'utilisateur. Cependant, l'identifiant d'utilisateur NE DOIT PAS être utilisé si il identifie un compte d'utilisateur qui peut être utilisé à partir de plus d'un nœud mobile fonctionnant dans le même domaine de mandataire IPv6 mobile.

- Dans certains cas, l'identifiant obtenu au titre de l'authentification d'accès, peut être un identifiant temporaire et de plus cet identifiant temporaire peut être différent à chaque ré-authentification. Cependant, la passerelle d'accès mobile DOIT être capable d'utiliser cet identifiant temporaire et obtenir l'identifiant stable du nœud mobile à partir de la mémorisation de politique. Par exemple, dans les systèmes fondés sur AAA, l'attribut du service d'authentification distante d'utilisateur appelant (RADIUS, *Remote Authentication Dial-In User Service*) l'identité de l'utilisateur facturable *(Chargeable-User-Identity)* [RFC4372] peut être utilisée, pour autant qu'elle identifie de façon univoque le nœud mobile, et non un compte d'utilisateur qui peut être utilisé par plusieurs nœuds mobiles.

- Dans certains cas et pour des raisons de confidentialité, le MN-Identifiant que la politique mémorisée livre à la passerelle d'accès mobile peut n'être pas le vrai identifiant du nœud mobile. Cependant, la passerelle d'accès mobile DOIT être capable d'utiliser cet identifiant dans les messages de signalisation échangés avec l'ancre de mobilité locale.

- La passerelle d'accès mobile DOIT être capable d'identifier le nœud mobile par son MN-Identifiant, et elle DOIT être capable d'associer cette identité à la liaison point à point partagée avec le nœud mobile.

6.7 Émulation de réseau de rattachement

Une des fonctions clés d'une passerelle d'accès mobile est d'émuler le réseau de rattachement du nœud mobile sur la liaison d'accès. Elle doit s'assurer que le nœud mobile ne détecte aucun changement par rapport à son rattachement de couche 3 même après qu'il a changé son point de rattachement dans ce domaine de mandataire IPv6 mobile.

Pour émuler la liaison de rattachement du nœud mobile sur la liaison d'accès, la passerelle d'accès mobile doit être capable d'envoyer des messages Annonce de routeur annonçant le ou les préfixes de réseau de rattachement du nœud mobile portés en utilisant la ou les options Information de préfixe [RFC4861] et avec d'autres paramètres de configuration d'adresse cohérents avec ses propriétés de liaison de rattachement. Normalement, ces réglages de configuration vont se fonder sur la politique globale du domaine ou sur une politique spécifique de chaque nœud mobile.

Normalement, la passerelle d'accès mobile apprend les détails du ou des préfixes de réseau de rattachement du nœud mobile du message Accusé de réception de lien de mandataire reçu, ou elle peut les obtenir du profil de politique du nœud mobile. Cependant, la passerelle d'accès mobile DEVRAIT n'envoyer des annonces de routeur annonçant le ou les préfixes de réseau de rattachement du nœud mobile qu'après avoir terminé avec succès l'enregistrement de lien auprès de l'ancre de mobilité locale du nœud mobile.

Quand elle annonce le ou les préfixes de réseau de rattachement dans les messages Annonce de routeur, la passerelle d'accès mobile PEUT régler la valeur de durée de vie du préfixe pour le ou les préfixes annoncés à toute valeur choisie à sa discrétion. Une mise en œuvre PEUT choisir de lier la durée de vie du préfixe à la durée de vie du lien du nœud mobile. La durée de vie du préfixe peut aussi être un paramètre de configuration facultatif dans le profil de politique du nœud mobile.

6.8 Unicité d'adresse de liaison locale et mondiale

Un nœud mobile dans le domaine de mandataire IPv6 mobile, lorsqu'il passe d'une passerelle d'accès mobile à une autre, va continuer de détecter son réseau de rattachement et ne détecte pas de changement du rattachement de couche 3. Chaque fois

que le nœud mobile se rattache à une nouvelle liaison, l'événement relatif au changement de l'état d'interface va déclencher l'opération par le nœud mobile de la détection d'adresse dupliquée (DAD, *Duplicate Address Detection*) sur la ou les adresses de liaison locale et globale. Cependant, si le nœud mobile a la capacité de détection du rattachement réseau dans IPv6 (DNAv6, *Detecting Network Attachment in IPv6*) comme spécifié dans [DNAV6], il peut ne pas détecter le changement de la liaison à cause des optimisations de DNAv6 et peut ne pas déclencher la procédure de détection d'adresse dupliquée (DAD) pour les adresses existantes, ce qui peut éventuellement conduire à des collisions d'adresses après le relais du nœud mobile à une nouvelle liaison.

La question de la collision d'adresses n'est pas pertinente pour les adresses mondiales de nœud mobile. Comme les préfixes de réseau de rattachement alloués sont pour l'usage exclusif du nœud mobile, aucun autre nœud ne partage d'adresse (autre que l'adresse d'envoi à la cantonade de routeur de sous réseau qui est configurée par la passerelle d'accès mobile) à partir du ou des préfixes, et donc l'unicité de l'adresse mondile du nœud mobile est assurée sur la liaison d'accès.

La question de la collision d'adresses est cependant pertinente pour les adresses de liaison locale du nœud mobile car la passerelle d'accès mobile et le nœud mobile vont avoir des adresses de liaison locale configurées à partir du même préfixe de liaison locale (FE80::/64). Cela laisse une place pour la collision d'adresse de liaison locale entre les deux voisins (c'est-à-dire, le nœud mobile et la passerelle d'accès mobile) sur cette liaison d'accès. Pour résoudre ce problème, la présente spécification exige que l'adresse de liaison locale que la passerelle d'accès mobile configure sur la liaison en point à point partagée avec un certain nœud mobile soit générée par l'ancre de mobilité locale et soit mémorisée dans l'entrée d'antémémoire de liens du nœud mobile. Cette adresse ne va pas changer pendant la durée de la session de mobilité de ce nœud mobile et peut être fournie à la passerelle d'accès mobile desservante à chaque relais du nœud mobile, au titre des messages de signalisation de mandataire IPv6 mobile. La méthode spécifique par laquelle l'ancre de mobilité locale génère l'adresse de liaison locale sort du domaine d'application de la présente spécification.

Il est très souhaitable que la liaison d'accès sur la passerelle d'accès mobile partagée avec le nœud mobile soit provisionnée de telle façon qu'avant que le nœud mobile achève l'opération de DAD [RFC4862] sur son adresse de liaison locale, la passerelle d'accès mobile sur cette liaison connaisse sa propre adresse de liaison locale fournie par l'ancre de mobilité locale qu'il a besoin d'utiliser sur cette liaison d'accès. Cela exige essentiellement un achèvement réussi de la signalisation de mandataire IPv6 mobile par la passerelle d'accès mobile avant que le nœud mobile achève l'opération de DAD. Cela peut être réalisé en s'assurant que le rattachement de couche de liaison ne se termine pas tant que la signalisation de mandataire IPv6 mobile n'est pas achevée. Autrement, les temporisateurs de retransmission de capacité et de signalisation du réseau et de l'ancre de mobilité locale peuvent être provisionnés de telle façon que la signalisation ait une forte probabilité de se terminer durant la période d'attente par défaut associée au processus de DAD.

Faculativement, les mises en œuvre PEUVENT choisir de configurer une adresse fixe de liaison locale à travers toutes les liaisons d'accès dans un domaine de mandataire IPv6 mobile et sans qu'il soit besoin de porter cette adresse de l'ancre de mobilité locale à la passerelle d'accès mobile dans les messages de signalisation de mandataire IPv6 mobile. La variable de configuration FixedMAGLinkLocalAddressOnAllAccessLinks *(adresse de liaison locale de passerelle d'accès mobile fixe dans toutes les liaisons d'accès)* détermine le mode activé dans ce domaine de mandataire IPv6 mobile.

6.9 Considérations de signalisation

6.9.1 Enregistrements de liens

6.9.1.1 Rattachement de nœud mobile et enregistrement de lien initial

1. Après avoir détecté un nouveau nœud mobile sur sa liaison d'accès, la passerelle d'accès mobile DOIT identifier le nœud mobile et acquérir son MN-Identifiant. Si elle détermine que le service de gestion de la mobilité fondé sur le réseau a besoin d'être offert au nœud mobile, elle DOIT envoyer un message de mise à jour de lien de mandataire à l'ancre de mobilité locale.

2. Le message de mise à jour de lien de mandataire DOIT inclure l'option Identifiant de nœud mobile [RFC4283], portant le MN-Identifiant pour identifier le nœud mobile.

3. L'option Préfixe de réseau de rattachement DOIT être présente dans le message de mise à jour de lien de mandataire. Si la passerelle d'accès mobile apprend le ou les préfixes de réseau de rattachement du nœud mobile de sa mémorisation de politique ou par d'autres moyens, la passerelle d'accès mobile PEUT choisir de demander à l'ancre de mobilité locale d'allouer le ou les préfixes spécifiques en incluant une option Préfixe de réseau de rattachement pour chacun des préfixes demandés. La passerelle d'accès mobile PEUT aussi choisir d'inclure juste une option Préfixe de réseau de rattachement avec la valeur de préfixe de TOUT_ZÉRO, pour demander à l'ancre de mobilité locale de faire l'allocation de préfixe. Cependant, quand on inclut une option Préfixe de réseau de rattachement avec la valeur de préfixe de TOUT_ZÉRO, il DOIT y avoir seulement une instance de l'option Préfixe de réseau de rattachement dans la demande.

4. L'option Indicateur de relais DOIT être présente dans le message de mise à jour de lien de mandataire. Le champ Indicateur de relais dans l'option Indicateur de relais DOIT être réglé à la valeur indiquant le conseil de relais.
   * Le champ Indicateur de relais DOIT être réglé à une valeur de 1 (Rattachement sur une nouvelle interface) si la passerelle d'accès mobile détermine (sous réserve des considérations d'indicateur de relais spécifiées dans ce paragraphe) que le rattachement actuel du nœud mobile au réseau sur cette interface n'est pas le résultat d'un relais d'une session de mobilité existante (sur la même interface ou par une interface différente) mais résulte d'un rattachement sur une nouvelle interface. Cela sert essentiellement de demande à l'ancre de mobilité locale de créer une nouvelle session de mobilité et de ne pas mettre à jour une entrée d'antémémoire de lien existante créée pour le même nœud mobile connecté au domaine de mandataire IPv6 mobile par une interface différente.
   * Le champ Indicateur de relais DOIT être réglé à une valeur de 2 (relais entre deux interfaces différentes du nœud mobile) si la passerelle d'accès mobile sait de façon définitive que le rattachement actuel du nœud mobile est dû à un relais d'une session de mobilité existante entre deux interfaces différentes du nœud mobile.
   * Le champ Indicateur de relais DOIT être réglé à une valeur de 3 (relais entre passerelles d'accès mobile pour la même interface) si la passerelle d'accès mobile sait de façon définitive que le rattachement actuel du nœud mobile est dû au relais d'une session de mobilité existante entre deux passerelles d'accès mobile et pour la même interface du nœud mobile.
   * Le champ Indicateur de relais DOIT être réglé à une valeur de 4 (état de relais inconnu) si la passerelle d'accès mobile ne peut pas déterminer si le rattachement actuel du nœud mobile est dû à un relais d'une session de mobilité existante.

5. La passerelle d'accès mobile DOIT appliquer les considérations suivantes quand elle choisit la valeur du champ Indicateur de relais.
   * La passerelle d'accès mobile ne peut choisir d'utiliser la valeur 2 (relais entre deux interfaces différentes du nœud mobile) que quand elle sait que le nœud mobile a, délibérément, passé d'une interface à une autre, et que l'interface précédente est sur le point d'être désactivée. Elle peut savoir cela à cause d'un certain nombre de facteurs. Par exemple, la plupart des réseaux cellulaires ont des transferts intercellulaires contrôlés où le réseau sait que l'hôte passe d'un rattachement à l'autre. Dans cette situation, le mécanisme de couche de liaison peut informer les fonctions de mobilité qu'il s'agit bien d'un mouvement, et non d'un nouveau rattachement.
   * Certaines couches de liaison ont des identifiants de couche de liaison qui peuvent être utilisés pour distinguer (a) le mouvement d'une interface particulière à un nouveau rattachement de (b) le rattachement d'une nouvelle interface du même hôte. La valeur d'option 3 (relais entre passerelles d'accès mobile pour la même interface) est approprié dans le cas (a) et une valeur de 1 (rattachement sur une nouvelle interface) dans le cas (b).
   * La passerelle d'accès mobile NE DOIT PAS régler la valeur d'option à 2 (relais entre deux interfaces différentes du nœud mobile) ou 3 (relais entre passerelles d'accès mobile pour la même interface) si elle ne peut pas déterminer si le nœud mobile peut déplacer l'adresse entre les interfaces impliquées dans le transfert ou si c'est la même interface qui a bougé. Autrement, les hôtes sans capacité de mandataire IPv6 mobile qui ont plusieurs interfaces physiques au même domaine peuvent subir des défaillances inattendues.
   * Lorsque il n'existe pas de prise en charge de la part de la couche de liaison, l'hôte et le réseau vont avoir besoin de s'informer l'un l'autre du mouvement prévu. Le protocole de mandataire IPv6 mobile ne spécifie pas cela et exige simplement que la connaissance des mouvements puisse être déduite de la couche de liaison ou d'ailleurs. La méthode par laquelle cela est accompli sort du domaine d'application de la présente spécification.

6. L'option Horodatage ou Numéro de séquence valide tenue par session de mobilité de nœud mobile comme spécifié dans la [RFC3775] (si le schéma fondé sur le numéro de séquence est utilisé) DOIT être présente. Cela peut être déterminé sur la base de la valeur du fanion de configuration TimestampBasedApproachInUse *(approche fondée sur l'horodatage utilisée)*. Quand l'option Horodatage est ajoutée au message, la passerelle d'accès mobile DEVRAIT aussi régler le champ Numéro de séquence à une valeur d'un compteur à croissance monotone (tenu par chaque passerelle d'accès mobile et à ne pas confondre avec le numéro de séquence par nœud mobile spécifié dans la [RFC3775]). L'ancre de mobilité locale va ignorer ce champ quand une option Horodatage est présente dans la demande, mais va retourner la même valeur dans le message Accusé de réception de lien de mandataire. Cela va être utile pour faire correspondre la réponse au message de demande.

7. L'option Identifiant de couche de liaison de nœud mobile qui porte l'identifiant de couche de liaison de l'interface actuellement rattachée DOIT être présente dans le message de mise à jour de lien de mandataire, si la passerelle d'accès mobile en a connaissance. Si l'identifiant de couche de liaison de l'interface actuellement rattachée n'est pas connu ou si la valeur de l'identifiant est TOUT_ZÉRO, cette option NE DOIT PAS être présente.

8. L'option Type de technologie d'accès DOIT être présente dans le message de mise à jour de lien de mandataire. Le champ Type de technologie d'accès dans l'option DEVRAIT être réglé au type de la technologie d'accès par laquelle le nœud mobile est actuellement rattaché à la passerelle d'accès mobile.

9. L'option Adresse de liaison locale ne DOIT être présente dans le message de mise à jour de lien de mandataire que si la valeur de la variable de configuration FixedMAGLinkLocalAddressOnAllAccessLinks est réglée à une valeur de TOUT_ZÉRO ; autrement, l'option Adresse de liaison locale NE DOIT PAS être présente dans la demande. Les considérations du paragraphe 6.8 DOIVENT être appliquées quand on utilise l'option Adresse de liaison locale.
   * Pour demander à l'ancre de mobilité locale de fournir l'adresse de liaison locale qui devrait être utilisée sur la liaison point à point partagée avec le nœud mobile, cette option DOIT être réglée à la valeur TOUT_ZÉRO. Cela sert essentiellement de demande à l'ancre de mobilité locale de fournir l'adresse de liaison locale qui peut être utilisée sur la liaison d'accès partagée avec le nœud mobile.

10. Le message de mise à jour de lien de mandataire DOIT être construit comme spécifié au paragraphe 6.9.1.5.

11. Si il n'existe pas d'entrée de liste de mises à jour de lien pour ce nœud mobile, la passerelle d'accès mobile DOIT créer une entrée de liste de mises à jour de lien pour le nœud mobile lors de l'envoi du message de mise à jour de lien de mandataire.

6.9.1.2 Réception d'accusé de réception de lien de mandataire

À réception d'un message Accusé de réception de lien de mandataire (format spécifié au paragraphe 8.2) provenant de l'ancre de mobilité locale, la passerelle d'accès mobile DOIT traiter le message comme spécifié ci-dessous.

1. Le message Accusé de réception de lien de mandataire reçu (un message Accusé de réception de lien avec le fanion (P) réglé à la valeur de 1 DOIT être authentifié comme décrit dans la Section 4. Quand IPsec est utilisé pour l'authentification de message, le SPI dans l'en-tête IPsec [RFC4306] du paquet reçu est nécessaire pour localiser l'association de sécurité, pour authentifier le message Accusé de réception de lien de mandataire.

2. La passerelle d'accès mobile DOIT observer les règles décrites au paragraphe 9.2 de la [RFC3775] quand elle traite des en-têtes de mobilité dans le message Accusé de réception de lien de mandataire reçu.

3. La passerelle d'accès mobile DOIT appliquer les considérations spécifiées au paragraphe 5.5 pour traiter le champ Numéro de séquence et l'option Horodatage (si elle est présente) dans le message.

4. La passerelle d'accès mobile DOIT ignorer toutes les vérifications, spécifiées dans la [RFC3775], relatives à la présence d'un en-tête d'acheminement de type 2 dans le message Accusé de réception de lien de mandataire.

5. La passerelle d'accès mobile PEUT utiliser l'identifiant de nœud mobile présent dans l'option Identifiant de nœud mobile pour le confronter à la réponse aux messages de demande qui ont été envoyés récemment. Cependant, si il y a plus d'un message de demande dans sa file d'attente de demandes pour le même nœud mobile, le champ Numéro de séquence peut être utilisé pour identifier le message exact parmi ces messages. Il y a d'autres façons de réaliser cela et les mises en œuvre sont libres d'adopter la meilleure approche qui leur convient. De plus, si le message Accusé de réception de lien de mandataire reçu ne correspond à aucun message de mise à jour de lien de mandataire qu'elle a envoyé récemment, le message DOIT être ignoré.

6. Si le message Accusé de réception de lien de mandataire reçu a une ou plusieurs des options suivantes, Indicateur de relais, Type de technologie d'accès, Identifiant de couche de liaison de nœud mobile, Identifiant de nœud mobile, portant des valeurs d'option qui sont différentes des valeurs d'option présentes dans le message de demande correspondant (mise à jour de lien de mandataire) le message DOIT être ignoré car l'ancre de mobilité locale est supposée faire écho à toutes ces options mentionnées et avec les mêmes valeurs d'option dans le message de réponse. Dans ce cas, la passerelle d'accès mobile NE DOIT PAS retransmettre le message de mise à jour de lien de mandataire jusqu'à ce qu'une action administrative soit effectuée.

7. Si le message Accusé de réception de lien de mandataire reçu a la valeur du champ État réglée à PROXY_REG_NOT_ENABLED *(enregistrement de mandataire non activé pour le nœud mobile)* la passerelle d'accès mobile NE DEVRAIT PAS envoyer de message de mise à jour de lien de mandataire à nouveau pour ce nœud mobile jusqu'à ce qu'une action administrative soit effectuée. Elle DOIT refuser le service de mobilité à ce nœud mobile.

8. Si le message Accusé de réception de lien de mandataire reçu a la valeur du champ État réglée à TIMESTAMP_LOWER_THAN_PREV_ACCEPTED *(valeur d'hordatage inférieure à celle précédemment acceptée)* la passerelle d'accès mobile DEVRAIT essayer de s'enregistrer à nouveau pour réaffirmer la présence du nœud mobile sur sa liaison d'accès. La passerelle d'accès mobile n'est pas spécifiquement obligée de synchroniser son horloge à réception de ce code d'erreur.

9. Si le message Accusé de réception de lien de mandataire reçu a la valeur du champ État réglée à TIMESTAMP_MISMATCH *(valeur d'horodatage invalide)* la passerelle d'accès mobile NE DEVRAIT essayer de s'enregistrer à nouveau qu'après qu'elle a synchronisé son horloge à une source horaire commune utilisée par toutes les entités de mobilité dans ce domaine pour leur synchronisation d'horloge. La passerelle d'accès mobile NE DEVRAIT PAS synchroniser son horloge au système d'horloge de l'ancre de mobilité locale, sur la base de l'horodatage présent dans le message reçu.

10. Si le message Accusé de réception de lien de mandataire reçu a la valeur du champ État réglée à NOT_AUTHORIZED_FOR_HOME_NETWORK_PREFIX *(le nœud mobile n'est pas autorisé pour un ou plusieurs des préfixes de réseau de rattachement demandés*) la passerelle d'accès mobile NE DEVRAIT PAS demanderr encore le ou les mêmes préfixes) mais PEUT demander à l'ancre de mobilité locale de faire l'allocation du ou des prefixes en incluant seulement une option Préfixe de réseau de rattachement avec la valeur de préfixe réglée à TOUT_ZÉRO.

11. Si le message Accusé de réception de lien de mandataire reçu a la valeur du champ État réglée à toute valeur supérieure ou égale à 128 (c'est-à-dire, si le lien est rejeté) la passerelle d'accès mobile NE DOIT PAS annoncer le ou les préfixes de réseau de rattachement du nœud mobile dans les messages Annonce de routeur envoyés sur cette liaison d'accès et DOIT refuser le service de mobilité au nœud mobile en ne transmettant aucun paquet reçu du nœud mobile utilisant une adresse provenant du ou des préfixes de réseau de rattachement. Elle PEUT aussi supprimer la liaison point à point partagée avec le nœud mobile.

12. Si le message Accusé de réception de lien de mandataire reçu a la valeur du champ État réglée à 0 (mise à jour de lien de mandataire acceptée) la passerelle d'accès mobile DOIT établir un tunnel bidirectionnel à l'ancre de mobilité locale (si il n'existe pas de tunnel bidirectionnel à cette ancre de mobilité locale). Les considérations du paragraphe 5.6.1 DOIVENT être appliquées pour gérer le tunnel bidirectionnel créé dynamiquement.

13. La passerelle d'accès mobile DOIT établir le chemin pour transmettre les paquets reçus du nœud mobile en utilisant la ou les adresses provenant de son ou ses préfixes de réseau de rattachement à travers l'établissement du tunnel bidirectionnel pour ce nœud mobile. Le tunnel créé et l'état d'acheminement DOIVENT résulter en le comportement de transmission sur la passerelle d'accès mobile spécifié au paragraphe 6.10.5.

14. La passerelle d'accès mobile DOIT aussi mettre à jour l'entrée de liste de mises à jour de lien pour refléter les valeurs d'enregistrement de lien acceptées. Elle DOIT aussi annoncer le ou les préfixes de réseau de rattachement du nœud mobile comme les préfixes hébergés en liaison, en les incluant dans les messages Annonce de routeur qu'elle envoie sur cette liaison d'accès.

15. Si le message Accusé de réception de lien de mandataire reçu a l'adresse dans l'option Adresse de liaison locale réglée à une valeur NON_ZÉRO, la passerelle d'accès mobile DEVRAIT configurer cette adresse de liaison locale sur cette liaison point à point et NE DEVRAIT PAS configurer d'autre audresse de liaison locale sans effectuer une opération de DAD [RFC4862]. Cela va éviter des collisions potentielles d'ddresse de liaison locale sur cette liaison d'accès. Cependant, si l'adresse de liaison locale générée par l'ancre de mobilité locale se trouve être déjà utilisée par le nœud mobile sur cette liaison, la passerelle d'accès mobile NE DOIT PAS utiliser cette adresse, mais DEVRAIT configurer une adresse de liaison locale différente. Elle DEVRAIT aussi télécharger cette adresse de liaison locale à l'ancre de mobilité locale en envoyant immédiatement un message de mise à jour de lien de mandataire et en incluant cette adresse dans l'option Adresse de liaison locale.

6.9.1.3 Extension de la durée de vie d'un lien

1. Pour étendre la durée de vie d'un nœud mobile actuellement enregistré (c'est-à-dire, après un enregistrement initial de lien réussi sur la même passerelle d'accès mobile) la passerelle d'accès mobile peut envoyer un message de mise à jour de lien de mandataire à l'ancre de mobilité locale avec une nouvelle valeur de durée de vie. Ce message de ré-enregistrement DOIT être construit avec le même ensemble d'options que le message initial de mise à jour de lien de mandataire, sous réserve des considérations spécifiées au paragraphe 6.9.1.1. Cependant, les exceptions suivantes s'appliquent.

2. Il DOIT y avoit une option Préfixe de réseau de rattachement pour chaque préfixe de réseau de rattachement alloué pour cette session de mobilité et avec la valeur de préfixe dans l'option réglée à cette valeur de préfixe.

3. Le champ Indicateur de relais dans l'option Indicateur de relais DOIT être réglée à une valeur de 5 (état de relais inchangé - ré-enregistrsment).

6.9.1.4 Détachement de nœud mobile et désenregistrement de lien

1. Si à un moment, la passerelle d'accès mobile détecte que le nœud mobile a quitté sa liaison d'accès, ou si elle décide de mettre un terme à la session de mobilité du nœud mobile, elle DEVRAIT envoyer un message de mise à jour de lien de mandataire à l'ancre de mobilité locale avec une valeur de durée de vie de zéro. Ce message de désenregistrement DOIT être construit avec le même ensemble d'options que le message initial de mise à jour de lien de mandataire, avec les considérations spécifiées au paragraphe 6.9.1.1. Cependant, les exceptions suivantes s'appliquent.

2. Il DOIT y avoir une option Préfixe de réseau de rattachement pour chaque préfixe de réseau de rattachement alloué pour cette session de mobilité et avec les valeurs de préfixe dans l'option réglées aux valeurs de préfixe respectives.

3. Le champ Indicateur de relais dans l'option Indicateur de relais DOIT être réglé à une valeur de 4 (état de relais inconnu).

À réception d'un message Accusé de réception de lien de mandataire provenant de l'ancre de mobilité locale avec le champ État réglé à 0 (mise à jour de lien de mandataire acceptée) ou après l'attente d'une temporisation de INITIAL_BINDACK_TIMEOUT [RFC3775] pour la réponse, la passerelle d'accès mobile DOIT faire ce qui suit :

1. Elle DOIT supprimer l'entrée de liste de mises à jour de lien pour le nœud mobile de sa liste de mises à jour de lien.

2. Elle DOIT supprimer l'état d'acheminement créé pour tunneler le trafic du nœud mobile.

3. Si il y a un tunnel créé dynamiquement à l'ancre de mobilité locale du nœud mobile et si il n'y a pas d'autres nœuds mobiles pour lesquels le tunnel est utilisé, le tunnel DOIT alors être supprimé.

4. Elle DOIT supprimer la liaison point à point partagée avec le nœud mobile. Cette action va forcer le nœud mobile à supprimer toute configuration d'adresse IPv6 sur l'interface connectée à cette liaison point à point.

6.9.1.5 Construction du message de mise à jour de lien de mandataire

o La passerelle d'accès mobile, quand elle envoie le message de mise à jour de lien de mandataire à l'ancre de mobilité locale, DOIT construire le message comme spécifié ci-dessous.

```
En-tête IPv6 (src=Proxy-CoA, dst=LMAA)
  En-tête de mobilité
    - BU                          /* Les fanions P & A DOIVENT être réglés à la valeur 1 (Options de mobilité)
    - option Identifiant de nœud mobile                          (obligatoire)
    - option Préfixe de réseau de rattachement                   (obligatoire)
    - option Indicateur de relais                                (obligatoire)
    - option Type de technologie d'accès                         (obligatoire)
    - option Horodatage                                          (facultatif)
    - option Identifiant de couche de liaison de nœud mobile     (facultatif)
    - option Adresse de liaison locale                           (facultatif)
```

Figure 12 : Format de message de mise à jour de lien de mandataire

o Le champ Adresse de source dans l'en-tête IPv6 du message DOIT être réglé à l'adresse mondiale configurée sur l'interface de sortie de la passerelle d'accès mobile. Quand il n'y a pas d'option Autre adresse d'entretien présente dans la demande, cette adresse va être considérée comme la Proxy-CoA pour ce message de mise à jour de lien de mandataire. Cependant, quand il y a une option Autre adresse d'entretien présente dans la demande, cette adresse ne va pas être être considérée comme la Proxy-CoA, mais c'est l'adresse dans l'option Autre adresse d'entretien qui va être considérée comme la Proxy-CoA.
o Le champ Adresse de destination dans l'en-tête IPv6 du message DOIT réglé à l'adresse de l'ancre de mobilité locale.
o L'option Identifiant de nœud mobile [RFC4283] DOIT être présente.
o Au moins une option Préfixe de réseau de rattachement DOIT être présente.
o L'option Indicateur de relais DOIT être présente.
o L'option Type de technologie d'accès DOIT être présente.
o L'option Horodatage PEUT être présente.
o L'option Identifiant de couche de liaison de nœud mobile PEUT être présente.
o L'option Adresse de liaison locale PEUT être présente.
o Si IPsec est utilisé pour protéger les messages de signalisation, le message DOIT être protégé en utilisant l'association de sécurité existante entre l'ancre de mobilité locale et la passerelle d'accès mobile.

- o À la différence de IPv6 mobile [RFC3775], l'option Adresse de rattachement [RFC3775] NE DOIT PAS être présente dans l'en-tête d'extension Options de destination IPv6 du message de mise à jour de lien de mandataire.

6.9.2 Messages de sollicitation de routeur

Un nœud mobile peut envoyer un message Sollicitation de routeur sur la liaison d'accès partagée avec la passerelle d'accès mobile. Le message Sollicitation de routeur que le nœud mobile envoie est comme spécifié dans la [RFC4861]. La passerelle d'accès mobile, à réception du message Sollicitation de routeur ou avant d'envoyer un message Annonce de routeur, DOIT appliquer les considérations suivantes.

1. La passerelle d'accès mobile, à réception du message Sollicitation de routeur, DEVRAIT envoyer un message Annonce de routeur contenant le ou les préfixes de réseau de rattachement du nœud mobile comme préfixes en liaison. Cependant, avant d'envoyer le message Annonce de routeur contenant le ou les préfixes de réseau de rattachement du nœud mobile, elle DEVRAIT achever le processus d'enregistrement de lien avec l'ancre de mobilité locale du nœud mobile.

2. Si l'ancre de mobilité locale rejette le message de mise à jour de lien de mandataire, ou, si la passerelle d'accès mobile échoue à achever le processus d'enregistrement de lien pour une raison quelconque, la passerelle d'accès mobile NE DOIT PAS annoncer le ou les préfixes de réseau de rattachement du nœud mobile dans les messages Annonce de routeur qu'elle envoie sur la liaison d'accès. Cependant, elle PEUT choisir d'annoncer un préfixe de réseau visité local pour permettre au nœud mobile un accès IPv6 régulier.

3. La passerelle d'accès mobile DEVRAIT ajouter l'option de MTU, comme spécifié dans la [RFC4861], aux messages Annonce de routeur qu'elle envoie sur la liaison d'accès. Cela va assurer que le nœud mobile sur la liaison utilise la valeur de MTU annoncée. La valeur de MTU DEVRAIT refléter la MTU du tunnel pour le tunnel bidirectionnel entre la passerelle d'accès mobile et l'ancre de mobilité locale. Les considérations du paragraphe 6.9.5 DEVRAIENT être appliquées pour déterminer la valeur de la MTU du tunnel.

6.9.3 Routeur par défaut

Dans le protocole de mandataire IPv6 mobile, la passerelle d'accès mobile est le routeur IPv6 par défaut pour le nœud mobile sur la liaison d'accès. Cependant, lorsque le nœud mobile passe d'une liaison d'accès à l'autre, c'est la passerelle d'accès mobile de service sur ces liaisons respectives qui va envoyer les messages Annonce de routeur. Si ces annonces de routeur sont envoyées en utilisant une adresse de liaison locale différente ou une adresse de couche de liaison différente, le nœud mobile va toujours détecter un nouveau routeur par défaut après chaque relais. Pour résoudre ce problème, la présente spécification exige que toutes les passerelles d'accès mobile dans le domaine de mandataire IPv6 mobile utilisent la même adresse de liaison locale et de couche de liaison sur chaque liaison d'accès chaque fois que le nœud mobile se rattache. Ces adresses peuvent être des adresses fixes à travers le domaine de mandataire IPv6 mobile entier, et toutes les passerelles d'accès mobile peuvent utiliser ces adresses fixées globalement sur toute liaison point à point. Les variables de configuration FixedMAGLinkLocalAddressOnAllAccessLinks *(adresse de liaison locale de passerelle d'accès mobile fixe sur toutes les liaisons d'accès)* et FixedMAGLinkLayerAddressOnAllAccessLinks *(adresse de couche de liaison de passerelle d'accès mobile fixe sur toutes les liaisons d'accès)* DEVRAIENT être utilisées à cette fin. De plus, la présente spécification permet à l'ancre de mobilité locale de générer l'adresse de liaison locale et de la fournir à la passerelle d'accès mobile au titre des messages de signalisation.

Cependant, ces deux approches (une adresse de liaison locale générée par l'ancre de mobilité locale ou l'utilisation d'une adresse de liaison locale fixée mondialement) ont des implications sur le déploiement de la découverte sécurisée de voisin (SEND, *SEcure Neighbor Discovery*) [RFC3971]. Dans SEND, les routeurs ont des certificats et des paires de clés publiques, et leurs annonces de routeur sont signées avec les clés privées de ces paires de clés. Quand un certain nombre de routeurs différents utilisent les mêmes adresses, les routeurs vont tous devoir être capables de construire ces signatures pour la même paire de clé, ou la paire de clés utilisée et l'identité cryptographique du routeur doivent changer après un mouvement. Les deux approches sont problématiques. Partager les informations de clé privée entre plusieurs nœuds dans un domaine PMIP6 est une mauvaise conception du point de vue de la sécurité. Et même changer l'identité cryptographique du routeur va à l'encontre de l'idée générale que le mandataire IPv6 mobile est autant que possible invisible aux hôtes.

Il y a cependant des travaux en cours à l'IETF pour réviser les spécifications SEND. Il est suggéré que ces révisions traitent aussi le probléme ci-dessus. D'autres révisions sont nécessaires pour traiter d'autres cas problématiques (comme les mandataires de découverte de voisin) avant un large déploiement de SEND.

6.9.4 Retransmissions et limitation de taux de retransmissions

La passerelle d'accès mobile est chargée des retransmissions et de la limitation du taux des messages de mise à jour de lien de mandataire qu'elle envoie à l'ancre de mobilité locale. Les règles de retransmission et de limitation de taux sont comme spécifié dans la [RFC3775]. Cependant, les considérations suivantes DOIVENT être appliquées.

1. Quand la passerelle d'accès mobile envoie un message de mise à jour de lien de mandataire, elle devrait utiliser la constante INITIAL_BINDACK_TIMEOUT [RFC3775], pour configurer le temporisateur de retransmission, comme spécifié au paragraphe 11.8 de la [RFC3775]. Cependant, la passerelle d'accès mobile n'est pas obligée d'utiliser un plus long intervalle de retransmission de InitialBindackTimeoutFirstReg, comme spécifié dans la [RFC3775], pour le message initial de mise à jour de lien de mandataire.

2. Si la passerelle d'accès mobile échoue à recevoir une réponse correspondante valide pour un message d'enregistrement ou de ré-enregistrement dans l'intervalle de retransmission, elle DEVRAIT retransmettre le message jusqu'à ce qu'une réponse soit reçue. Cependant, la passerelle d'accès mobile DOIT s'assurer que le nœud mobile est encore rattaché à la liaison connectée avant de retransmettre le message.

3. Comme spécifié au paragraphe 11.8 de la [RFC3775], la passerelle d'accès mobile DOIT utiliser un processus de retard exponentiel dans lequel la période de temporisation est doublée à chaque retransmission, jusqu'à ce que soit le nœud reçoive une réponse, soit la période de temporisation atteigne la valeur MAX_BINDACK_TIMEOUT [RFC3775]. La passerelle d'accès mobile PEUT continuer à envoyer ces messages à ce rythme plus lent indéfiniment.

4. Si le schéma fondé sur l'hordatage est utilisé, les messages de mise à jour de lien de mandataire retransmis DOIVENT utiliser le dernier horodatage. Si le schéma de numéro de séquence est utilisé, les messages de mise à jour de lien de mandataire retransmis DOIVENT utiliser une valeur de numéro de séquence supérieure à celle utilisée pour la précédente transmission de ce message de mise à jour de lien de mandataire, comme spécifié dans la [RFC3775].

6.9.5 Découverte de la MTU de chemin

Il est important que le nœud mobile, la passerelle d'accès mobile, et l'ancre de mobilité locale aient une compréhension correcte des MTU. Quand le nœud mobile utilise la MTU correcte, il peut envoyer des paquets qui n'excèdent pas la MTU de la liaison locale et ne causent pas la fragmentation des paquets tunnelés à partir de la passerelle d'accès mobile. C'est important du point de vue de l'efficacité, ainsi que pour empêcher des problèmes de MTU difficiles à diagnostiquer. Les considérations suivantes se rapportent à la découverte de la MTU de chemin.

- L'ancre de mobilité locale et la passerelle d'accès mobile PEUVENT utiliser les mécanismes de découverte de la MTU de chemin, comme spécifié dans la [RFC1981] ou dans la [RFC4821], pour déterminer la MTU de chemin (PMTU) pour les chemins (LMA-MAG). Le mécanime spécifique de découverte à utiliser dans un déploiement donné peut être configurable.

- Les entités de mobilité DOIVENT mettre en œuvre et DEVRAIENT prendre en charge un mécanisme de découverte de la MTU de chemin fondé sur ICMP, comme spécifié dans la [RFC1981]. Cependant, ce mécanisme ne peut pas fonctionner correctement si le mandataire de réseau mobile IPv6 ne livre pas ou ne traite pas les messages ICMP "Paquet trop gros".

- Les entités de mobilité PEUVENT mettre en œuvre des mécanismes de découverte de MTU de chemin de couche de mise en paquets, comme spécifié dans la [RFC4821], et utiliser tout trafic d'application comme une charge utile pour la découverte de la PMTU. Ni le protocole de mandataire IPv6 mobile ni le tunnel entre la passerelle d'accès mobile et l'agent de mobilité local ne peuvent être facilement utilisés à cette fin. Cependant, les mises en œuvre DEVRAIENT prendre en charge au moins l'utilisation d'une demande/réponse explicite d'écho ICMP à cette fin.

- Les entités de mobilité PEUVENT choisir d'effectuer la découverte de la MTU de chemin pour tous les chemins (LMA-MAG) au moment de l'amorçage et peuvent répéter cette opération périodiquement pour s'assurer que les valeurs de la MTU de chemin n'ont pas changé pour ces chemins. Si les mécanismes de découverte dynamique de la PMTU échouent à déterminer la MTU de chemin, une valeur configurée administrativement par défaut DOIT être utilisée.

- La MTU de tunnel IPv6 pour un tunnel établi entre l'ancre de mobilité locale et la passerelle d'accès mobile DOIT être calculée sur la base de la valeur de MTU de chemin déterminée pour ce chemin spécifique et le calcul devrait être comme spécifié au paragraphe 6.7 de la [RFC2473].

- La passerelle d'accès mobile DEVRAIT utiliser la valeur de MTU de chemin de tunnel déterminée (pour le tunnel établi avec l'ancre de mobilité locale du nœud mobile) comme valeur de MTU dans l'option de MTU qu'elle envoie dans les

annonces de routeur sur la liaison d'accès partagée avec le nœud mobile. Mais, si la valeur de MTU de la liaison d'accès partagée avec le nœud mobile est inférieure à la valeur de la MTU de chemin déterminée, alors la MTU de la liaison d'accès DOIT être utilisée dans l'option de MTU.

o Si la passerelle d'accès mobile détecte un changement de la valeur de la MTU pour un des chemins (LMA-MAG) et à tout moment, la valeur de MTU correspondante du tunnel DOIT être mise à jour pour refléter le changement de valeur de MTU de chemin. La valeur ajustée de MTU de tunnel (le plus bas de la MTU de chemin et de la MTU de liaison d'accès) DEVRAIT être notifiée aux nœuds mobiles impactés en envoyant des messages Annonce de routeur supplémentaires. De plus, la valeur ajustée de MTU de tunnel DOIT aussi être utilisée dans tous les messages Annonce de routeur suivants.

6.10 Considérations d'acheminement

Ce paragraphe décrit comment la passerelle d'accès mobile traite le trafic de/vers le nœud mobile qui est rattaché à une de ses interfaces d'accès.

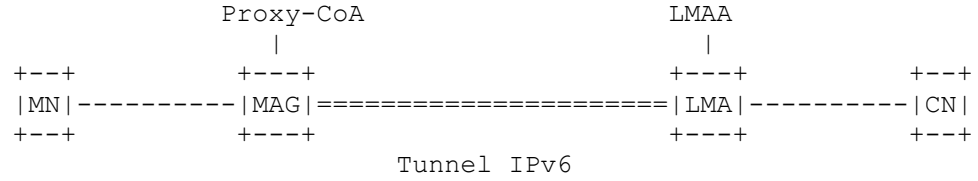


Figure 13 : Tunnel de mandataire IPv6 mobile

6.10.1 Réseau de transport

Selon la présente spécification, le réseau de transport entre l'ancre de mobilité locale et la passerelle d'accès mobile est un réseau IPv6. La [RFC5844] spécifie les extensions requises pour négocier le transport IPv4 et le mode d'encapsulation correspondant.

6.10.2 Modes de tunnelage et d'encapsulation

Une adresse IPv6 qu'un nœud mobile utilise à partir de son ou ses préfixes de réseau de rattachement est topologiquement ancrée à l'ancre de mobilité locale. Pour qu'un nœud mobile utilise cette adresse à partir d'un réseau d'accès rattaché à une passerelle d'accès mobile, des techniques de tunnelage appropriées doivent être en place. Le tunnelage cache la topologie du réseau et permet que le datagramme IPv6 du nœud mobile soit encapsulé comme une charge utile d'un autre paquet IPv6 et soit acheminé entre l'ancre de mobilité locale et la passerelle d'accès mobile. La spécification de base de IPv6 mobile [RFC3775] définit l'utilisation du tunnelage IPv6 sur IPv6 [RFC2473] entre l'agent de rattachement et le nœud mobile, et la présente spécification étend l'utilisation du même mécanisme de tunnelage à utiliser entre l'ancre de mobilité locale et la passerelle d'accès mobile.

Sur la plupart des systèmes d'exploitation, un tunnel est mis en œuvre comme une interface point à point virtuelle. Les adresses de source et de destination des deux points d'extrémité de cette interface virtuelle ainsi que le mode d'encapsulation sont spécifiés pour cette interface virtuelle. Tout paquet qui est acheminé sur cette interface est encapsulé avec l'en-tête externe comme spécifié pour cette interface de tunnel point à point.

Pour créer un tunnel point à point avec toute ancre de mobilité locale, la passerelle d'accès mobile peut mettre en œuvre une interface de tunnel avec le champ Adresse de source réglé à une adresse mondiale sur son interface de sortie (Proxy-CoA) et le champ Adresse de destination réglé à l'adresse mondiale de l'ancre de mobilité locale (LMAA).

Le mode d'encapsulation de paquet pris en charge qui peut être utilisé par la passerelle d'accès mobile et l'ancre de mobilité locale pour acheminer les datagrammes IPv6 du nœud mobile est IPv6 dans IPv6, le datagramme IPv6 est encapsulé dans un paquet IPv6 [RFC2473].

La [RFC5844] spécifie d'autres modes d'encapsulation pour prendre en charge le transport IPv4.

o IPv6 dans IPv4 - encapsulation du datagramme IPv6 dans un paquet IPv4. Les détails sur la façon de négocier ce mode sont spécifiés dans la [RFC5844].

- IPv6 dans UDP IPv4 - encapsulation du datagramme IPv6 dans un paquet UDP IPv4. Ce mode est spécifié dans la [RFC5844].

- IPv6 dans une TLV UDP IPv4 - encapsulation du datagramme IPv6 dans un paquet UDP IPv4 avec un en-tête de TLV. Ce mode est spécifié dans la [RFC5844].

6.10.3 Acheminement local

Si il y a du trafic de données entre un nœud mobile visiteur et un nœud correspondant qui est rattaché en local à une liaison d'accès connectée à la passerelle d'accès mobile, la passerelle d'accès mobile PEUT optimiser les efforts de livraision en acheminant localement les paquets et en ne leur faisant pas subir de tunnelage inverse à l'ancre de mobilité locale du nœud mobile. Le fanion EnableMAGLocalRouting *(activer l'acheminement local de MAG)* PEUT être utilisé pour contrôler ce comportement. Cependant, dans certains systèmes, cela peut avoir une implication sur la comptabilité et l'application de la politique du nœud mobile car l'ancre de mobilité locale n'est pas dans le chemin de ce trafic et ne va pas être capable d'appliquer des politiques de trafic ou de faire de comptabilité pour ces flux.

Cette décision d'optimisation de chemin DEVRAIT être fondée sur la politique configurée sur la passerelle d'accès mobile, mais appliquée par l'ancre de mobilité locale du nœud mobile. Les détails spécifiques de la façon de réaliser cela sortent du domaine d'application du présent document.

6.10.4 Gestion de tunnel

Toutes les considérations mentionnées au paragraphe 5.6.1 pour la gestion de tunnel sur l'ancre de mobilité locale s'appliquent aussi pour la passerelle d'accès mobile.

6.10.5 Règles de transmission

Transmission des paquets envoyés au réseau de rattachement du nœud mobile :

- À réception d'un paquet provenant du tunnel bidirectionnel établi avec l'ancre de mobilité locale du nœud mobile, la passerelle d'accès mobile DOIT utiliser l'adresse de destination du paquet interne pour le transmettre sur l'interface où est hébergé le préfixe du réseau de destination. La passerelle d'accès mobile DOIT retirer l'en-tête externe avant de transmettre le paquet. Les considérations de la [RFC2473] DOIVENT être appliquées pour la désencapsulation IPv6. Si la passerelle d'accès mobile ne peut pas trouver l'interface connectée pour cette adresse de destination, elle DOIT éliminer en silence le paquet. Pour rapporter une erreur dans un tel scénario, sous la forme d'un message de contrôle ICMP, les considérations de la [RFC2473] DOIVENT être appliquées.
- À réception d'un paquet provenant d'un nœud correspondant connecté à la passerelle d'accès mobile comme hôte IPv6 régulier (voir le paragraphe 6.14) destiné à un nœud mobile qui est aussi rattaché en local, la passerelle d'accès mobile DOIT vérifier le fanion EnableMAGLocalRouting pour déterminer si le paquet peut être livré directement au nœud mobile. Si il n'est pas permis à la passerelle d'accès mobile d'acheminer directement le paquet, elle DOIT acheminer le paquet vers l'ancre de mobilité locale où l'adresse de destination est topologiquement ancrée ; autrement, elle peut acheminer le paquet directement au nœud mobile.

Transmission des paquets envoyés par le nœud mobile :

- À réception d'un paquet provenant d'un nœud mobile connecté à sa liaison d'accès, la passerelle d'accès mobile DOIT s'assurer qu'il y a un lien établi pour ce nœud mobile avec son ancre de mobilité locale avant de transmettre le paquet directement à la destination ou avant de tunneler le paquet à l'ancre de mobilité locale du nœud mobile.

- À réception d'un paquet provenant d'un nœud mobile connecté à sa liaison d'accès pour une destination qui est connectée localement, la passerelle d'accès mobile DOIT vérifier le fanion EnableMAGLocalRouting pour s'assurer qu'il est permis à la passerelle d'accès mobile d'acheminer le paquet directement à la destination. Si il n'est pas permis à la passerelle d'accès mobile d'acheminer directement le paquet, elle DOIT acheminer le paquet à travers le tunnel bidirectionnel établi entre elle-même et l'ancre de mobilité locale du nœud mobile. Autrement, elle DOIT acheminer le paquet directement à la destination.

- À réception d'un paquet provenant d'un nœud mobile connecté à sa liaison d'accès, pour une destination qui n'est pas directement connectée, le paquet DOIT être transmis à l'ancre de mobilité locale à travers le tunnel bidirectionnel établi entre elle-même et l'ancre de mobilité locale du nœud mobile. Cependant, les paquets qui sont envoyés avec l'adresse de source de liaison locale NE DOIVENT PAS être tranmis.

- Le format du paquet tunnelé est montré ci-dessous. Les considérations de la [RFC2473] DOIVENT être appliquées pour l'encapsulation IPv6. Cependant, quand on utilise un transport IPv4, le format du paquet tunnelé est comme décrit dans la [RFC5844].

```
en-tête IPv6 (src= Proxy-CoA, dst= LMAA        /* en-tête de tunnel */
  en-tête IPv6 (src= MN-HoA, dst= CN )         /* en-tête de paquet */
    Protocoles de couche supérieure            /* contenu de paquet*/
```

Figure 14 : Paquet tunnelé de MAG à LMA

- Le format du paquet tunnelé est montré ci-dessous, quand la protection de charge utile avec IPsec est activée pour le trafic de données du nœud mobile. Cependant, quand on utilise le transport IPv4, le format du paquet est comme décrit dans la [RFC5844].

```
en-tête IPv6 (src= Proxy-CoA, dst= LMAA        /* en-tête de tunnel */
  en-tête ESP en mode tunnel                   /* en-tête ESP */
    en-tête IPv6 (src= MN-HoA, dst= CN )       /* en-tête de paquet */
    Protocoles de couche supérieure            /* contenu de paquet*/
```

Figure 15 : Paquet tunnelé de MAG à LMA avec protection de la charge utile

6.11 Prise en charge de la configuration d'adresse fondée sur DHCP sur la liason d'accès

Ce paragraphe explique comment la prise en charge de la configuration d'adresse à états utilisant DHCP peut être activée dans un domaine de mandataire IPv6 mobile. Il identifie aussi la configuration requise dans DHCP et les infrastructures de mobilité pour prendre en charge ce mode de configuration d'adresse et les interactions de protocole entre ces deux systèmes.

- Pour prendre en charge la configuration d'adresse à états pleins en utilisant DHCP, le service d'agent de relais DHCP [RFC3315] DOIT être pris en charge sur toutes les passerelles d'accès mobile dans le domaine de mandataire IPv6 mobile. De plus, comme spécifié à la section 20 de la [RFC3315], l'agent de relais DHCP devrait être configuré à utiliser une liste d'adresses de destination, qui PEUT inclure des adresses d'envoi individuel, l'adresse de diffusion groupée Tous_les_serveurs_DHCP, ou d'autres adresses comme requis dans un déploiement donné.

- L'infrastructure DHCP doit être configurée à allouer des adresses provenant de chaque préfixe alloué à une liaison dans ce domaine de mandataire IPv6 mobile. L'agent de relais DHCP indique la liaison à laquelle le nœud mobile est rattaché en incluant une adresse IPv6 provenant d'un des préfixes alloués à cette liaison dans le champ Adresse de liaison du message Relais de transmission. Donc, pour chaque liaison dans le domaine IPv6 mobile, l'infrastructure DHCP va :
  * être configurée avec une liste de tous les préfixes associés à cette liaison ;
  * identifier la liaison à laquelle le nœud mobile est rattaché en cherchant le préfixe pour le champ Adresse de liaison dans le message Relais de transmission dans la liste des préfixes associés à chaque liaison ;
  * allouer à l'hôte une adresse provenant de chaque préfixe associé à la liaison à laquelle le nœud mobile est rattaché.

  Cette exigence de configuration d'infrastructure DHCP est identique aux autres réseaux IPv6 ; à part de recevoir des messages DHCP d'un nœud mobile par différents agents de relais (MAG) au fil du temps, l'infrastructure DHCP ne va pas connaître les capacités du nœud mobile par rapport à la prise en charge de la mobilité.

- L'ancre de mobilité locale a besoin d'avoir la même connaissance par rapport aux liaisons ainsi que les préfixes associés dans un domaine de mandataire IPv6 mobile. Quand une ancre de mobilité locale alloue un ou des préfixes à un nœud mobile, elle DOIT allouer tous les préfixes associés à une certaine liaison et tous ces préfixes alloués vont rester comme préfixes de réseau de rattachement pour ce nœud mobile pendant toute la vie de cette session de mobilité. La passerelle d'accès mobile desservante qui héberge ces préfixes est physiqsuement connectée à cette liaison et peut fonctionner comme agent de relais DHCP. Cette compréhension commune entre DHCP et entités de mobilité sur toutes les liaisons dans le domaine ainsi que les préfixes associés fournit la coordination requise pour permettre aux entités de mobilité d'effectuer dynamiquement l'allocation de préfixes à un nœud mobile et permet quand même à l'infrastructure DHCP d'effectuer l'allocation d'adresse pour ce nœud mobile seulement à partir de ses préfixes de réseau de rattachement.

- Quand un nœud mobile envoie un message de demande DHCP, la fonction d'agent de relais DHCP sur la passerelle d'accès mobile va régler le champ Adresse de liaison dans le message DHCP à une adresse dans le préfixe de réseau de rattachement du nœud mobile (un quelconque des préfixes de réseau de rattachement du nœud mobile alloué à l'interface rattachée du nœud mobile). La passerelle d'accès mobile peut générer une autoconfiguration d'adresse à partir d'un des préfixes de réseau de rattachement du nœud mobile [RFC4862] et peut utiliser cette option d'adresse de liaison,

pour fournir une indication au serveur DHCP pour l'identification de la liaison. Le serveur DHCP, à réception de la demande du nœud mobile, va allouer des adresses provenant de tous les préfixes associés à cette liaison (identifiée en utilisant le champ Adresse de liaison de la demande).

- Une fois que le nœud mobile obtient une ou des adresses, passe à une différente liaison, et envoie une demande DHCP (à n'importe quel moment) pour étendre le prêt DHCP, l'agent de relais DHCP sur la nouvelle liaison va régler le champ Adresse de liaison dans le mesage DHCP Transmission de relais à un des préfixes de réseau de rattachement du nœud mobile. Le serveur DHCP identifie le client à partir de l'option Client-DUID, identifie la liaison à partir de l'option Adresse de liaison présente dans la demande, et va allouer les mêmes adresses qu'auparavant.

- Pour un fonctionnement correct du modèle de gestion de la mobilité fondée sur le réseau dans lequel l'hôte ne participe pas à la gestion de la mobilité, le nœud mobile DOIT toujours avoir alloué un ensemble identique d'adresses IPv6 sans considération de la liaison d'accès à laquelle le nœud mobile est rattaché. Par exemple, les passerelles d'accès mobile dans le domaine de mandataire IPv6 mobile devraient être configurées de telle façon que les messages DHCP provenant d'un nœud mobile soient toujours traités par le même serveur DHCP ou par un serveur du même groupe de serveurs DHCP coordonnés desservant ce domaine. La configuration d'adresse fondée sur DHCP n'est pas recommandée pour les déploiements dans lesquels l'ancre de mobilité locale et la passerelle d'accès mobile sont localisées dans des domaines administratifs différents.

6.12 Changement du numéro de préfixe du réseau de rattachement

Si le ou les préfixes de réseau de rattachement du nœud mobile sont dénumérotés ou deviennent invalides durant une session de mobilité, la passerelle d'accès mobile DOIT retirer le ou les préfixes en envoyant un message Annonce de routeur sur la liaison d'accès avec une durée de vie de préfixe de zéro pour le ou les préfixes qui sont renumérotés. Aussi, l'ancre de mobilité locale et la passerelle d'accès mobile DOIVENT supprimer l'état d'acheminement créé pour le ou les préfixes renumérotés. Cependant, les détails spécifiques de la façon dont l'ancre de mobilité locale notifie à la passerelle d'accès mobile la renumérotation du ou des préfixes de réseau de rattachement du nœud mobile sortent du domaine d'application du présent document.

6.13 Détection de détachement de nœud mobile et purge des ressources

Avant d'envoyer un message de mise à jour de lien de mandataire à l'ancre de mobilité locale pour étendre la durée de vie d'un lien existant actuellement d'un nœud mobile, la passerelle d'accès mobile DOIT s'assurer que le nœud mobile est encore rattaché à la liaison connectée en utilisant une méthode fiable. Si la passerelle d'accès mobile ne peut pas détecter de façon prévisible la présence du nœud mobile sur la liaison connectée, elle NE DOIT PAS tenter d'étendre la durée de vie de l'enregistrement du nœud mobile. De plus, dans ce scénario, la passerelle d'accès mobile DEVRAIT terminer le lien du nœud mobile par l'envoi d'un message de mise à jour de lien de mandataire à l'ancre de mobilité locale du nœud mobile avec la valeur de durée de vie réglée à 0. Elle DOIT aussi supprimer tout état local comme l'entrée de liste de mises à jour de lien créée pour ce nœud mobile.

Le mécanisme de détection spécifique de la perte d'un nœud mobile en visite sur la liaison connectée est spécifique de la liaison d'accès entre le nœud mobile et la passerelle d'accès mobile et sort du domaine d'application de ce document. Normalement, il y a divers événements spécifiques de la couche de liaison de chaque technologie d'accès dont la passerelle d'accès mobile peut dépendre pour détecter la perte du nœud. En général, la passerelle d'accès mobile peut dépendre d'une ou plusieurs des méthodes suivantes pour la détection de la présence du nœud mobile sur la liaison connectée :

- événement de couche de liaison spécifique de la technologie d'accès,
- événement de terminaison de session sur les types de liaison point à point,
- événement de détection d'inacessibilité de voisin IPv6 à partir de la pile IPv6,
- événement de notification par l'ancre de mobilité locale.

6.14 Permettre l'accès au réseau aux autres nœuds IPv6

Dans certains déploiements de mandataire IPv6 mobile, les opérateurs de réseau peuvent provisionner la passerelle d'accès mobile à n'offrir le service de gestion de la mobilité fondée sur le réseau service qu'à certains nœuds mobiles visiteurs et ne permettre que l'accès IP régulier à d'autres. Cela exige que le réseau ait le contrôle de quand il permet le service de gestion de la mobilité fondée sur le réseau à un nœud mobile et quand il active l'accès IPv6 régulier. La présente spécification n'interdit pas une telle configuration.

Après avoir détecté un nœud mobile sur sa liaison d'accès et après les considérations de politique, la passerelle d'accès mobile DOIT déterminer si le service de gestion de la mobilité fondée sur le réseau devrait être offert à ce nœud mobile. Si le nœud mobile est justiciable du service de gestion de la mobilité fondée sur le réseau, alors la passerelle d'accès mobile

doit s'assurer que le nœud mobile ne détecte aucun changement par rapport à son rattachement de couche 3, comme expliqué dans diverses sections de la présente spécification.

Si le nœud mobile n'est pas justiciable du service de gestion de la mobilité fondée sur le réseau, comme déterminé à partir des considérations de politique, la passerelle d'accès mobile PEUT choisir d'offrir l'accès IPv6 régulier au nœud mobile, et dans ce scénario, les considérations normales d'IPv6 s'appliquent. Si l'accès IPv6 est activé, le nœud mobile DEVRAIT être capable d'obtenir la ou les adresses IPv6 en utilisant les procédures normales de configuration d'adresse IPv6. La ou les adresses obtenues doivent provenir d'un ou de préfixes de réseau visité local. Cela assure essentiellement que la passerelle d'accès mobile fonctionne comme un routeur d'accès normal à un nœud mobile rattaché à sa liaison d'accès et sans impacter son fonctionnement de protocole de mobilité fondé sur l'hôte.

7. Fonctionnement du nœud mobile

Cette section non normative explique le fonctionnement du nœud mobile dans un domaine de mandataire IPv6 mobile.

7.1 Passage dans un domaine IPv6 de mandataire mobile

Quand un nœud mobile entre dans un domaine de mandataire IPv6 mobile et se rattache à un réseau d'accès, la passerelle d'accès mobile sur la liaison d'accès détecte le rattachement du nœud mobile et complète l'enregistrement de lien avec l'ancre de mobilité locale du nœud mobile. Si l'opération de mise à jour de lien est effectuée avec succès, la passerelle d'accès mobile va créer l'état requis et établir la transmission pour le trafic de données du nœud mobile.

Quand un nœud mobile se rattache à la liaison d'accès, il va normalement envoyer un message Sollicitation de routeur [RFC4861]. La passerelle d'accès mobile sur la liaison d'accès va répondre au message Sollicitation de routeur avec un message Annonce de routeur. Le message Annonce de routeur va porter le ou les préfixes de réseau de rattachement du nœud mobile, l'adresse du routeur par défaut, et les autres paramètres de configuration d'adresse.

Si la passerelle d'accès mobile sur la liaison d'accès reçoit un message Sollicitation de routeur du nœud mobile, avant qu'elle ait achevé la signalisation avec l'ancre de mobilité locale du nœud mobile, la passerelle d'accès mobile ne peut pas connaître le ou les préfixes de réseau de rattachement du nœud mobile et ne peut pas être capable d'émuler la liaison de rattachement du nœud mobile sur la liaison d'accès. Dans ce scénario, le nœud mobile peut remarquer un délai avant qu'il reçoive un message Annonce de routeur. Cela va aussi affecter les nœuds mobiles qui seraient capables de traiter leur propre mobilité, ou les nœuds mobiles qui n'ont pas besoin de conserver la même adresse IP à travers leurs mouvements.

Si le message Annonce de routeur reçu a le fanion Configuration d'adresse gérée établi, le nœud mobile, comme il le ferait normalement, va envoyer une demande DHCP [RFC3315]. Le service de relais DHCP activé sur cette liaison d'accès va s'assurer que le nœud mobile peut obtenir une ou plusieurs adresses provenant de son ou ses préfixes de réseau de rattachement.

Si le message Annonce de routeur reçu n'a pas le fanion Configuration d'adresse gérée établi et si il est permis au nœud mobile d'utiliser des adresses autoconfigurées, le nœud mobile va être capable d'obtenir une ou des adresses IPv6 de chacun de ses préfixes de réseau de rattachement en utilisant un des mécanismes standard de configuration d'adresse IPv6 permis pour ce mode.

Si le nœud mobile est à capacité IPv4 et si le réseau le permet, il va être capable d'obtenir la configuration d'adresse IPv4, comme spécifié dans la [RFC5844].

Une fois achevée la configuration d'adresse, le nœud mobile peut continuer d'utiliser cette configuration d'adresse tant qu'il est rattaché au réseau qui est dans la portée de ce domaine de mandataire IPv6 mobile.

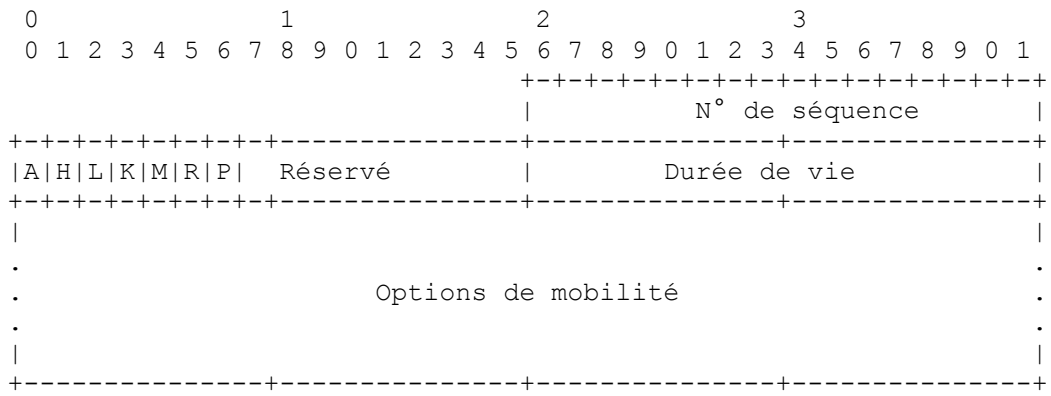
7.2 Itinérance dans le domaine de mandataire IPv6 mobile

Après avoir obtenu la configuration d'adresse dans le domaine de mandataire IPv6 mobile, lorsque le nœud mobile se déplace et change son point de rattachement d'une passerelle d'accès mobile à une autre, il peut continuer d'utiliser la même configuration d'adresse. Tant que la liaison d'accès rattachée est dans la portée de ce domaine de mandataire IPv6 mobile, le nœud mobile va toujours détecter le même routeur qui s'annonce comme routeur par défaut et qui annonce le ou les préfixes de réseau de rattachement du nœud mobile sur chaque liaison connectée. Si le nœud mobile a la configuration d'adresse qu'il a obtenue en utilisant DHCP, il va être capable de conserver la configuration d'adresse et d'étendre la durée de vie de prêt.

8. Formats de message

Cette section définit les extensions aux messages de protocole IPv6 mobile [RFC3775].

8.1 Message de mise à jour de lien de mandataire



Un message Mise à jour de lien qui est envoyé par une passerelle d'accès mobile à une ancre de mobilité locale est appelé un message de "mise à jour de lien de mandataire". Un nouveau fanion (P) est inclus dans le message Mise à jour de lien. Le reste du format du message Mise à jour de lien est le même que défini dans la [RFC3775] et avec les fanions supplémentaires (R) et (M) comme spécifié respectivement dans les [RFC3963] et [RFC4140].

Fanion Enregistrement de mandataire (P) : un nouveau fanion (P) est inclus dans le message Mise à jour de lien pour indiquer à l'ancre de mobilité locale que le message Mise à jour de lien est un enregistrement de mandataire. Le fanion DOIT être réglé à la valeur 1 pour les enregistrements de mandataire et DOIT être réglé à 0 pour les enregistrements directs envoyés par un nœud mobile.

Options de mobilité : champ de longueur variable tel que l'en-tête de mobilité complet soit un multiple entier de 8 octets. Ce champ contient zéro, une ou plusieurs options de mobilité codées en TLV. Le codage et le format des options définies sont décrits au paragraphe 6.2 de la [RFC3775]. L'ancre de mobilité locale DOIT ignorer et sauter toute option qu'elle ne comprend pas.

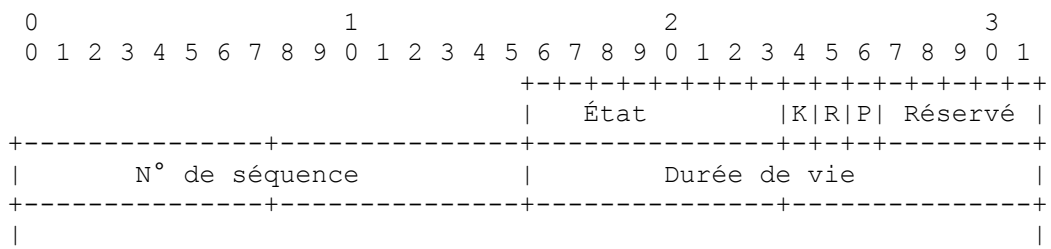
Selon la présente spécification, les options de mobilité suivantes sont valides dans un message de mise à jour de lien de mandataire. Ces options peuvent être présentes dans le message dans n'importe quel ordre. Il peut y avoir une ou plusieurs instances de l'option Préfixe de réseau de rattachement présentes dans le message. Cependant, il ne peut pas y avoir plus d'une instance d'une des options suivantes :

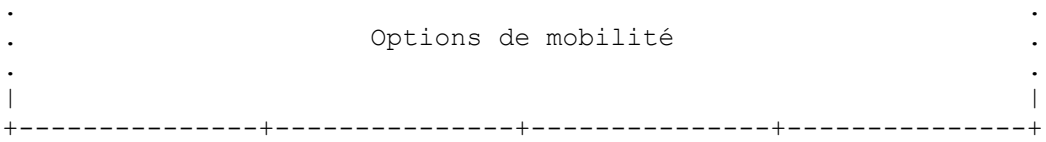
- option Identifiant de nœud mobile
- option Indicateur de relais
- option Type de technologie d'accès
- option Horodatage
- option Identifiant de couche de liaison de nœud mobile
- option Adresse de liaison locale

De plus, il peut y avoir une ou plusieurs instances de l'option Mobilité spécifique du fabricant [RFC5094].

Pour la description des autres champs présents dans ce message, se reporter au paragraphe 6.1.7 de la [RFC3775].

8.2 Message Accusé de réception de lien de mandataire





Un message Accusé de réception de lien qui est envoyé par une ancre de mobilité locale à une passerelle d'accès mobile est appelé un message "Accusé de réception de lien de mandataire". Un nouveau fanion (P) est inclus dans le message Accusé de réception de lien. Le reste du format de message Accusé de réception de lien reste le même que défini dans la [RFC3775] et avec le fanion supplémentaire (R) comme spécifié dans la [RFC3963].

Fanion Enregistrement de mandataire (P) : un nouveau fanion (P) est inclus dans le message Accusé de réception de lien pour indiquer que l'ancre de mobilité locale qui a traité le message correspondant de mise à jour de lien de mandataire prend en charge les enregistrements de mandataires. Le fanion n'est réglé à une valeur de 1 que si la mise à jour de lien de mandataire correspondante avait le fanion Enregistrement de mandataire (P) réglé à 1.

Options de mobilité : champ de longueur variable tel que la longueur de l'en-tête de mobilité complet soit un entier multiple de 8 octets. Ce champ contient zéro, une, ou plusieurs options de mobilité codées en TLV. Le codage et le format des options définis sont décrits au paragraphe 6.2 de la [RFC3775]. La passerelle d'accès mobile DOIT ignorer et sauter toutes les options qu'elle ne comprend pas.

Selon la présente spécification, les options de mobilité suivantes sont valides dans un message Accusé de réception de lien de mandataire. Ces options peuvent être présentes dans le message dans n'importe quel ordre. Il peut y avoir une ou plusieurs instances de l'option Préfixe de réseau de rattachement présentes dans le message. Cependant, il ne peut pas y avoir plus d'une instance d'une des options suivantes :

- option Identifiant de nœud mobile
- option Indicateur de relais
- option Type de technologie d'accès
- option Horodatage
- option Identifiant de couche de liaison de nœud mobile
- option Adresse de liaison locale

De plus, il peut y avoir une ou plusieurs instances de l'option de mobilité spécifique du fabricant [RFC5094].

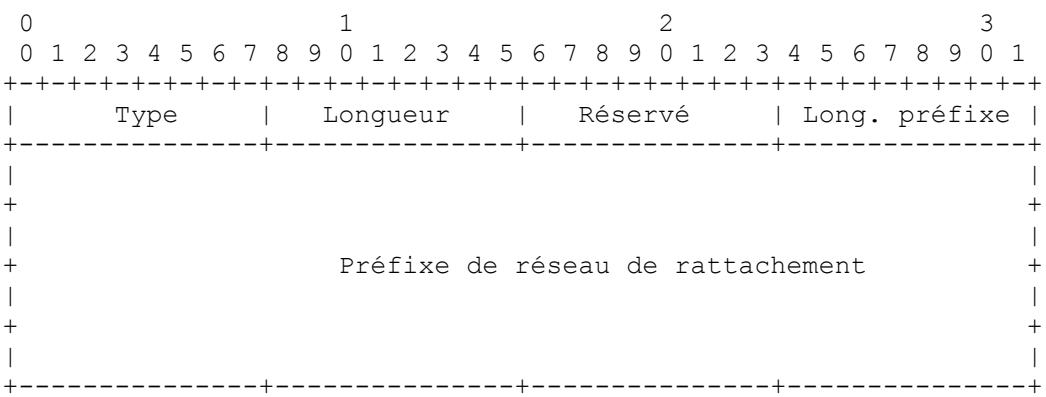
État : entier non signé de 8 bits indiquant la disposition de la mise à jour de lien de mandataire. Les valeurs du champ État de moins de 128 indiquent que la mise à jour de lien de mandataire a été acceptée par l'ancre de mobilité locale. Les valeurs supérieures ou égales à 128 indiquent que le message de mise à jour de lien de mandataire a été rejeté par l'ancre de mobilité locale. Le paragraphe 8.9 définit les valeurs d'état qui peuvent être utilisées dans le message Accusé de réception de lien de mandataire.

Pour la description des autres champs présents dans ce message, se reporter au paragraphe 6.1.8 de la [RFC3775].

8.3 Option Préfixe de réseau de rattachement

Une nouvelle option, l'option Préfixe de réseau de rattachement est définie pour être utilisée avec les messages Mise à jour de lien de mandataire et Accusé de réception de lien de mandataire échangés entre une ancre de mobilité locale et une passerelle d'accès mobile. Cette option est utilisée pour échanger les informations de préfixe de réseau de rattachement du nœud mobile. Il peut y avoir plusieurs options Préfixe de réseau de rattachement présentes dans le message.

L'option Préfixe de réseau de rattachement a une exigence d'alignement de 8n+4. Son format est comme suit :



Type : 22

Longueur : entier non signé de 8 bits indiquant la longueur de l'option en octets, sans compter les champs Type et Longueur. Ce champ DOIT être réglé à 18.

Réservé : ce champ de 8 bits n'est pas utilisé actuellement. La valeur DOIT être initialisée à 0 par l'envoyeur et DOIT être ignorée par le receveur.

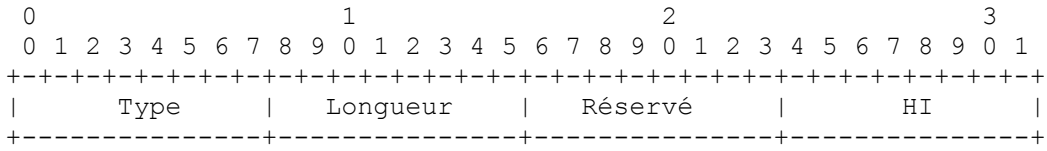
Longueur de préfixe : entier non signé de 8 bits indiquant la longueur du préfixe IPv6 contenu dans l'option.

Préfixe de réseau de rattachement : champ de seize octets contenant le préfixe de réseau de rattachement IPv6 du nœud mobile.

8.4 Option Indicateur de relais

Une nouvelle option, l'option Indicateur de relais est définie pour être utilisée avec les messages Mise à jour de lien de mandataire et Accusé de réception de lien de mandataire échangés entre une ancre de mobilité locale et une passerelle d'accès mobile. Cette option est utilisée pour échanger les indications relatives au relais du nœud mobile.

L'option Indicateur de relais n'a pas d'exigence d'alignement. Son format est comme suit :



Type : 23

Longueur : entier non signé de 8 bits indiquant la longueur de l'option en octets, sans compter les champs Type et Longueur. Ce champ DOIT être réglé à 2.

Réservé : ce champ de 8 bits n'est pas utilisé pour l'instant. Sa valeur DOIT être initialisée à 0 par l'envoyeur et DOIT être ignorée par le receveur.

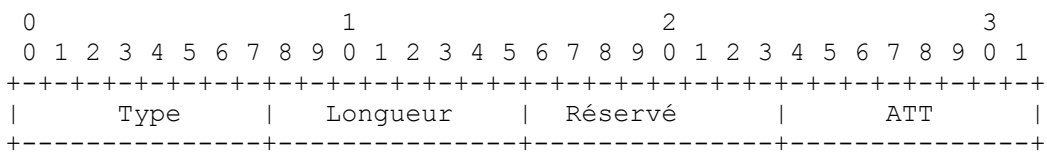
Indicateur de relais (HI, *Handoff Indicator*) : champ de 8 bits qui spécifie le type de relais. Les valeurs (0 - 255) vont être allouées et gérées par l'IANA. Les valeurs suivantes sont actuellement définies :

0 : Réservé
1 : Rattachement sur une nouvelle interface
2 : Relais entre deux interfaces différentes du nœud mobile
3 : Relais entre passerelles d'accès mobile pour la même interface
4 : État de relais inconnu
5 : État de relais non changé (ré-enregistrement)

8.5 Option Type de technologie d'accès

Une nouvelle option, l'option Type de technologie d'accès (ATT, *Access Technology Type*) est définie pour être utilisée avec les messages Mise à jour de lien de mandataire et Accusé de réception de lien de mandataire échangés entre une ancre de mobilité locale et une passerelle d'accès mobile. Cette option est utilisée pour échanger le type de la technologie d'accès par laquelle le nœud mobile est actuellement rattaché à la passerelle d'accès mobile.

L'option Type de technologie d'accès n'a pas d'exigence d'alignement. Son format est le suivant :



Type : 24

Longueur : entier non signé de 8 bits indiquant la longueur de l'option en octets, sans compter les champs Type et Longueur. Ce champ DOIT être réglé à 2.

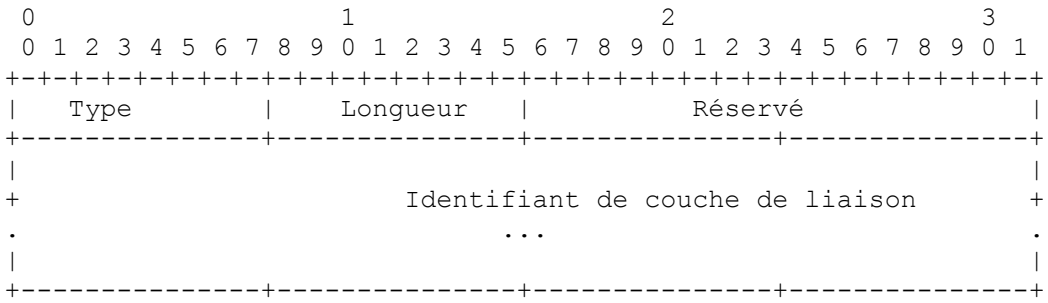
Réservé : ce champ de 8 bits n'est pas utilisé pour l'instant. La valeur DOIT être initialisée à 0 par l'envoyeur et DOIT être ignorée par le receveur.

Type de technologie d'accès : champ de 8 bits qui spécifie la technologie d'accès par laquelle le nœud mobile est connecté à la liaison d'accès sur la passerelle d'accès mobile.
Les valeurs (0 à 255) vont être allouées et gérées par l'IANA. Les valeurs suivantes sont actuellement réservées pour les types de technologie d'accès spécifiés ci-dessous :
0 : Réservé
1 : Virtuel ("Interface de réseau logique")
2 : PPP ("Protocole point à point")
3 : IEEE 802.3 ("Ethernet")
4 : IEEE 802.11a/b/g ("LAN sans fil")
5 : IEEE 802.16e ("WIMAX")

8.6 Option Identifiant de couche de liaison de nœud mobile

Une nouvelle option, l'option Identifiant de couche de liaison de nœud mobile est définie pour être utilisée avec les messages Mise à jour de lien de mandataire et Accusé de réception de lien de mandataire échangés entre une ancre de mobilité locale et une passerelle d'accès mobile. Cette option est utilisée pour échanger l'identifiant de couche de liaison de nœud mobile.

Le format de l'option Identifiant de couche de liaison est montré ci-dessous. Sur la base de la taille de l'identifiant, l'option DOIT être alignée de façon appropriée, selon les exigences d'alignement de l'option de mobilité spécifiées dans la [RFC3775].



Type : 25

Longueur : entier non signé de 8 bits indiquant la longueur de l'option en octets, sans compter les champs Type et Longueur.

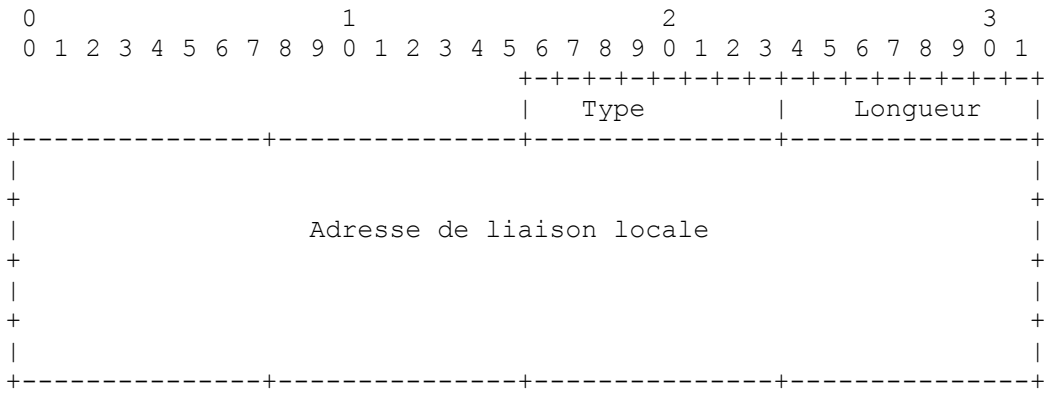
Réservé : ce champ n'est pas utilisé pour l'instant. La valeur DOIT être initialisée à 0 par l'envoyeur et DOIT être ignorée par le receveur.

Identifiant de couche de liaison : champ de longueur variable contenant l'identifiant de couche de liaison du nœud mobile. Le contenu et le format de ce champ (incluant l'ordre des octets et des bits) est comme spécifié au paragraphe 4.6 de la [RFC4861] pour porter les adresses de couche de liaison. Sur certaines liaisons d'accès, où l'adresse de couche de liaison n'est pas utilisée ou ne peut pas être déterminée, cette option peut ne pas être utilisée.

8.7 Option Adresse de liaison locale

Une nouvelle option, l'option Adresse de liaison locale est définie pour être utilisée avec les messages de mise à jour de lien de mandataire et d'accusé de réception de lien de mandataire échangés entre une ancre de mobilité locale et une passerelle d'accès mobile. Cette option est utilisée pour échanger l'adresse de liaison locale de la passerelle d'accès mobile.

L'option Adresse de liaison locale a une exigence d'alignement de 8n+6. Son format est le suivant :



Type : 26

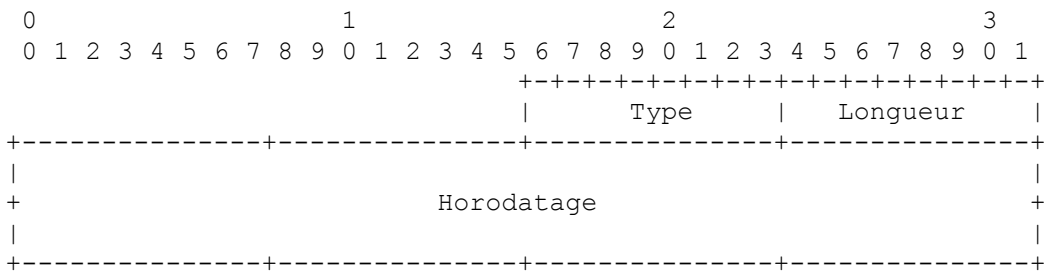
Longueur : entier non signé de 8 bits indiquant la longueur de l'option en octets, sans compter les champs Type et Longueur. Ce champ DOIT être réglé à 16.

Adresse de liaison locale : champ de seize octets contenant l'adresse de liaison locale.

8.8 Option Horodatage

Une nouvelle option, l'option Horodatage est définie pour être utilisée dans les messages Mise à jour de lien de mandataire et Accusé de réception de lien de mandataire.

L'option Horodatage a une exigence d'alignement de 8n+2. Son format est le suivant :



Type : 27

Longueur : entier non signé de 8 bits indiquant la longueur en octets de l'option, sans compter les champs Type et Longueur. La valeur de ce champ DOIT être réglée à 8.

Hordatage : champ d'entier non signé de 64 bits contenant un horodatage. La valeur indique le nombre de secondes depuis le 1er janvier 1970, 00:00 UTC, en utilisant un format de virgule fixe. Dans ce format, le nombre entier de secondes est contenu dans les 48 premiers bits du champ, et les 16 bits restants indiquent le nombre de 1/65536 fractions de seconde.

8.9 Valeurs d'état

Le présent document définit les nouvelles valeurs d'état suivantes à utiliser dans les messages Accusé de réception de lien de mandataire. Ces valeurs sont à allouer à partir du même espace de numéros, défini à la Section 6.1.8 de la [RFC3775].

Les valeurs d'état inférieures à 128 indiquent que le message de mise à jour de lien de mandataire a été accepté par l'ancre de mobilité locale. Les valeurs d'état supérieures à 128 indiquent que la mise à jour de lien de mandataire a été rejetée par l'ancre de mobilité locale.

PROXY_REG_NOT_ENABLED : 152. Enregistrement de mandataire non activé pour le nœud mobile.

NOT_LMA_FOR_THIS_MOBILE_NODE : 153. Pas d'ancre de mobilité locale pour ce nœud mobile.

MAG_NOT_AUTHORIZED_FOR_PROXY_REG : 154. La passerelle d'accès mobile n'est pas autorisée à envoyer des mises à jour de lien de mandataire.

NOT_AUTHORIZED_FOR_HOME_NETWORK_PREFIX : 155. Le nœud mobile n'est pas autorisé pour un ou plusieurs des préfixes de réseau de rattachement demandés.

TIMESTAMP_MISMATCH : 156. Valeur d'horodatage invalide (les horloges sont désynchronisées).

TIMESTAMP_LOWER_THAN_PREV_ACCEPTED : 157. La valeur d'horodatage est inférieure à la valeur acceptée précédemment.

MISSING_HOME_NETWORK_PREFIX_OPTION : 158. Option Préfixe de réseau de rattachement manquante.

BCE_PBU_PREFIX_SET_DO_NOT_MATCH : 159. Tous les préfixes de réseau de rattachement mentionnées dans le BCE ne correspondent pas à tous les préfixes de la PBU reçue.

MISSING_MN_IDENTIFIER_OPTION : 160. Option Identifiant de nœud mobile manquante.

MISSING_HANDOFF_INDICATOR_OPTION : 161. Option Indicateur de relais manquante.

MISSING_ACCESS_TECH_TYPE_OPTION : 162. Option Type de technologie d'accès manquante.

De plus, les valeurs d'état suivantes définies dans la [RFC3775] peuvent aussi être utilisées dans un message Accusé de réception de lien de mandataire :

0 Mise à jour de lien de mandataire acceptée
128 Raison non spécifiée
129 Administrativement interdit
130 Ressources insuffisantes

9. Variables de configuration du protocole

9.1 Variables de configuration d'ancre de mobilité locale

L'ancre de mobilité locale DOIT permettre à la gestion de système de gérer les variables suivantes. Les valeurs configurées pour ces variables de protocole DOIVENT survivre aux réamorçages et redémarrages du serveur.

MinDelayBeforeBCEDelete *(délai minimum avant la suppression de l'entrée d'antémémoire de lien)* : cette variable spécifie en millisecondes le temps pendant lequel l'ancre de mobilité locale DOIT attendre avant de supprimer une entrée d'antémémoire de liens d'un nœud mobile, à réception d'un message de mise à jour de lien de mandataire provenant d'une passerelle d'accès mobile avec une valeur de durée de vie de 0. Durant ce temps d'attente, si l'ancre de mobilité locale reçoit une mise à jour de lien de mandataire pour le même lien de mobilité, avec une valeur de durée de vie supérieure à 0, elle doit alors mettre à jour l'entrée d'antémémoire de lien avec les valeurs de lien acceptées. À la fin de cette période d'attente, si l'ancre de mobilité locale n'a pas reçu de message valide de mise à jour de lien de mandataire pour ce lien de mobilité, elle DOIT supprimer l'entrée d'antémémoire de lien. Ce délai assure surtout qu'une entrée d'antémémoire de liens de nœud mobile n'est pas supprimée trop vite et donne un peu de temps pour que la nouvelle passerelle d'accès mobile achève la signalisation pour le nœud mobile.
La valeur par défaut pour cette variable est 10 000 millisecondes.

MaxDelayBeforeNewBCEAssign *(délai maximum avant l'allocaion d'une nouvelle BCE)* : cette variable spécifie en millisecondes le temps pendant lequel l'ancre de mobilité locale DOIT attendre le message de désenregistrement d'une session de mobilité existante avant de décider de créer une nouvelle session de mobilité.
La valeur par défaut pour cette variable est 1 500 millisecondes.
Noter qu'il y a une relation entre cette valeur et les valeurs utilisées dans l'algorithme de retransmission des mises à jour de lien de mandataire. Les retransmissions doivent se produire avant que MaxDelayBeforeNewBCEAssign s'écoule, car autrement il y a des situations où un désenregistrement d'une passerelle d'accès mobile précédente peut être perdu, et l'ancre de mobilité locale crée inutilement une nouvelle session de mobilité et de nouveaux préfixes pour le nœud mobile. Cependant, cela affecte les situations où il n'y a pas d'informations provenant des couches inférieures sur le type d'un relais ou d'autres paramètres qui peuvent être utilisés pour identifier la session de mobilité.

TimestampValidityWindow *(fenêtre de validité de l'horodatage)* : cette variable spécifie la durée maximum de la différence en millisecondes entre l'horodatage du message de mise à jour de lien de mandataire reçu et l'heure actuelle

sur l'ancre de mobilité locale, qui est permise par l'ancre de mobilité locale pour que le message reçu soit considéré comme valide.
La valeur par défaut pour cette variable est 300 millisecondes. Cette variable doit être ajustée pour s'adapter aux déploiements.

9.2 Variables de configuration de passerelle d'accès mobile

La passerelle d'accès mobile DOIT permettre que la variable suivante soit configurée par la gestion du système. Les valeurs configurées pour cette variale de protocole DOIVENT survivre aux réamorçages du serveur et aux redémarrages de service.

EnableMAGLocalRouting *(permettre l'acheminement local de la passerelle d'accès mobile)* : ce fanion indique si il est ou non permis à la passerelle d'accès mobile d'activer l'acheminement local du trafic échangé entre un nœud mobile en visite et un nœud correspondant qui est connecté localement à une des interfaces de la passerelle d'accès mobile. Le nœud correspondant peut être aussi un autre nœud mobile en visite, ou un nœud fixe local.
La valeur par défaut pour ce fanion est réglée à une valeur de 0, indiquant que la passerelle d'accès mobile DOIT inverser le tunnel pour tout le trafic pour l'ancre de mobilité locale du nœud mobile.
Quand la valeur de ce fanion est réglée à une valeur de 1, la passerelle d'accès mobile DOIT acheminer le trafic localement.
Cet aspect d'acheminement local PEUT être défini comme la politique mobile par mobile et quand il est présent va prendre la préséance sur ce fanion.

9.3 Variables de configuration Domaine IPv6 de mandataire mobile

Toutes les entités mobiles (ancres de mobilité locales et passerelles d'accès mobile) dans un domaine de mandataire IPv6 mobile DOIVENT permettre que les variables suivantes soient configurées par la gestion du système. Les valeurs configurées pour ces variales de protocole DOIVENT survivre aux réamorçages de serveur et aux redémarrages de service. Ces variables DOIVENT être fixées globalement pour un domaine de mandataire IPv6 mobile donné résultant en les mêmes valeurs appliquées sur toutes les entités de mobilité dans ce domaine.

TimestampBasedApproachInUse *(utilisation de l'approche fondée sur l'horodatage)* : ce fanion indique si l'approche fondée sur l'horodatage pour l'ordre des messages est utilisée ou non dans ce domaine de mandataire IPv6 mobile. Quand la valeur de ce fanion est réglée à 1, toutes les passerelles d'accès mobile dans ce domaine de mandataire IPv6 mobile DOIVENT appliquer les considérations fondées sur l'horodatage mentionnées au paragraphe 5.5. Quand la valeur de ce fanion est réglée à 0, les considérations fondées sur le numéro de séquence mentionnées au paragraphe 5.5 DOIVENT être appliquées. La valeur par défaut pour ce fanion est de 1, qui indique que le mécanisme fondé sur l'horodatage est utilisé dans ce domaine de mandataire IPv6 mobile.

MobileNodeGeneratedTimestampInUse *(utilisation de l'horodatage généré par le nœud mobile)* : ce fanion indique si l'approche de l'horodatage généré par le nœud mobile est utilisée ou non dans ce domaine de mandataire IPv6 mobile. Quand la valeur de ce fanion est 1, les ancres de mobilité locales et passerelles d'accès mobile dans ce domaine de mandataire IPv6 mobile DOIVENT appliquer les considérations d'horodatage généré par le nœud mobile spécifiées au paragraphe 5.5. Ce fanion n'est pertinent que quand l'approche fondée sur l'horodatage est utilisée. La valeur de ce fanion NE DOIT PAS être réglée à 1 si la valeur du fanion TimestampBasedApproachInUse est de 0. La valeur par défaut de ce fanion est 0, qui indique que le mécanisme de l'horodatage généré par le nœud mobile n'est pas utilisé dans ce domaine de mandataire IPv6 mobile.

FixedMAGLinkLocalAddressOnAllAccessLinks *(adresse locale de lien de passerelle d'accès mobile fixe sur toutes les liaisons d'accès)* : cette variable indique la valeur de l'adresse de liaison locale que toutes les passerelles d'accès mobile DEVRAIENT utiliser sur toutes les liaisons d'accès partagées avec tous les nœuds mobiles dans ce domaine de mandataire IPv6 mobile. Si cette variable est initialisée à la valeur TOUT_ZÉRO, cela implique que l'utilisation du mode d'adresse de liaison locale fixe n'est pas activé pour ce domaine de mandataire IPv6 mobile.

FixedMAGLinkLayerAddressOnAllAccessLinks *(adresse de couche de liaison de passerelle d'accès mobile fixe sur toutes les liaisons d'accès)* : cette variable indique la valeur d'adresse de couche de liaison que toutes les passerelles d'accès mobile DEVRAIENT utiliser sur toutes les liaisons d'accès partagées avec tous les nœuds mobiles dans ce domaine de mandataire IPv6 mobile. Pour les technologies d'accès où il n'y a pas d'adresse de couche de liaison, cette variable DOIT être initialisée à la valeur TOUT_ZÉRO.

10. Considérations relatives à l'IANA

Le présent document définit six nouvelles options d'en-tête de mobilité : Préfixe de réseau de rattachement, Indicateur de relais, Type de technologie d'accès, Identifiant de couche de liaison de nœud mobile, Adresse de liaison locale, et Horodatage. Ces options sont décrites à la Section 8. La valeur de type de ces options a été allouée du même espace de numéros que pour les autres options de mobilité, comme défini dans la [RFC3775].

L'option Indicateur de relais, définie au paragraphe 8.4 de ce document, introduit un nouvel espace de numéros d'indicateur de relais (HI, *Handoff Indicator* où les valeurs de 0 à 5 ont été réservées par ce document. L'approbation de nouvelles valeurs de type d'indicateur de relais est faite par revue d'expert.

L'option Type de technologie d'accès, définie au paragraphe 8.5 de ce document, introduit un nouvel espace de numéros de type de technologie d'accès (ATT, *Access Technology Type*) où les valeurs de 0 à 5 ont été réservées par ce document. L'approbation de nouvelles valeurs de type de technologie d'accès est faite par revue d'expert.

Le présent document définit aussi de nouvelles valeurs d'état d'accusé de réception de lien, comme décrit au paragraphe 8.9. Les valeurs d'état DOIVENT être allouées dans le même espace de numéros qu'utilisé pour les valeurs d'état d'accusé de réception de lien, comme défini dans la [RFC3775]. Les valeurs allouées pour chacune de ces valeurs d'état doivent être supérieures à 128.

Le présent document crée un nouveau registre pour les fanions dans le message Mise à jour de lien appelé "Fanions de mise à jour de liens".

Les fanions suivants sont réservés :
(A) 0x8000 [RFC3775]
(H) 0x4000 [RFC3775]
(L) 0x2000 [RFC3775]
(K) 0x1000 [RFC3775]
(M) 0x0800 [RFC4140]
(R) 0x0400 [RFC3963]

Le présent document réserve un nouveau fanion (P) comme suit :

(P) 0x0200

Le reste des valeurs dans le champ de 16 bits est réservé. De nouvelles valeurs peuvent être allouées par action de normalisation ou approbation de l'IESG.

Le présent document crée aussi un nouveau registre pour les fanions du message Accusé de réception de lien appelé "Fanions d'accusé de réception de lien". Les valeurs suivantes sont réservées :
(K) 0x80 [RFC3775]
(R) 0x40 [RFC3963]

Le présent document réserve un nouveau fanion (P) comme suit : (P) 0x20

Le reste des valeurs dans le champ de 8 bits est réservé. De nouvelles valeurs peuvent être allouées par action de normalisation ou approbation de l'IESG.

11. Considérations sur la sécurité

Les menances potentielles contre la sécurité pour toute gestion du protocole de mobilité fondée sur le réseau sont décrites dans la [RFC4832]. Cette section explique comment le protocole de mandataire IPv6 mobile se défend contre ces menaces.

Le protocole de mandataire IPv6 mobile recommande que les messages de signalisation, de mise à jour de lien de mandataire et d'accusé de réception de lien de mandataire, échangés entre la passerelle d'accès mobile et l'ancre de mobilité locale soient protégés en utilisant IPsec avec l'association de sécurité établie entre elles. Cela élimine essentiellement les menaces relatives à l'usurpation d'identité de la passerelle d'accès mobile ou de l'ancre de mobilité locale.

La présente spécification permet à une passerelle d'accès mobile d'envoyer des messages d'enregistrement de lien au nom d'un nœud mobile. Si les vérifications d'autorisation appropriées ne sont pas en place, un nœud malveillant peut être

capable de capturer la session de mobilité d'un nœud mobile ou peut monter une attaque de déni de service. Pour empêcher cette attaque, la présente spécification exige que l'ancre de mobilité locale ne permette qu'aux passerelles d'accès mobile autorisées qui font partie de ce domaine de mandataire IPv6 mobile d'envoyer des messages de mise à jour de lien de mandataire au nom d'un nœud mobile.

Pour éliminer les menaces sur l'interface entre la passerelle d'accès mobile et le nœud mobile, la présente spécification exige l'établissement d'un certain niveau de confiance entre la passerelle d'accès mobile et le nœud mobile, et l'authentification et l'autorisation du nœud mobile avant qu'il lui soit permis d'accéder au réseau. De plus, les mécanismes d'authentification activés sur cette liaison d'accès vont assurer qu'il y a un lien sûr entre l'identité du nœud mobile et son adresse de couche de liaison. La passerelle d'accès mobile va identifier de façon certaine le nœud mobile à partir des paquets qu'elle reçoit sur cette liaison d'accès.

Pour traiter la menace de compromission d'une passerelle d'accès mobile, l'ancre de mobilité locale, avant d'accepter un message de mise à jour de lien de mandataire provenant d'un certain nœud mobile, peut s'assurer que le nœud mobile est rattaché à la passerelle d'accès mobile qui envoie le message de mise à jour de lien de mandataire. Cela peut être réalisé en contactant une entité de confiance, qui est capable de retracer le point de rattachement actuel du nœud mobile. Cependant, les détails spécifiques des mécanismes réels pour le faire sortent du domaine d'application de ce document.

12. Remerciements

Les auteurs tiennent à remercier tout spécialement Jari Arkko, Julien Laganier, Christian Vogt, Dave Thaler, Pasi Eronen, Pete McCann, Brian Haley, Ahmad Muhanna, JinHyeock Choi, et Elwyn Davies de leur relecture attentive de ce document.

Les auteurs remercient aussi Alex Petrescu, Alice Qinxia, Alper Yegin, Ashutosh Dutta, Behcet Sarikaya, Charles Perkins, Domagoj Premec, Fred Templin, Genadi Velev, George Tsirtsis, Gerardo Giaretta, Henrik Levkowetz, Hesham Soliman, James Kempf, Jean-Michel Combes, John Jason Brzozowski, Jun Awano, John Zhao, Jong-Hyouk Lee, Jonne Soininen, Jouni Korhonen, Kalin Getov, Kilian Weniger, Lars Eggert, Magnus Westerlund, Marco Liebsch, Mohamed Khalil, Nishida Katsutoshi, Pierrick Seite, Phil Roberts, Ralph Droms, Ryuji Wakikawa, Sangjin Jeong, Suresh Krishnan, Tero Kauppinen, Uri Blumenthal, Ved Kafle, Vidya Narayanan, Youn-Hee Han, et de nombreux autres des discussions passionnées sur la liste de diffusion du groupe de travail sur les solutions de la gestion de la mobilité localisée. Ces discussions ont beaucoup stimulé la réflexion et ont donné au document sa forme actuelle et nous les en remercions !

Les auteurs voudraient aussi remercier Ole Troan, Akiko Hattori, Parviz Yegani, Mark Grayson, Michael Hammer, Vojislav Vucetic, Jay Iyer, Tim Stammers, Bernie Volz, et Josh Littlefield de leurs apports à ce document.

13. Références

13.1 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)

[RFC2473] A. Conta, S. Deering, "Spécification du tunnelage générique de paquet dans IPv6", décembre 1998. *(P.S.)*

[RFC3168] K. Ramakrishnan et autres, "Ajout de la notification explicite d'encombrement (ECN) à IP", septembre 2001. *(P.S. ; MàJ par* RFC8311)

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

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

[RFC4282] B. Aboba et autres, "L'identifiant d'accès réseau", décembre 2005. *(P.S., Remplacée par* RFC7542)

[RFC4283] A. Patel et autres, "Option d'identifiant de nœud mobile pour IPv6 mobile (MIPv6)", novembre 2005. *(P.S.)*

[RFC4291] R. Hinden, S. Deering, "Architecture d'adressage IP version 6", février 2006. (*MàJ par* 5952 et 6052, 8064) *(D.S.)*

[RFC4301] S. Kent et K. Seo, "Architecture de sécurité pour le protocole Internet", décembre 2005. *(P.S.) (Remplace la* RFC2401)

[RFC4303] S. Kent, "Encapsulation de charge utile de sécurité dans IP (ESP)", décembre 2005. (*Remplace* RFC2406) *(P.S.)*

[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)

13.2 Références pour information

[RFC1981] J. McCann, S. Deering, J. Mogul, "Découverte de la MTU de chemin pour IP version 6", août 1996. *(D.S. ; Remplacé par* [RFC8201], STD87)

[RFC2865] C. Rigney et autres, "Service d'authentification à distance de l'utilisateur appelant (RADIUS)", juin 2000. (*MàJ par* RFC2868, RFC3575, RFC5080, RFC8044) *(D.S.)*

[RFC3588] P. Calhoun et autres, "Protocole fondé sur Diameter", septembre 2003. (*Remplacée par la* RFC6733) *(P.S.)*

[RFC3963] V. Devarapalli et autres, "Protocole de base de prise en charge de la mobilité sur le réseau (NEMO)", janvier 2005. *(P.S.)*

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

[RFC4140] H. Soliman et autres, "Gestion hiérarchisée de la mobilité dans IPv6 mobile (HMIPv6)", août 2005. (*Obsolète, voir* RFC5380) *(Expérimentale)*

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

[RFC4330] D. Mills, "Version 4 du protocole simple de l'heure du réseau (SNTP) pour IPv4, IPv6 et OSI", janvier 2006. (*Remplace* RFC2030, RFC1769) *(Information) (Remplacée par* RFC5905)

[RFC4372] F. Adrangi et autres, "Identité de l'utilisateur facturé", janvier 2006. *(P.S.)*

[RFC4821] M. Mathis, J. Heffner, "Découverte de la MTU de chemin de couche de mise en paquet", mars 2007. *(P.S.)*

[RFC4830] J. Kempf, éd., "Position des problèmes de la gestion de la mobilité localisée sur la base des réseaux (NETLMM)", avril 2007. *(Information)*

[RFC4831] J. Kempf, éd., "Objectifs de la gestion de la mobilité localisée sur la base des réseaux (NETLMM)", avril 2007. *(Info.)*

[RFC4832] C. Vogt, J. Kempf, "Menaces sur la sécurité de la gestion de la mobilité localisée sur la base des réseaux (NETLMM)" avril 2007. *(Information)*

[RFC4862] S. Thomson et autres, "Auto configuration d'adresse IPv6 sans état", septembre 2007. (*Remplace* RFC2462) *(D.S.)*

[RFC4941] T. Narten et autres, "Extensions de confidentialité pour l'auto configuration d'adresse sans état dans IPv6", septembre 2007. (*D.S. ; remplace* RFC3041 ; r*emplacée par* RFC8981*)*

[RFC5094] V. Devarapalli et autres, "Option spécifique du fabricant pour IPv6 mobile", décembre 2007. *(P.S.)*

[RFC5844] R. Wakikawa, S. Gundavelli, "Prise en charge par IPv4 du mandataire IPv6 mobile", mai 2010. *(P. S.)*

[DNAV6] Narayanan, S., ed., "Detecting Network Attachment in IPv6 Networks (DNAv6)", Travail en cours, février 2008.

Appendice A. Interactions de mandataire IPv6 mobile avec l'infrastructure AAA

Chaque nœud mobile qui visite un domaine de mandataire IPv6 mobile va normalement être identifié par un identifiant, MN-Identifiant, et cet identifiant va avoir un profil de politique associé qui identifie interface par interface le ou les préfixes de réseau de rattachement du nœud mobile, les modes de configuration d'adresse permis, la politique d'itinérance, et autres paramètres qui sont essentiels pour assurer le service de gestion de la mobilité fondée sur le réseau. Ces informations sont normalement configurées dans AAA. Dans certains cas, le ou les préfixes de réseau de rattachement peuvent être alloués dynamiquement à l'interface du nœud mobile, après son rattachement initial au domaine de mandataire IPv6 mobile sur cette interface et peuvent n'être pas configurés dans le profil de politique du nœud mobile.

Les entités du réseau dans le domaine de mandataire IPv6 mobile, tout en desservant un nœud mobile, vont avoir accès au profil de politique du nœud mobile et ces entités peuvent interroger ces informations en utilisant RADIUS [RFC2865] ou DIAMETER [RFC3588].

Appendice B. État d'acheminement

Cette section explique l'état d'acheminement créé pour un nœud mobile sur la passerelle d'accès mobile. Cet état d'acheminement reflète seulement une façon spécifique de mise en œuvre, et on PEUT choisir de le mettre en œuvre d'autres façons. Le chemin fondé sur la politique défini ci-dessous agit comme une règle de sélection de trafic pour acheminer le trafic d'un nœud mobile à travers un tunnel spécifique créé entre la passerelle d'accès mobile et l'ancre de mobilité locale de ce nœud mobile et avec le mode d'encapsulation spécifique négocié.

L'exemple ci-dessous identifie l'état d'acheminement pour deux nœuds mobiles visiteurs, MN1 et MN2, avec leurs ancres de mobilité locale respectives, LMA1 et LMA2.

Pour tout le trafic provenant du nœud mobile, identifié par l'adresse MAC du nœud mobile, l'interface d'entrée ou le préfixe de source (MN-HNP) pour _ANY_DESTINATION_ on achemine via l'interface tunnel0, au LMAA de prochain bond.

Source du paquet	**Adresse de destination**	**Interface de destination**
MAC_Address_MN1,	_ANY_DESTINATION_	Tunnel0
(préfixe IPv6 ou interface d'entrée)	Connecté en local	Tunnel0
MAC_Address_MN2,	_ANY_DESTINATION_	Tunnel1
+ (préfixe IPv6 ou interface d'entrée)	Connecté en local	direct

Exemple - Tableau de chemin fondés sur la politique

Interface	**Adresse de source**	**Adresse de destination**	**Encapsulation**
Tunnel0	Proxy-CoA	LMAA1	IPv6 dans IPv6 |
Tunnel1	Proxy-CoA	LMAA2	IPv6 dans IPv6 |

Exemple - Tableau d'interface de tunnel

Adresse des auteurs

Sri Gundavelli (éditeur)
Cisco
170 West Tasman Drive
San Jose, CA 95134
USA
mél : sgundave@cisco.com

Kent Leung
Cisco
170 West Tasman Drive
San Jose, CA 95134
USA
mél : kleung@cisco.com

Vijay Devarapalli
Wichorus
3590 North First Street
San Jose, CA 95134
USA
mél : vijay@wichorus.com

Kuntal Chowdhury
Starent Networks
30 International Place

Basavaraj Patil
Nokia
6000 Connection Drive

Tewksbury, MA
USA
mél : kchowdhury@starentnetworks.com

Irving, TX 75039
USA
mél : basavaraj.patil@nokia.com

Déclaration complète de droits de reproduction