Équipe d'ingénierie de l'Internet (IETF)
Request for Comments : 6275
RFC rendue obsolète : 3775
Catégorie : En cours de normalisation
ISSN: 2070-1721

C. Perkins, éd.,Tellabs, Inc.
D. Johnson, Rice University
J. Arkko, Ericsson
juillet 2011
Traduction Claude Brière de L'Isle

Prise en charge de la mobilité dans IPv6

Résumé
Le présent document spécifie IPv6 mobile, un protocole qui permet aux nœuds de rester accessibles tout en se déplaçant dans l'Internet IPv6. Chaque nœud mobile est toujours identifié par son adresse de rattachement, sans considération de son point de rattachement actuel à l'Internet. Bien que situé loin de son point de rattachement, un nœud mobile est toujours associé à une adresse d'entretien *(care-of address)* qui fournit des informations sur la localisation actuelle du nœud mobile. Les paquets IPv6 adressés à l'adresse de rattachement d'un nœud mobile sont acheminés de façon transparente à son adresse d'entretien. Le protocole permet aux nœuds IPv6 de mettre en antémémoire le lien entre l'adresse de rattachement *(home address)* d'un nœud mobile et son adresse d'entretien, et d'envoyer ensuite tout paquet destiné au nœud mobile directement à cette adresse d'entretien. Pour prendre cette opération en charge, IPv6 mobile définit un nouveau protocole IPv6 et une nouvelle option de destination. Tous les nœuds IPv6, qu'ils soient mobiles ou fixes, peuvent communiquer avec des nœuds mobiles. Le présent document rend obsolète la RFC 3775.

Table des matières

1. Introduction

Le présent document spécifie un protocole qui permet aux nœuds de rester accessibles tout en se déplaçant dans l'Internet IPv6. Sans prise en charge spécifique de la mobilité dans IPv6 [RFC2460], les paquets destinés à un nœud mobile ne seraient pas capables de l'atteindre lorsque le nœud mobile est hors de sa liaison de rattachement. Afin de continuer la communication en dépit de son mouvement, un nœud mobile pourrait changer son adresse IP chaque fois qu'il passe à une nouvelle liaison, mais le nœud mobile ne serait alors pas capable de conserver les connexions de couches transport et supérieures quand il change de localisation. La prise en charge de la mobilité dans IPv6 est particulièrement importante, car les ordinateurs mobiles vont probablement devenir la majorité ou au moins une fraction substantielle de la population de l'Internet pendant la durée de vie de IPv6.

Le protocole défini dans le présent document, connu comme IPv6 mobile, permet à un nœud mobile de se déplacer d'une liaison à une autre sans changer l'adresse de rattachement du nœud mobile. Les paquets peuvent être acheminés au nœud mobile en utilisant cette adresse sans considération du point de rattachement actuel du nœud mobile à l'Internet. Le nœud mobile peut aussi continuer de communiquer avec les autres nœuds (stationnaires ou mobiles) après s'être déplacé sur une nouvelle liaison. Le mouvement d'un nœud mobile hors de sa liaison de rattachement est donc transparent aux protocoles et applications de couche de transport et de couche supérieure.

Le protocole IPv6 mobile convient aussi bien pour la mobilité à travers des supports homogènes que pour la mobilité à travers des supports hétérogènes. Par exemple, IPv6 mobile facilite les mouvements d'un nœud d'un segment Ethernet à un autre aussi bien qu'il facilite les mouvements du nœud d'un segment Ethernet à une cellule de LAN sans fil, l'adresse IP du nœud mobile restant inchangée en dépit de ce mouvement.

On peut voir le protocole IPv6 mobile comme résolvant le problème de la gestion de la mobilité de la couche réseau. Certaines applications de gestion de la mobilité -- par exemple, le transfert inter-cellulaire entre des répéteurs sans fil, dont chacun ne couvre qu'une très petite zone géographique -- a été résolu en utilisant des techniques de couche de liaison. Par exemple, dans de nombreux produits de LAN sans fil actuels, les mécanismes de mobilité de couche de liaison permettent un "transfert inter cellulaire" d'un nœud mobile d'une cellule à une autre, rétablissant la connexité à la couche de liaison du nœud dans chaque nouvelle localisation.

IPv6 mobile ne tente pas de résoudre tous les problèmes généraux relatifs à l'utilisation des ordinateurs mobiles ou des réseaux sans fil. En particulier, ce protocole ne tente pas de résoudre :

- le traitement des liaisons avec une connexité unidirectionnelle ou une accessibilité partielle, comme le problème du terminal caché où un hôte est caché à seulement certains des routeurs sur la liaison ;
- le contrôle d'accès sur une liaison qui est visitée par un nœud mobile ;
- les formes locales ou hiérarchiques de gestion de la mobilité (similaires à de nombreuses solutions des gestion de mobilité actuelles de couche de liaison) ;
- l'assistance aux applications adaptatives ;
- les routeurs mobiles ;
- la découverte de service ;
- la distinction entre les paquets perdus à cause d'erreurs de bits et ceux perdus à cause de l'encombrement du réseau.

Le présent document rend obsolète la RFC 3775. Des problèmes avec le document d'origine ont été observés durant l'intégration, les essais, et le déploiement de la RFC 3775. Une liste plus détaillée des changements depuis la RFC 3775 se trouve en Appendice B.

2. Comparaison avec IP mobile pour IPv4

La conception de la prise en charge de IP mobile dans IPv6 (IPv6 mobile) bénéficie à la fois de l'expérience tirée du développement de la prise en charge de IP mobile dans IPv4 (IPv4 mobile) [RFC2003] [RFC2004] [RFC5944], et des opportunités fournies par IPv6. IPv6 mobile partage donc de nombreuses caractéristiques avec IPv4 mobile, mais est intégré dans IPv6 et offre de nombreuses autres améliorations. Cette section résume les différences majeures entre IPv4 mobile et IPv6 mobile :

- Il n'est pas besoin de déployer des routeurs spéciaux comme "agents étrangers", comme dans IPv4 mobile. IPv6 mobile fonctionne en tous lieux sans qu"aucun soutien du routeur local soit nécessaire.

- La prise en charge de l'optimisation de chemin est une partie fondamentale du protocole, plutôt qu'un ensemble non standard d'extensions.

- L'optimisation de chemin IPv6 mobile peut opérer de façon sûre même sans association de sécurité pré arrangée. Il est prévu que l'optimisation de chemin puisse être déployée à l'échelle mondiale entre tous les nœuds mobiles et les nœuds correspondants.

- La prise en charge est aussi intégrée dans IPv6 mobile pour permettre que l'optimisation de chemin coexiste efficacement avec les routeurs qui effectuent le "filtrage d'entrée" [RFC2827].

- La détection de voisin IPv6 injoignable assure une accessibilité symétrique entre le nœud mobile et son routeur par défaut dans la localisation courante.

- La plupart des paquets envoyés à un nœud mobile lorsque il est éloigné de chez lui dans IPv6 mobile sont envoyés en utilisant un en-tête d'acheminement IPv6 plutôt que l'encapsulation IP, ce qui réduit la quantité de frais généraux résultants par rapport à IPv4 mobile.

- IPv6 mobile est découplé de toute couche de liaison particulière, car il utilise la découverte de voisin IPv6 [RFC4861] au lieu du protocole de résolution d'adresse (ARP, *Address Resolution Protocol*). Cela améliore aussi la robustesse du protocole.

- L'utilisation de l'encapsulation IPv6 (et de l'en-tête d'acheminement) supprime le besoin dans IPv6 mobile de gérer un "état mou de tunnel".

- Le mécanisme de découverte dynamique d'adresse d'agent de rattachement dans IPv6 mobile retourne une seule réponse au nœud mobile. L'approche de la diffusion dirigée utilisée dans IPv4 retourne des réponses séparées de chaque agent de rattachement.

3. Terminologie

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

3.1 Termes généraux

IP : protocole Internet version 6 (IPv6).

nœud : appareil qui met en œuvre IP.

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

adresse acheminable en envoi individuel *:* identifiant pour une seule interface telle qu'un paquet qui lui est envoyé d'un autre sous réseau IPv6 est livré à l'interface identifiée par cette adresse. Par conséquent, une adresse d'acheminement en envoi individuel doit être soit une adresse IPv6 mondiale, soit une adresse IPv6 localement unique.

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

liaison : facilité ou la prise en charge de communication sur laquelle les nœuds peuvent communiquer à la couche de liaison, comme un Ethernet (simple ou ponté). Une liaison est la couche immédiatement en dessous de IP.

interface : rattachement d'un nœud à une liaison.

préfixe de sous réseau : chaîne de bits qui consiste en un certain nombre de bits initiaux d'une adresse IP.

identifiant d'interface : nombre utilisé pour identifier l'interface d'un nœud sur une liaison. L'identifiant d'interface est les bits de moindre poids restants dans l'adresse IP du nœud après le préfixe de sous réseau.

adresse de couche de liaison : identifiant de couche de liaison pour une interface, comme les adresses IEEE 802 sur les liaisons Ethernet.

paquet : un en-tête IP plus une charge utile.

association de sécurité : une association de sécurité IPsec est une relation coopérative formée par le partage de matériel de chiffrement et du contexte associé. Les associations de sécurité sont unidirectionnelles. C'est-à-dire que deux associations de sécurité sont nécessaires pour protéger le trafic bidirectionnel entre deux nœuds, une pour chaque direction.

base de données de politique de sécurité : base de données qui spécifie quels services de sécurité vont être offerts aux paquets IP et de quelle façon.

option de destination : les options de destination sont portées par l'en-tête d'extension d'options de destination IPv6. Les options de destination incluent des informations facultatives qui ne doivent être examinées que par le nœud IPv6 donné comme adresse de destination dans l'en-tête IPv6, et non par les routeurs sur le chemin. IPv6 mobile définit une nouvelle option de destination, l'option de destination Adresse de rattachement (voir au paragraphe 6.3).

en-tête d'acheminement : il peut être présent comme extension d'en-tête IPv6, et indique que la charge utile doit être livrée à une adresse de destination IPv6 d'une façon qui est différente de ce qui serait effectué par l'acheminement Internet standard. Dans le présent document, l'utilisation du terme "en-tête d'acheminement" se réfère normalement à l'utilisation d'un en-tête d'acheminement de type 2, comme spécifié au paragraphe 6.4.

"|" (enchaînement) : certaines formules de cette spécification utilisent le symbole "|" pour indiquer l'enchaînement au bit près, comme dans A | B. Cet enchaînement exige que tous les octets de l'élément de données A apparaissent d'abord dans le résultat, suivis par tous les octets de l'élément de données B.

First (taille, entrée) : certaines formules de cette spécification utilisent une forme fonctionnelle "First (taille, entrée)" pour indiquer la troncature des données d'une "entrée" afin que seuls les "taille" premiers bits restent à utiliser.

3.2 Termes d'IPv6 mobile

Ces termes sont destinées à être compatibles avec les définitions données dans la [RFC3753]. Cependant, en cas de conflit, les définitions données ici devraient être considérées comme se substituant à celles de la RFC 3753.

adresse de rattachement : adresse d'acheminement en envoi individuel allouée à un nœud mobile, utilisée comme adresse permanente du nœud mobile. Cette adresse est dans la liaison de rattachement du nœud mobile. Les mécanismes standard d'acheminement IP vont livrer les paquets destinés à l'adresse de rattachement d'un nœud mobile sur sa liaison de rattachement. Les nœuds mobiles peuvent avoir plusieurs adresses de rattachement, par exemple, quand il y a plusieurs préfixes de rattachement sur la liaison de rattachement.

préfixe de sous réseau de rattachement : préfixe de sous réseau IP correspondant à l'adresse de rattachement d'un nœud mobile.

liaison de rattachement : liaison sur laquelle est défini le préfixe de sous réseau de rattachement d'un nœud mobile.

nœud mobile : nœud qui peut changer son point de rattachement d'une liaison à une autre, tout en restant joignable via son adresse de rattachement.

mouvement : changement du point de rattachement à l'Internet d'un nœud mobile tel qu'il ne soit plus connecté à la même liaison que précédemment. Si un nœud mobile n'est pas actuellement rattaché à sa liaison de rattachement, le nœud mobile est dit être "hors de chez lui".

transfert intercellulaire de couche 2 (L2) : processus par lequel le nœud mobile passe d'une connexion de couche de liaison à une autre. Par exemple, un changement de point d'accès sans fil est un transfert intercellulaire L2.

transfert intercellulaire de couche 3 (L3) : à la suite d'un transfert intercellulaire de couche L2, un nœud mobile détecte un changement d'un préfixe de sous réseau sur la liaison qui va exiger un changement de la principale adresse d'entretien. Par exemple, un changement de routeur d'accès suite à un changement de point d'accès sans fil résulte normalement en un transfert intercellulaire de couche L3.

nœud correspondant : nœud homologue avec lequel un nœud mobile communique. Le nœud correspondant peut être mobile ou stationnaire.

préfixe de sous réseau étranger : tout préfixe de sous réseau IP autre que le préfixe du sous réseau de rattachement du nœud mobile.

liaison étrangère : toute liaison autre que la liaison de rattachement du nœud mobile.

adresse d'entretien : adresse acheminable en envoi individuel associée à un nœud mobile qui visite une liaison étrangère ; le préfixe de sous-réseau de cette adresse IP est un préfixe de sous-réseau étranger. Parmi les nombreuses adresses d'entretien qu'un nœud mobile peut avoir à un moment donné (par exemple, avec des préfixes de sous-réseau différents) celle qui est enregistrée auprès de l'agent de rattachement du nœud mobile pour une adresse de rattachement donnée est appelée son adresse d'entretien "principale".

agent de rattachement : routeur sur la liaison de rattachement du nœud mobile avec lequel le nœud mobile a enregistré son adresse d'entretien actuelle. Lorsque le nœud mobile est hors de chez lui, l'agent de rattachement intercepte les paquets sur la liaison de rattachement destinés à l'adresse de rattachement du nœud mobile, les encapsule, et les tunnelle à l'adresse d'entretien enregistrée du nœud mobile.

lien : association de l'adresse de rattachement d'un nœud mobile avec une adresse d'entretien pour ce nœud mobile, pour la durée de vie restante de cette association.

enregistrement : processus durant lequel un nœud mobile envoie une mise à jour de lien à son agent de rattachement ou à un nœud correspondant, causant l'enregistrement d'un lien pour le nœud mobile.

message de mobilité : message contenant un en-tête de mobilité (voir au paragraphe 6.1).

autorisation de lien : l'enregistrement du correspondant doit être autorisé pour permettre au receveur de croire que l'envoyeur a le droit de spécifier un nouveau lien.

procédure d'acheminement de retour : elle autorise les enregistrements par l'utilisation d'un échange de jetons cryptographiques.

enregistrement de correspondant : procédure d'acheminement de retour suivie par un enregistrement, faite entre le nœud mobile et un nœud correspondant.

enregistrement de rattachement : enregistrement entre le nœud mobile et son agent de rattachement, autorisé par l'utilisation de IPsec.

nom occasionnel : les noms occasionnels sont des nombres aléatoires utilisés en interne par le nœud correspondant pour la création de jetons de génération de clé relatifs à la procédure d'acheminement de retour. Les noms occasionnels ne sont pas spécifiques d'un nœud mobile, et sont gardés secrets dans le nœud correspondant.

indice de nom occasionnel : il est utilisé pour indiquer quels noms occasionnels ont été utilisés lors de la création de valeurs de jeton de génération de clé, sans révéler les noms occasionnels eux-mêmes.

mouchard *(cookie)* : c'est un nombre aléatoire utilisé par un nœud mobile pour empêcher de se faire mystifier par un nœud correspondant bogué dans la procédure d'acheminement de retour.

mouchard d'initiation d'entretien : mouchard envoyé par le nœud correspondant dans le message Initiation d'essai d'entretien pour être retourné dans le message Essai d'entretien.

mouchard d'initialisation de rattachement : mouchard envoyé au nœud correspondant dans le message Initiation d'essai de rattachement, pour être retourné dans le message Essai de rattachement.

jeton de génération de clé *(keygen token)* : c'est un nombre fourni par un nœud correspondant dans la procédure d'acheminement de retour pour permettre au nœud mobile de calculer la clé de gestion de lien nécessaire pour autoriser une mise à jour de lien.

jeton de génération de clé d'entretien *(care-of keygen token)* : jeton de génération de clé envoyé par le nœud correspondant dans le message Essai d'entretien.

jeton de génération de clé de rattachement *(home keygen token)* : jeton de génération de clé envoyé par le nœud correspondant dans le message Essai de rattachement.

clé de gestion de lien (Kbm, *binding management key*) : clé utilisée pour autoriser un message de gestion d'antémémoire de lien (par exemple, mise à jour de lien ou accusé de réception de lien). L'acheminement de retour donne le moyen de créer une clé de gestion de lien.

4. Vue d'ensemble d'IPv6 mobile

4.1 Fonctionnement de base

Un nœud mobile est toujours supposé être adressable à son adresse de rattachement, qu'il soit actuellement rattaché à sa liaison de rattachement ou qu'il soit hors de chez lui. Une "adresse de rattachement" est une adresse IP allouée au nœud mobile au sein de son préfixe de sous réseau de rattachement sur sa liaison de rattachement. Lorsque un nœud mobile est chez lui, les paquets adressés à son adresse de rattachement sont acheminés à la liaison de rattachement du nœud mobile, en utilisant les mécanismes conventionnels d'acheminement de l'Internet.

Lorsque un nœud mobile est rattaché à une liaison étrangère hors de chez lui, il est aussi adressable à une ou plusieurs adresses d'entretien. Une adresse d'entretien est une adresse IP associée à un nœud mobile qui a le préfixe de sous réseau d'une liaison étrangère particulière. Le nœud mobile peut acquérir son adresse d'entretien par les mécanismes conventionnels IPv6, comme une autoconfiguration sans état ou à états pleins. Tant que le nœud mobile reste dans cette localisation, les paquets adressés à cette adresse d'entretien vont être acheminés au nœud mobile. Le nœud mobile peut aussi accepter des paquets pour plusieurs adresses d'entretien, comme lorsque il est en train de se déplacer mais est encore accessible par la liaison précédente.

L'association entre l'adresse de rattachement et l'adresse d'entretien d'un nœud mobile est appelée un "lien" pour le nœud mobile. Lorsque il est hors de chez lui, un nœud mobile enregistre son adresse d'entretien principale auprès d'un routeur sur sa liaison de rattachement, demandant à ce routeur de fonctionner comme "agent de rattachement" pour le nœud mobile. Le nœud mobile effectue cet enregistrement de lien en envoyant un message de "mise à jour de lien" à l'agent de rattachement. L'agent de rattachement répond au nœud mobile en retournant un message "Accusé de réception de lien". Le fonctionnement du nœud mobile est spécifié à la Section 11, et celui de l'agent de rattachement à la Section 10.

Tout nœud qui communique avec un nœud mobile est appelé dans le présent document un "nœud correspondant" du nœud mobile, et peut lui-même être soit un nœud stationnaire, soit un nœud mobile. Les nœuds mobiles peuvent fournir des informations sur leur localisation actuelle aux nœuds correspondants. Cela se fait par l'enregistrement de correspondant. Au titre de cette procédure, un essai d'acheminement de retour est effectué afin d'autoriser l'établissement du lien. Le fonctionnement du nœud correspondant est spécifié à la Section 9.

Il y a deux modes possibles pour les communications entre le nœud mobile et un nœud correspondant. Le premier mode, tunnelage bidirectionnel, n'exige pas la prise en charge de IPv6 mobile de la part du nœud correspondant et est disponible même si le nœud mobile n'a pas enregistré son lien actuel avec le nœud correspondant. Les paquets provenant du nœud correspondant sont acheminés à l'agent de rattachement et ensuite tunnelés au nœud mobile. Les paquets pour le nœud correspondant sont tunnelés du nœud mobile à l'agent de rattachement ("tunnelage inverse") et ensuite acheminés normalement depuis le réseau de rattachement au nœud correspondant. Dans ce mode, l'agent de rattachement utilise la découverte de voisin mandataire pour intercepter tous les paquets IPv6 adressés à l'adresse de rattachement du nœud mobile (ou ses adresses de rattachement) sur la liaison de rattachement. Chaque paquet intercepté est tunnelé à l'adresse d'entretien principale du nœud mobile .Ce tunnelage est effectué en utilisant l'encapsulation IPv6 [RFC2473].

Le second mode, "optimisation de chemin", exige que le nœud mobile enregistre son lien actuel auprès du nœud correspondant. Les paquets provenant du nœud correspondant peuvent être acheminés directement à l'adresse d'entretien du nœud mobile. Quand il envoie un paquet à toute destination IPv6, le nœud correspondant vérifie dans ses liens en

antémémoire qu'il a une entrée pour l'adresse de destination du paquet. Si il trouve un lien en antémémoire pour cette adresse de destination, le nœud utilise un nouveau type d'en-tête d'acheminement IPv6 [RFC2460] (voir au paragraphe 6.4) pour acheminer le paquet au nœud mobile au moyen de l'adresse d'entretien indiquée dans ce lien.

Acheminer les paquets directement à l'adresse d'entretien du nœud mobile permet d'utiliser le plus court chemin de communication. Cela élimine aussi l'encombrement chez l'agent de rattachement et sur la liaison de rattachement du nœud mobile. De plus, l'impact de défaillances temporaires de l'agent de rattachement ou des réseaux sur le chemin de ou vers l'agent de rattachement est réduit.

Quand on achemine les paquets directement au nœud mobile, le nœud correspondant règle l'adresse de destination dans l'en-tête IPv6 à l'adresse d'entretien du nœud mobile. Un nouveau type d'en-tête d'acheminement IPv6 (voir au paragraphe 6.4) est aussi ajouté au paquet pour porter l'adresse de rattachement désirée. De même, le nœud mobile règle l'adresse de source dans l'en-tête IPv6 du paquet à ses adresses d'entretien actuelles. Le nœud mobile ajoute une nouvelle option de destination IPv6 "Adresse de rattachement" (voir le paragraphe 6.3) pour porter son adresse de rattachement. L'inclusion des adresses de rattachement dans ces paquets rend l'utilisation de l'adresse d'entretien transparente au dessus de la couche réseau (par exemple, à la couche transport).

IPv6 mobile fournit aussi la prise en charge de plusieurs agents de rattachement, et une prise en charge limitée de la reconfiguration du réseau de rattachement. Dans ce cas, le nœud mobile peut ne pas connaître l'adresse IP de son propre agent de rattachement, et même les préfixes des sous réseaux de rattachement peuvent changer dans le temps. Un mécanisme appelé "découverte dynamique d'adresse d'agent de rattachement" permet au nœud mobile de découvrir dynamiquement l'adresse IP d'un agent de rattachement sur sa liaison de rattachement, même quand le nœud mobile est hors de chez lui. Les nœuds mobiles peuvent aussi apprendre de nouvelles informations sur les préfixes de sous réseau de rattachement par le mécanisme de "découverte de préfixe mobile". Ces mécanismes sont décrits à partir du paragraphe 6.5.

Le présent document est écrit avec l'hypothèse que le nœud mobile est configuré avec le préfixe de rattachement pour que le nœud mobile soit capable de découvrir un agent de rattachement et configure une adresse de rattachement. Ce peut être une limitation dans des déploiements où l'agent de rattachement et l'adresse de rattachement pour le nœud mobile doivent être alloués de façon dynamique. Des mécanismes supplémentaires ont été spécifiés pour que le nœud mobile configure de façon dynamique un agent de rattachement, une adresse de rattachement, et le préfixe de rattachement. Ces mécanismes sont décrits dans "Amorçage IPv6 mobile dans un scénario de partage" [RFC5026] et "Amorçage de IPv6 mobile (MIPv6) pour le scénario intégré" [RFC6611].

4.2 Nouveau protocole IPv6

IPv6 mobile définit un nouveau protocole IPv6 qui utilise l'en-tête de mobilité (voir le paragraphe 6.1). Cet en-tête est utilisé pour porter les messages suivants :
Initiation d'essai de rattachement
Essai de rattachement
Initiation d'essai d'entretien
Essai d'entretien

Ces quatre messages sont utilisés pour effectuer la procédure d'acheminement de retour depuis le nœud mobile à un nœud correspondant. Cela assure l'autorisation des mises à jour de lien suivantes, comme décrit au paragraphe 5.2.5.

Mise à jour de lien : une mise à jour de lien est utilisée par un nœud mobile pour notifier à un nœud correspondant ou à l'agent de rattachement du nœud mobile son lien actuel. La mise à jour de lien envoyée à l'agent de rattachement du nœud mobile pour enregistrer son adresse d'entretien principale est marquée comme un "enregistrement de rattachement".

Accusé de réception de lien : un accusé de réception de lien est utilisé pour accuser réception d'une mise à jour de lien, si un accusé de réception était demandé dans la mise à jour de lien (par exemple, la mise à jour de lien a été envoyée à l'agent de rattachement) ou si une erreur s'est produite.

Demande de rafraîchissement de lien : une demande de rafraîchissement de lien est utilisée par un nœud correspondant pour demander qu'un nœud mobile rétablisse son lien avec le nœud correspondant. Ce message est normalement utilisé quand le lien en antémémoire est en utilisation active mais que la durée de vie du lien est proche de l'expiration. Le nœud correspondant peut utiliser, par exemple, le trafic récent et des connexions de couche transport ouvertes comme indication d'utilisation active.

Erreur de lien : l'erreur de lien est utilisée par le nœud correspondant pour signaler une erreur relative à la mobilité, comme une tentative inappropriée d'utiliser l'option Adresse de destination de rattachement sans un lien existant. Le message

Erreur de lien est aussi utilisé par l'agent de rattachement pour signaler une erreur au nœud mobile, si il reçoit un type de message En-tête de mobilité non reconnu de la part du nœud mobile.

4.3 Nouvelle option de destination IPv6

IPv6 mobile définit une nouvelle option de destination IPv6, l'option de destination Adresse de rattachement. Cette option est décrite en détail au paragraphe 6.3.

4.4 Nouveaux messages ICMP IPv6

IPv6 mobile introduit aussi quatre nouveaux types de messages ICMP, deux à utiliser dans le mécanisme de découverte dynamique d'adresse d'agent de rattachement, et deux pour les mécanismes de dénumérotage et de configuration mobile. Comme décrit aux paragraphes 10.5 et 11.4.1, les deux nouveaux types de message ICMP suivants sont utilisés pour la découverte d'adresse d'agent de rattachement :

- o Demande de découverte d'adresse d'agent de rattachement, décrit au paragraphe 6.5.
- o Réponse de découverte d'adresse d'agent de rattachement, décrit au paragraphe 6.6.

Les deux types de message suivants sont utilisés pour le dénumérotage de réseau et la configuration d'adresse sur le nœud mobile, comme décrit au paragraphe 10.6:

- o Sollicitation de préfixe mobile, décrit au paragraphe 6.7.
- o Annonce de préfixe mobile, décrit au paragraphe 6.8.

4.5 Terminologie de structure de données conceptuelles

Le présent document décrit le protocole IPv6 mobile dans les termes des structures de données conceptuelles suivants :

Antémémoire de liens : antémémoire des liens pour les autres nœuds. Cette antémémoire est tenue par les agents de rattachement et les nœuds correspondants. L'antémémoire contient les entrées des "enregistrements de correspondants" (voir au paragraphe 9.1) et des "enregistrements de rattachement" (voir au paragraphe 10.1).

Liste de mise à jour de liens : cette liste est tenue par chaque nœud mobile. La liste a un élément pour chaque lien que le nœud mobile a ou essaye d'établir avec un autre nœud spécifique. Les enregistrements de correspondants et de rattachement sont tous deux inclus dans cette liste. Les entrées de la liste sont supprimées lorsque la durée de vie du lien expire. Voir au paragraphe 11.1.

Liste des agents de rattachement : les agents de rattachement ont besoin de savoir quels autres agents de rattachement sont sur la même liaison. Cette information est mémorisée dans la liste des agents de rattachement, comme décrit plus en détails au paragraphe 10.1. La liste est utilisée pour informer les nœuds mobiles durant la découverte dynamique d'adresse d'agent de rattachement.

4.6 Adressage local univoque

La présente spécification exige que les adresses de rattachement et d'entretien DOIVENT être des adresses d'acheminement en envoi individuel. Les adresses IPv6 d'envoi individuel uniques localement (ULA, *Unique-local IPv6 unicast address*, [RFC4193]) peuvent être utilisables sur des réseaux qui utilisent de telles adresses non acheminables mondialement, mais la présente spécification ne définit pas quand un tel usage est sûr et quand il ne l'est pas. Les nœuds mobiles peuvent n'être pas capables de distinguer entre leur site de rattachement et le site auquel ils sont actuellement localisés. Cela peut rendre difficile d'empêcher un rattachement accidentel aux autres sites, parce que le nœud mobile peut utiliser la ULA à un autre site, qui ne pourrait pas être utilisé pour réussir à envoyer des paquets à l'agent de rattachement (HA, *home agent*) du nœud mobile. Il en résulterait une injoignabilité entre le nœud mobile (MN) et le HA, quand des adresses IPv6 acheminables uniques localement sont utilisées comme adresses d'entretien. De façon similaire, des CN en dehors du propre site de la MN ne sont pas accessibles quand des ULA sont utilisées comme adresses de rattachement. Donc, les adresses IPv6 d'envoi individuel uniques localement NE DEVRAIENT PAS être utilisées comme adresse de rattachement ou d'entretien quand d'autres choix d'adresses sont disponibles. Si de telles adresses sont utilisées, cependant, conformément à la [RFC4193], elles sont traitées comme toutes les adresses IPv6 mondiales en envoi individuel, donc, pour le reste de cette spécification, l'utilisation des adresses IPv6 d'envoi individuel uniques localement n'est pas différencié des autres adresses IPv6 mondialement uniques.

5. Vue d'ensemble de la sécurité d'IPv6 mobile

La présente spécification fournit un certain nombre de dispositifs de sécurité. Cela inclut la protection des mises à jour de lien avec les agents de rattachement et nœuds correspondants, la protection de la découverte de préfixe mobile, et la protection des mécanismes que IPv6 mobile utilise pour transporter les paquets de données.

Les mises à jour de lien sont protégées par l'utilisation des en-têtes d'extension IPsec, ou par l'utilisation de l'option Données d'autorisation de lien. Cette option emploie une clé de gestion de lien, Kbm, qui peut être établie par la procédure d'acheminement de retour. La découverte de préfixe mobile est protégée par l'utilisation des en-têtes d'extension IPsec. Les mécanismes relatifs au transport des paquets de charge utile -- tels que l'option de destination Adresse de rattachement et En-tête d'acheminement de type 2 -- ont été spécifiés d'une manière qui restreint leur utilisation dans les attaques.

5.1 Mise à jour des liens aux agents de rattachement

Le nœud mobile et l'agent de rattachement DOIVENT utiliser une association de sécurité IPsec pour protéger l'intégrité et l'authenticité des mises à jour de lien et de leurs accusés de réception. Les nœuds mobiles et les agents de rattachement DOIVENT prendre en charge et DEVRAIENT utiliser l'en-tête d'encapsulation de charge utile de sécurité (ESP, *Encapsulating Security Payload*) [RFC4303] en mode transport et DOIVENT utiliser un algorithme d'authentification de charge utile non NUL pour assurer l'authentification de l'origine des données, l'intégrité sans connexion, et la protection facultative anti répétition. Noter que l'en-tête d'authentification (HA, *Authentication Header*) [RFC4302] est aussi possible mais non discuté dans la présente spécification dans un souci de concision.

Afin de protéger les messages échangés entre le nœud mobile et l'agent de rattachement avec IPsec, des entrées appropriées de base de données de politique de sécurité doivent être créées. Un nœud mobile doit être empêché d'utiliser son association de sécurité pour envoyer une mise à jour de lien au nom d'un autre nœud mobile qui utilise le même agent de rattachement. Ceci DOIT être réalisé en faisant que l'agent de rattachement vérifie que l'adresse de rattachement donnée a été utilisée avec la bonne association de sécurité. Une telle vérification est fournie dans le traitement IPsec, en ayant des entrées de base de données de politique de sécurité qui identifient de façon non équivoque une seule association de sécurité pour protéger les mises à jour de lien entre toute adresse de rattachement donnée et l'agent de rattachement. Afin de rendre cela possible, il est nécessaire que l'adresse de rattachement du nœud mobile soit visible dans les mises à jour de lien et leurs accusés de réception. L'adresse de rattachement est utilisée dans ces paquets comme source ou destination, ou dans l'option de destination Adresse de rattachement ou En-tête d'acheminement de type 2.

Comme avec toutes les associations de sécurité IPsec dans la présente spécification, la configuration manuelle des associations de sécurité DOIT être prise en charge. Les secrets partagés utilisés DOIVENT être aléatoires et uniques pour les différent nœuds mobiles, et DOIVENT être distribués hors ligne aux nœuds mobiles. La gestion de clés automatique avec le protocole d'échange de clé Internet version 2 (IKEv2, *Internet Key Exchange Protocol version 2*) [RFC5996] PEUT être prise en charge comme décrit dans la [RFC4877].

Le paragraphe 11.3.2 discute la façon dont les connexions IKEv2 avec l'agent de rattachement ont besoin d'un traitement attentif des adresses utilisées pour transporter IKEv2. Ceci est nécessaire pour s'assurer qu'une mise à jour de lien n'est pas nécessaire avant l'échange IKEv2 indispensable pour sécuriser la mise à jour de lien.

Des descriptions et exemples plus détaillés d'utilisation de IPsec pour protéger les communications entre le nœud mobile et l'agent de rattachement ont été publiés dans les [RFC3776] et [RFC4877].

5.2 Mise à jour des liens aux nœuds correspondants

La protection des mises à jour de lien envoyées aux nœuds correspondants n'exige pas la configuration d'associations de sécurité ou l'existence d'une infrastructure d'authentification entre les nœuds mobiles et les nœuds correspondants. Une méthode appelée la procédure d'acheminement de retour est plutôt utilisée pour s'assurer que c'est le bon nœud mobile qui envoie le message. Cette méthode ne protège pas contre des attaquants qui sont sur le chemin entre le réseau de rattachement et le nœud correspondant. Cependant, des attaquants dans une telle situation sont capables d'effectuer les mêmes attaques mêmes sans IPv6 mobile. Le principal avantage de la procédure d'acheminement de retour est qu'elle limite les attaquants potentiels à ceux qui ont un accès à un chemin spécifique dans l'Internet, et évite des mises à jour de lien falsifiées provenant de n'importe où ailleurs dans l'Internet. Pour une explication plus en profondeur des propriétés de sécurité de la procédure d'acheminement de retour, voir la Section 15. Aussi, consulter la [RFC4225].

L'intégrité et l'authenticité des messages de mise à jour de lien adressés aux nœuds correspondants sont protégées en utilisant un algorithme de chiffrement-hachage. La clé de gestion de lien, Kbm, est utilisée pour chiffrer l'algorithme de hachage à cette fin. La Kbm est établie en utilisant les données échangées durant la procédure d'acheminement de retour. L'échange de données est réalisé par l'utilisation de clés de nœud, de noms occasionnels, de mouchards, de jetons, et de

certaines fonctions cryptographiques. Le paragraphe 5.2.5 présente les procédures de base de l'acheminement de retour. Le paragraphe 5.2.6 montre comment les résultats de cette procédure sont utilisés pour autoriser une mise à jour de lien avec un nœud correspondant.

5.2.1 Clés de nœud

Chaque nœud correspondant a une clé secrète, Kcn, appelée "clé de nœud", qu'il utilise pour produire les jetons de génération de clé (keygen) envoyés aux nœuds mobiles. La clé de nœud DOIT être un nombre aléatoire de 20 octets. La clé de nœud permet au nœud correspondant de vérifier que les jetons de génération de clé utilisés par le nœud mobile dans les autorisations de mise à jour de lien sont bien les siens. Cette clé NE DOIT PAS être partagée avec une autre entité.

Un nœud correspondant PEUT générer une clé de nœud fraîche à tout moment ; cela évite d'avoir besoin d'une mémorisation de clés persistante sûre. Les procédures pour mettre facultativement à jour la clé de nœud sont exposées au paragraphe 5.2.7.

5.2.2 Noms occasionnels

Chaque nœud correspondant génère aussi des noms occasionnels à des intervalles réguliers. Les noms occasionnels devraient être générés en utilisant un générateur de nombres aléatoires connu pour avoir de bonnes propriétés d'aléa [RFC4086]. Un nœud correspondant peut utiliser les mêmes Kcn et nom occasionnel avec tous les nœuds mobiles avec lesquels il est en communication.

Chaque nom occasionnel est identifié par un indice de nom occasionnel. Quand un nouveau nom occasionnel est généré, il doit être associé à un nouvel indice de nom occasionnel ; ceci peut être fait, par exemple, en incrémentant la valeur de l'indice de nom occasionnel précédent, si l'indice de nom occasionnel est utilisé comme pointeur dans un dispositif linéaire de noms occasionnels. Cependant, il n'est pas exigé que les noms occasionnels soient mémorisés de cette façon, ou que les valeurs des indices de nom occasionnel suivants aient de relations particulières entre eux. La valeur de l'indice est communiquée dans le protocole, afin que si un nom occasionnel est remplacé par un nouveau nom occasionnel durant le fonctionnement d'un protocole, le nœud correspondant puisse distinguer les messages qui devraient être vérifiés par rapport au vieux nom occasionnel de ceux qui devraient être vérifiés par rapport au nouveau nom occasionnel. Strictement parlant, les indices ne sont pas nécessaires dans l'authentification, mais permettent au nœud correspondant de trouver efficacement la valeur de nom occasionnel qu'il a utilisé pour créer un jeton de génération de clé.

Les nœuds correspondants conservent le nom occasionnel en cours et un petit ensemble de noms occasionnels valides antérieurs dont la durée de vie n'est pas encore expirée. Les valeurs expirées DOIVENT être éliminées, et les messages qui utilisent des indices périmés ou inconnus seront rejetés.

Les valeurs spécifiques d'indice de nom occasionnel ne peuvent pas être utilisées par les nœuds mobiles pour déterminer la validité du nom occasionnel. Les temps de validité attendus pour les valeurs de noms occasionnels et les procédures pour les mettre à jour sont exposés au paragraphe 5.2.7.

Un nom occasionnel est une chaîne d'octets de longueur quelconque. La longueur recommandée est 64 bits.

5.2.3 Mouchards et jetons

La procédure d'essai d'adresse d'acheminement de retour utilise des mouchards et des jetons de génération de clé comme valeurs opaques dans les messages respectivement d'initiation d'essai et d'essai.

- Le "mouchard initiation de rattachement" et le "mouchard d'initiation d'entretien" sont des valeurs de 64 bits envoyées au nœud correspondant par le nœud mobile, et ensuite retournés au nœud mobile. Le mouchard d'initiation de rattachement est envoyé dans le message Initiation d'essai de rattachement, et retourné dans le message Essai de rattachement. Le mouchard initiation d'entretien est envoyé dans le message Initiation d'essai d'entretien, et retourné dans le message Essai d'entretien.

- Le "jeton de génération de clé de rattachement" et le "jeton de génération de clé d'entretien" sont des valeurs de 64 bits envoyées par le nœud correspondant au nœud mobile respectivement via l'agent de rattachement (via le message Essai de rattachement) et l'adresse d'entretien (par le message Essai d'entretien).

Le nœud mobile devrait régler le mouchard initiation de rattachement ou d'entretien à un nouveau nombre aléatoire généré dans chaque message Initiation d'essai de rattachement ou d'entretien qu'il envoie. Les mouchards sont utilisés pour vérifier que le message Essai de rattachement ou d'entretien correspond au message respectivement Initiation de rattachement ou

d'entretien. Ces mouchards servent aussi à s'assurer que les parties qui n'ont pas vu la demande ne peuvent pas faire des réponses falsifiées.

Les jetons de génération de clé de rattachement et d'entretien sont produits par le nœud correspondant sur la base de sa clé secrète (Kcn) actuellement active et des noms occasionnels, ainsi que l'adresse (respectivement) de rattachement ou d'entretien. Un jeton de génération de clé est valide tant que la clé secrète (Kcn) et le nom occasionnel utilisés pour le créer sont valides.

5.2.4 Fonctions cryptographiques

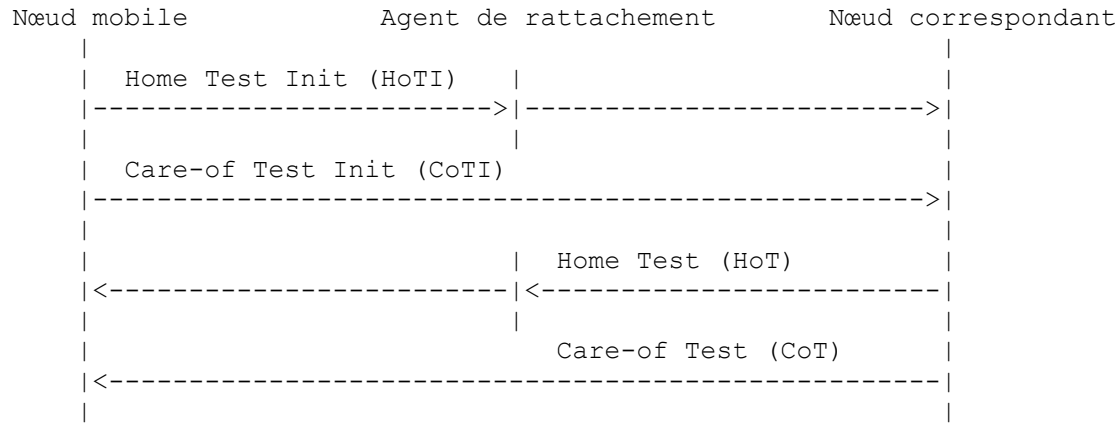
Dans la présente spécification, la fonction utilisée par défaut pour calculer les valeurs de hachage est SHA-1 [FIPS180-1], qui est considérée offrir une protection suffisante pour les messages de commandes IPv6 mobile (voir au paragraphe 15.10). Les codes d'authentification de message (MAC, *Message Authentication Code*) sont alors calculés en utilisant HMAC_SHA1 [RFC2104], [FIPS180-1]. HMAC_SHA1(K,m) note un tel MAC calculé sur le message m avec la clé K.

5.2.5 Procédure d'acheminement de retour

La procédure d'acheminement de retour permet au nœud correspondant d'obtenir des assurances raisonnables que le nœud mobile est en fait adressable à l'adresse d'entretien qu'il prétend avoir ainsi qu'à son adresse de rattachement. C'est seulement avec cette assurance que le nœud correspondant est capable d'accepter les mises à jour de lien provenant du nœud mobile, qui va alors donner pour instruction au nœud correspondant de diriger le trafic de données du nœud mobile sur l'adresse d'entretien qu'il revendique.

Ceci est fait en vérifiant si les paquets adressés aux deux adresses revendiquées sont acheminés au nœud mobile. Le nœud mobile ne peut réussir l'essai que si il est capable de fournir la preuve qu'il a reçu certaines données (les "jetons keygen") que le nœud correspondant envoie à ces adresses. Ces données sont combinées par le nœud mobile dans une clé de gestion de lien, notée Kbm.

La figure ci-dessous montre le flux de messages pour la procédure d'acheminement de retour.



Les messages Initiation d'essai de rattachement et Initiation d'essai d'entretien sont envoyés en même temps. La procédure exige très peu de traitement au nœud correspondant, et les messages Essai de rattachement et Essai d'entretien peuvent être retournés rapidement, peut-être presque simultanément. Ces quatre messages forment la procédure d'acheminement de retour.

Initiation d'essai de rattachement (HoTI, *Home Test Init)*
Un nœud mobile envoie un message Initiation d'essai de rattachement au nœud correspondant (via l'agent de rattachement) pour acquérir le jeton de génération de clé de rattachement. Le contenu du message peut être résumé comme suit :
* Adresse de source = adresse de rattachement
* Adresse de destination = correspondant
* Paramètres : mouchard d'initiation de rattachement
Le message Initiation d'essai de rattachement porte l'adresse de rattachement du nœud mobile au nœud correspondant. Le nœud mobile envoie aussi un mouchard d'initiation de rattachement que le nœud correspondant doit retourner ultérieurement. Le message Initiation d'essai de rattachement est tunnelé en sens inverse à travers l'agent de rattachement. (Les en-têtes et adresses relatifs au tunnelage inverse ont été omis de la présentation ci-dessus dans les contenus de messages.) Le nœud mobile se souvient de ces valeurs de mouchards pour obtenir l'assurance que ses messages de protocole sont bien traités par le nœud correspondant désiré.

Initiation d'essai d'entretien (CoTI, *Care-of Test Init*)
Le nœud mobile envoie un message Initiation d'essai d'entretien au nœud correspondant (directement, et non via l'agent de rattachement) pour acquérir le jeton de génération de clé d'entretien. Le contenu de ce message peut être résumé comme suit :
* Adresse de source = adresse d'entretien
* Adresse de destination = correspondant
* Paramètres : mouchard d'initiation d'entretien
Le message Initiation d'essai d'entretien porte l'adresse d'entretien du nœud mobile au nœud correspondant. Le nœud mobile envoie aussi avec un mouchard d'initiation d'entretien que le nœud correspondant doit retourner ultérieurement. Le message Initiation d'essai d'entretien est envoyé directement au nœud correspondant.

Essai de rattachement (HoT, *Home Test*)
Le message Essai de rattachement est envoyé en réponse à un message Initiation d'essai de rattachement. Il est envoyé via l'agent de rattachement. Le contenu du message est :
* Adresse de source = correspondant
* Adresse de destination = adresse de rattachement
* Paramètres :
  + mouchard d'initiation de rattachement
  + jeton de génération de clé de rattachement
  + indice de nom occasionnel de rattachement
Quand le nœud correspondant reçoit le message Initiation d'essai de rattachement, il génère un jeton de génération de clé de rattachement comme suit :
jeton de génération de clé de rattachement = First (64, HMAC_SHA1 (Kcn, (adresse de rattach. | nom occas. | 0)))

où | note l'enchaînement. Le "0" final dans la fonction HMAC_SHA1 est un octet d'un seul zéro, utilisé pour distinguer l'un de l'autre les mouchards de rattachement et d'entretien.

Le jeton de génération de clé de rattachement est formé à partir des 64 premiers bits du MAC. Le jeton de génération de clé de rattachement vérifie que le nœud mobile peut recevoir les messages envoyés à son adresse de rattachement. Kcn est utilisé dans la production du jeton de génération de clé de rattachement afin de permettre au nœud correspondant de vérifier qu'il a généré les noms occasionnels de rattachement et d'entretien, sans forcier le nœud correspondant à mémoriser une liste de tous les jetons qu'il a traités.

Le message Essai de rattachement est envoyé au nœud mobile via le réseau de rattachement, où il est présumé que l'agent de rattachement va tunneler le message au nœud mobile. Cela signifie que le nœud mobile doit avoir déjà envoyé une mise à jour de lien à l'agent de rattachement, de sorte que l'agent de rattachement va avoir reçu et autorisé la nouvelle adresse d'entretien pour le nœud mobile avant la procédure d'acheminement de retour. Pour une sécurité améliorée, les données passées entre l'agent de rattachement et le nœud mobile sont immunisées contre les attaques d'inspection et les attaques passives. Une telle protection est obtenue en chiffrant le jeton de génération de clé de rattachement lorsque il est tunnelé de l'agent de rattachement au nœud mobile comme spécifié au paragraphe 10.4.6. Les propriétés de sécurité de ce dispositif supplémentaire sont discutées au paragraphe 15.4.1.

Le mouchard d'initiation de rattachement provenant du nœud mobile est retourné dans le message Essai de rattachement, pour assurer que le message vient d'un nœud sur le chemin entre l'agent de rattachement et le nœud correspondant.

L'indice de nom occasionnel de rattachement est livré au nœud mobile pour permettre ultérieurement au nœud correspondant de trouver efficacement la valeur de nom occasionnel qui est utilisée pour créer le jeton de génération de clé de rattachement.

Essai d'entretien (CoT, *Care-of Test*)
Ce message est envoyé en réponse à un message Initiation d'essai d'entretien. Ce message n'est pas envoyé via l'agent de rattachement ; il est envoyé directement au nœud mobile. Le contenu du message est :
* Adresse de source = correspondant
* Adresse de destination = adresse d'entretien
* Paramètres :
  + mouchard d'initiation d'entretien
  + jeton de génération de clé d'entretien
  + indice de nom occasionnel d'entretien
Quand le nœud correspondant reçoit le message Initiation d'essai d'entretien, il génère un jeton de génération de clé d'entretien comme suit :
jeton de génération de clé d'entretien = First (64, HMAC_SHA1 (Kcn, (adresse d'entretien | nom occasionnel | 1)))

Ici, le "1" final dans la fonction HMAC_SHA1 est un seul octet contenant la valeur hexadécimale 0x01, et est utilisé pour distinguer les mouchards de rattachement de ceux d'entretien. Le jeton de génération de clé est formé à partir des 64 premiers bits du MAC, et envoyé directement au nœud mobile à son adresse d'entretien. Le mouchard d'initiation d'entretien provenant du message Initiation d'essai d'entretien est retourné pour s'assurer que le message vient d'un nœud sur le chemin du nœud correspondant.

L'indice de nom occasionnel d'entretien est fourni pour identifier le nom occasionnel utilisé pour le jeton de génération de clé d'entretien. Les indices de nom occasionnel de rattachement et d'entretien PEUVENT être les mêmes, ou différents, dans les messages d'essai de rattachement et d'entretien.

Quand le nœud mobile a reçu les deux messages d'essai de rattachement et d'entretien, la procédure d'acheminement de retour est achevée. Par suite de la procédure, le nœud mobile a les données dont il a besoin pour envoyer une mise à jour de lien au nœud correspondant. Le nœud mobile hache les jetons ensemble pour former une clé de lien Kbm de 20 octets :

Kbm = SHA-1 (jeton de génération de clé de rattachement | jeton de génération de clé d'entretien)

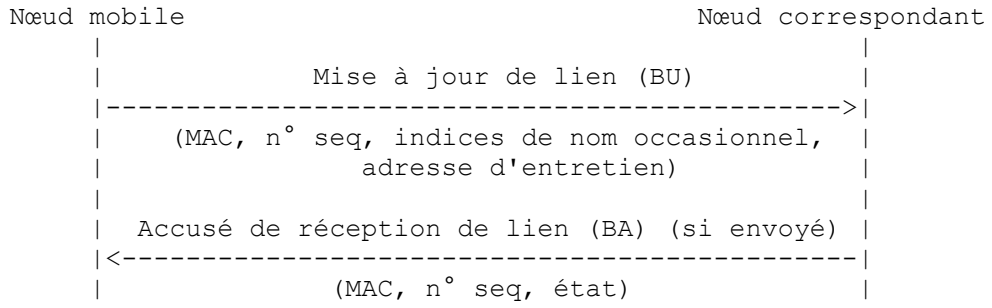
Une mise à jour de lien peut aussi être utilisée pour supprimer un lien précédemment établi (paragraphe 6.1.7). Dans ce cas, le jeton de génération de clé d'entretien n'est pas utilisé. À la place, la clé de gestion de lien est générée comme suit :

Kbm = SHA-1(jeton de génération de clé de rattachement)

Noter que le nœud correspondant ne crée aucun état spécifique du nœud mobile, jusqu'à ce qu'il reçoive la mise à jour de lien provenant du nœud mobile. Le nœud correspondant ne conserve pas la valeur de la clé de gestion de lien Kbm ; il crée Kbm quand sont donnés les indices de nom occasionnel et les adresses du nœud mobile.

5.2.6 Autorisation des messages de gestion de lien

Après que le nœud mobile a créé la clé de gestion de lien (Kbm), il peut fournir une mise à jour de lien vérifiable au nœud correspondant. Ce paragraphe donne une vue d'ensemble de cet enregistrement. La figure ci-dessous montre le flux de messages.



Mise à jour de lien
Pour autoriser une mise à jour de lien, le nœud mobile crée une clé de gestion de lien Kbm à partir des jetons de génération de clé comme décrit au paragraphe précédent. Le contenu de la mise à jour de lien (BU, *Binding Update*) inclut ce qui suit :
* Adresse de source = adresse d'entretien
* Adresse de destination = correspondant
* Paramètres :
  + adresse de rattachement (dans l'option de destination Adresse de rattachement si différente de l'adresse de source)
  + numéro de séquence (dans l'en-tête du message de mise à jour de lien)
  + indice de nom occasionnel de rattachement (dans l'option Indices de nom occasionnel)
  + indice de nom occasionnel d'entretien (dans l'option Indices de nom occasionnel)
  + First (96, HMAC_SHA1 (Kbm, (adresse d'entretien | correspondent | indice de lien)))

La mise à jour de lien contient une option Indices de nom occasionnel, indiquant au nœud correspondant quels noms occasionnels de rattachement et d'entretien utiliser pour recalculer Kbm, la clé de gestion de lien. Le MAC est calculé comme décrit au paragraphe 6.2.7, en utilisant l'adresse du nœud correspondant comme adresse de destination et le message de mise à jour de lien lui-même ("BU" ci-dessus) comme données d'en-tête de mobilité (MH, *Mobility Header*).

Une fois que le nœud correspondant a vérifié le MAC, il peut créer une entrée d'antémémoire de liens pour le mobile.

Accusé de réception de lien
La mise à jour de lien est dans certains cas acquittée par le nœud correspondant. Le contenu du message est le suivant :

* Adresse de source = correspondant
* Adresse de destination = adresse d'entretien
* Paramètres :
  + numéro de séquence (dans l'en-tête de message de mise à jour de lien)
  + First (96, HMAC_SHA1 (Kbm, (adresse d'entretien | correspondant | BA)))

L'accusé de réception de lien contient le même numéro de séquence que la mise à jour de lien. Le MAC est calculé comme décrit au paragraphe 6.2.7, en utilisant l'adresse du nœud correspondant comme adresse de destination et le message lui-même ("BA" ci-dessus) comme données de MH.

Les liens établis avec les nœuds correspondants en utilisant les clés créées au moyen de la procédure d'acheminement de retour NE DOIVENT PAS excéder MAX_RR_BINDING_LIFETIME secondes (voir la Section 12).

La valeur dans le champ Adresse de source dans l'en-tête IPv6 portant la mise à jour de lien est normalement aussi l'adresse d'entretien qui est utilisée dans le lien. Cependant, une adresse d'entretien différente PEUT être spécifiée en incluant une option de mobilité Autre adresse d'entretien dans la mise à jour de lien (voir au paragraphe 6.2.5). Quand un tel message est envoyé au nœud correspondant et que la procédure d'acheminement de retour est utilisée comme méthode d'autorisation, les messages Initiation d'essai d'entretien et Essai d'entretien DOIVENT avoir été envoyés pour l'adresse dans l'option Autre adresse d'entretien (pas l'adresse de source). Les indices de nom occasionnel et la valeur de MAC DOIVENT se fonder sur les informations obtenues de cette vérification.

Les mises à jour de lien peuvent aussi être envoyées pour supprimer un lien établi précédemment. Dans ce cas, la génération de la clé de gestion de lien dépend exclusivement du jeton de génération de clé de rattachement, et l'indice de nom occasionnel d'entretien est ignoré.

5.2.7 Mise à jour des clés et noms occasionnels de nœud

Les nœuds correspondants génèrent des noms occasionnels à des intervalles réguliers. Il est recommandé de garder chaque nom occasionnel (identifié par un indice de nom occasionnel) acceptable pendant au moins MAX_TOKEN_LIFETIME secondes (voir la Section 12) après sa première utilisation dans la construction d'une réponse au message d'acheminement de retour. Cependant, le nœud correspondant NE DOIT PAS accepter des noms occasionnels au delà de MAX_NONCE_LIFETIME secondes (voir la Section 12) après la première utilisation. Comme la différence entre ces deux constantes est 30 secondes, une façon pratique de mettre en application les durées de vie ci-dessus est de générer un nouveau nom occasionnel toutes les 30 secondes. Le nœud peut alors continuer d'accepter les jetons qui se sont fondés sur les huit derniers (MAX_NONCE_LIFETIME / 30) noms occasionnels. Il en résulte des jetons acceptables de MAX_TOKEN_LIFETIME à MAX_NONCE_LIFETIME secondes après qu'ils ont été envoyés au nœud mobile, selon que le jeton a été envoyé au début ou à la fin de la période de 30 secondes. Noter que le nœud correspondant peut aussi tenter de générer à la demande de nouveaux noms occasionnels, ou seulement si les vieux noms occasionnels ont été utilisés. Ceci est possible, pour autant que le nœud correspondant garde trace du moment où les noms occasionnels ont été utilisés pour la première fois, et ne génère pas de nouveaux noms occasionnels à chaque demande d'acheminement de retour.

Du fait de limitations de ressources, de la suppression rapide des liens, ou des réamorçages, le nœud correspondant ne peut pas dans tous les cas reconnaître les noms occasionnels sur lesquels étaient fondés les jetons. Si un indice de nom occasionnel n'est pas reconnu, le nœud correspondant répond par un code d'erreur dans l'accusé de réception de lien (136, 137, ou 138 comme exposé au paragraphe 6.1.8). Le nœud mobile peut alors réessayer la procédure d'acheminement de retour.

Une mise à jour de Kcn DEVRAIT être faite au même moment qu'une mise à jour d'un nom occasionnel, de sorte que des indices de nom occasionnel peuvent identifier à la fois le nom occasionnel et la clé. Les vieilles valeurs de Kcn doivent donc être mémorisées aussi longtemps que les vieilles valeurs de nom occasionnel.

Étant donné que les jetons sont supposés être normalement utilisables pendant MAX_TOKEN_LIFETIME secondes, le nœud mobile PEUT les utiliser au delà d'un seul cours de la procédure d'acheminement de retour jusqu'à ce que MAX_TOKEN_LIFETIME expire. Après cela, le nœud mobile NE DEVRAIT PAS utiliser les jetons. Un nœud mobile qui se déplace rapidement PEUT réutiliser un jeton de génération de clé de rattachement récent provenant d'un nœud correspondant quand il passe à une nouvelle localisation, et juste acquérir un nouveau jeton de génération de clé d'entretien pour montrer la capacité d'acheminement dans la nouvelle localisation.

Bien que cela n'économise pas le nombre d'allers-retours dus au traitement simultané des essais d'acheminement de retour de rattachement et d'entretien, il y a moins de messages échangés, et un aller-retour potentiellement long à travers l'agent de rattachement est évité. Par conséquent, cette optimisation est souvent utile. Un nœud mobile qui a plusieurs adresses de

rattachement PEUT aussi utiliser le même jeton de génération de clé d'entretien pour les mises à jour de lien concernant toutes des adresses.

5.2.8 Prévention des attaques en répétition

La procédure d'acheminement de retour protège aussi les participants contre les répétitions de mises à jour de lien à travers l'utilisation d'un numéro de séquence et d'un MAC. Il faut cependant faire attention quand on supprime des liens au nœud correspondant. Les nœuds correspondants doivent conserver les liens et les informations de numéro de séquence associés au moins tant que les noms occasionnels utilisés dans l'autorisation du lien sont encore valides. Autrement, si la mémoire est très réduite, le nœud correspondant PEUT invalider les noms occasionnels qui ont été utilisés pour le lien supprimé (ou un plus grand groupe de noms occasionnels auxquels ils appartiennent). Ceci peut cependant impacter la capacité d'accepter les mises à jour de lien provenant de nœuds mobiles qui ont récemment reçu des jetons de génération de clé. Cette solution de remplacement n'est donc recommandée qu'en dernière instance.

5.2.9 Traitement des interruptions de l'acheminement de retour

Dans certains scénarios, comme d'une mobilité simultanée, où les deux hôtes, correspondant et mobile, se déplacent en même temps, ou dans le cas où le nœud correspondant réamorce et perd les données, l'optimisation de chemin ne peut pas se faire, ou les données pertinentes de l'antémémoire de lien peuvent être perdues.

- La signalisation d'acheminement de retour DOIT être envoyée à l'adresse de rattachement du nœud correspondant si il en a une (c'est-à-dire, pas à l'adresse d'entretien des nœuds correspondants si le nœud correspondant est aussi mobile).

- Si la signalisation d'acheminement de retour est arrivée en fin de temporisation après MAX_RO_FAILURE tentatives, le nœud mobile DOIT revenir à l'envoi des paquets à l'adresse de rattachement du nœud correspondant à travers son agent de rattachement.

Le nœud mobile peut faire le tunnelage bidirectionnel en parallèle avec la procédure d'acheminement de retour jusqu'à ce qu'elle réussisse. Le retard exponentiel DEVRAIT être utilisé pour la retransmission des messages d'acheminement de retour.

La procédure d'acheminement de retour peut être déclenchée par le mouvement du nœud mobile ou par des pertes continues de communication de bout en bout avec un nœud correspondant (par exemple, sur la base d'indications provenant des couches supérieures) qui a utilisé une connexion à chemin optimisé pour le nœud mobile. Si de telles indications sont reçues, le nœud mobile PEUT revenir au tunnelage bidirectionnel tout en redémarrant la procédure d'acheminement de retour.

5.3 Découverte dynamique de l'adresse d'agent de rattachement

La découverte dynamique d'adresse d'agent de rattachement a été conçue pour être utilisée dans des déploiements où la sécurité n'est pas nécessaire. Pour cette raison, aucune solution de sécurité n'est fournie dans ce document pour la découverte dynamique d'adresse d'agent de rattachement.

5.4 Découverte du préfixe mobile

Le nœud mobile et l'agent de rattachement DEVRAIENT utiliser une association de sécurité IPsec pour protéger l'intégrité et l'authenticité des sollicitations et annonces de préfixe mobile. Les nœuds mobiles et les agents de rattachement DOIVENT prendre en charge et DEVRAIENT utiliser l'en-tête d'encapsulation de charge utile de sécurité (ESP) en mode transport avec un algorithme d'authentification de charge utile non NUL pour assurer l'authentification de l'origine des données, l'intégrité sans connexion, et la protection facultative contre la répétition.

5.5 Paquets de charge utile

Les paquets de charge utile échangés avec les nœuds mobiles peuvent être protégés de la façon usuelle, de la même façon que les hôtes stationnaire peuvent les protéger. Cependant, IPv6 mobile introduit l'option de destination Adresse de rattachement, un en-tête d'acheminement, et des en-têtes de tunnelage dans les paquets de charge utile. On définit dans ce qui suit les mesures de sécurité pour les protéger, et empêcher leur utilisation dans les attaques contre d'autres parties.

La présente spécification limite l'utilisation de l'option de destination Adresse de rattachement à la situation où le nœud correspondant a déjà une entrée d'antémémoire de liens pour l'adresse de rattachement en question. Cela évite l'utilisation de l'option Adresse de rattachement dans les attaques décrites au paragraphe 15.1.

IPv6 mobile utilise un type d'en-tête d'acheminement spécifique de IPv6 mobile. Ce type fournit les fonctionnalités nécessaires mais n'ouvre pas les vulnérabilités discutées au paragraphe 15.1 et dans la [RFC5095].

Les tunnels entre le nœud mobile et l'agent de rattachement sont protégés en assurant une utilisation appropriée des adresses de source, et une protection cryptographique facultative. Le nœud mobile vérifie que l'adresse IP externe correspond à son agent de rattachement. L'agent de rattachement vérifie que l'adresse IP externe correspond à la localisation actuelle du nœud mobile (les mises à jour de lien envoyées aux agents de rattachement sont sécurisées). L'agent de rattachement identifie le nœud mobile par l'adresse de source du paquet interne. (Normalement, c'est l'adresse de rattachement du nœud mobile, mais elle peut aussi être une adresse de liaison locale, comme expliqué au paragraphe 10.4.2. Pour reconnaître le dernier type d'adresses, l'agent de rattachement exige que le bit Compatibilité d'adresse de liaison locale (L) soit établi dans la mise à jour de lien.) Ces mesures protègent les tunnels contre les vulnérabilités discutées au paragraphe 15.1.

Pour le trafic tunnelé via l'agent de rattachement, une encapsulation IPsec ESP supplémentaire PEUT être prise en charge et utilisée. Si des protocoles de contrôle d'adhésion à des groupes de diffusion groupée ou d'autoconfiguration d'adresse à état plein sont pris en charge, la protection des données de charge utile DOIT être supportée.

6. Nouveau protocole IPv6, types de message, et option de destination

6.1 En-tête de mobilité

L'en-tête de mobilité est une extension d'en-tête utilisée par les nœuds mobiles, les nœuds correspondants, et les agents de rattachement dans tous les messages relatifs à la création et la gestion des liens. Les paragraphes de cette Section décrivent les types de message qui peuvent être envoyés en utilisant l'en-tête de mobilité.

Les messages En-tête de mobilité NE DOIVENT PAS être envoyés avec un en-tête d'acheminement de type 2, excepté comme décrit au paragraphe 9.5.4 pour l'accusé de réception de lien. Les messages En-tête de mobilité NE DOIVENT PAS non plus être utilisés avec l'option de destination Adresse de rattachement, sauf comme décrit aux paragraphes 11.7.1 et 11.7.2 pour la mise à jour de lien. La liste de mise à jour de lien ou les informations d'antémémoire de liens (lorsque présente) pour la destination NE DOIT PAS être utilisée dans l'envoi des messages En-tête de mobilité. C'est-à-dire que les messages En-tête de mobilité outrepassent aussi bien la vérification d'antémémoire de liens décrite au paragraphe 9.3.2 et la vérification de liste de mise à jour de lien décrite au paragraphe 11.3.1 qui sont normalement effectuées pour tous les paquets. Ceci s'applique même aux messages envoyés de ou à un nœud correspondant qui est lui-même un nœud mobile.

6.1.1 Format

L'en-tête de mobilité est identifié par une valeur de prochain en-tête de 135 dans l'en-tête immédiatement précédant, et a le format suivant

Protocole de charge utile : sélecteur de 8 bits. Identifie le type de l'en-tête qui suit immédiatement l'en-tête de mobilité. Utilise les mêmes valeurs que le champ Prochain en-tête IPv6 [RFC2460]. Ce champ est destiné à être utilisé par une future extension (voir l'Appendice A.1). Les mises en œuvre conformes à la présente spécification DEVRAIENT régler le type de protocole de charge utile à IPPROTO_NONE (59 décimal).

Longueur de charge utile : entier non signé de 8 bits, représentant la longueur de l'en-tête de mobilité en unités de 8 octets, excluant les 8 premiers octets. La longueur de l'en-tête de mobilité DOIT être un multiple de 8 octets.

Type de MH : sélecteur de 8 bits. Identifie le message de mobilité particulier en question. Les valeurs courantes sont spécifiées au paragraphe 6.1.2 et suivants. Un champ Type de MH non reconnu cause l'envoi d'une indication d'erreur.

Réservé : champ de 8 bits réservé pour utilisation ultérieure. La valeur DOIT être initialisée à zéro par l'envoyeur, et DOIT être ignorée par le receveur.

Somme de contrôle : entier non signé de 16 bits. Ce champ contient la somme de contrôle de l'en-tête de mobilité. La somme de contrôle est calculée à partir de la chaîne d'octets consistant en un "pseudo en-tête" suivi par l'en-tête de mobilité entier en commençant par le champ Protocole de charge utile. La somme de contrôle est le complément à un de 16 bits de la somme des compléments à un de cette chaîne.

Le pseudo en-tête contient les champs d'en-tête IPv6, comme spécifié au paragraphe 8.1 de la [RFC2460]. La valeur de Prochain en-tête utilisée dans le pseudo en-tête est 135. Les adresses utilisées dans le pseudo en-tête sont les adresses qui apparaissent dans les champs Adresse de source et Adresse de destination dans le paquet IPv6 qui porte l'en-tête de mobilité.

Noter que les procédures de calcul des sommes de contrôle de couche supérieure lorsque le MN est hors de chez lui décrites au paragraphe 11.3.1 s'appliquent même pour l'en-tête de mobilité. Si un message de mobilité a une option de destination Adresse de rattachement, le calcul de la somme de contrôle utilise alors l'adresse de rattachement dans cette option comme valeur du champ Adresse IPv6 de source. L'en-tête d'acheminement de type 2 est traité comme expliqué dans la [RFC2460].

L'en-tête de mobilité est considéré comme le protocole de couche supérieure pour les besoins du calcul du pseudo en-tête. Le champ Longueur de paquet de couche supérieure dans le pseudo en-tête DOIT être réglé à la longueur totale de l'en-tête de mobilité.

Pour calculer la somme de contrôle, le champ Somme de contrôle est réglé à zéro.

Données de message : champ de longueur variable qui contient les données spécifiques du type d'en-tête de mobilité indiqué.

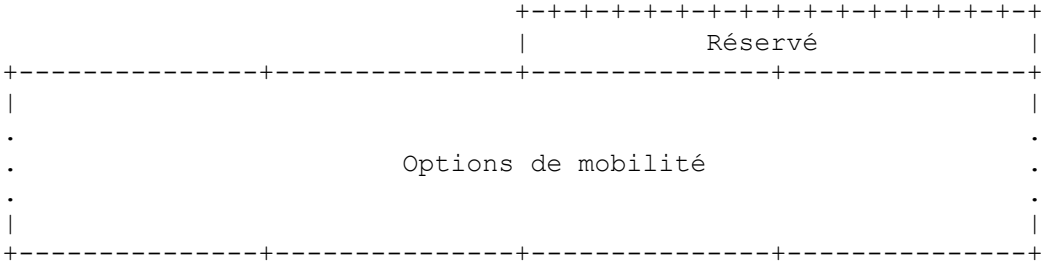
IPv6 mobile définit aussi un certain nombre "d'options de mobilité" à utiliser dans ces messages ; si il en est d'incluses, toutes les options DOIVENT apparaître après la portion fixe des données de message spécifiées dans le présent document. La présence de telles options va être indiquée par le champ Longueur d'en-tête au sein du message. Quand la valeur de Longueur d'en-tête est supérieure à la longueur exigée pour le message spécifié ici, les octets restants sont interprétés comme des options de mobilité. Ces options incluent des options de bourrage qui peuvent être utilisées pour s'assurer que les autres options sont alignées correctement, et que la longueur totale du message est divisible par 8. Le codage et le format des options définies sont décrits au paragraphe 6.2.

Les exigences d'alignement pour l'en-tête de mobilité sont les mêmes que pour tout en-tête de protocole IPv6. C'est -à-dire que ils DOIVENT être alignés sur une frontière de 8 octets.

6.1.2 Message de demande de rafraîchissement de lien

Le message de demande de rafraîchissement de lien (BRR, *Binding Refresh Request*) demande à un nœud mobile de mettre à jour son lien de mobilité. Ce message est envoyé par les nœuds correspondants conformément aux règles du paragraphe 9.5.5. Quand un nœud mobile reçoit un paquet contenant un message de demande de rafraîchissement de lien, il traite le message conformément aux règles du paragraphe 11.7.4.

Le message de demande de rafraîchissement de lien utilise la valeur de type MH de 0. Quand cette valeur est indiquée dans le champ Type de MH, le format du champ Données de message dans l'en-tête de mobilité est le suivant :



Réservé : champ de 16 bits réservé pour utilisation ultérieure. La valeur DOIT être initialisée à zéro par l'envoyeur, et DOIT être ignorée par le receveur.

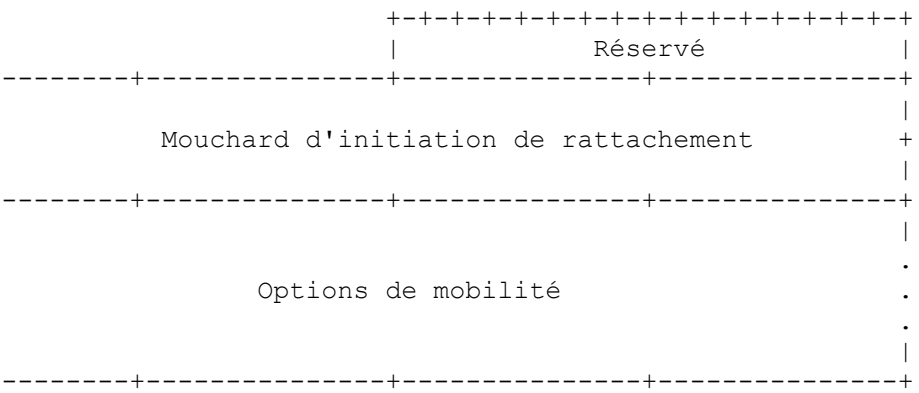
Options de mobilité : champ de longueur variable d'une longueur telle que l'en-tête de mobilité complet soit un multiple entier de 8 octets. Ce champ contient zéro, une ou plusieurs options de mobilité codées en TLV. Le codage et le format des options définies sont décrits au paragraphe 6.2. Le receveur DOIT ignorer et sauter toutes les options qu'il ne comprend pas.

Il PEUT y avoir des informations supplémentaires, associées à ce message de demande de rafraîchissement de lien qui n'ont pas besoin d'être présentes dans tous les messages de demande de rafraîchissement de lien envoyées. Les options de mobilité permettent que de futures extensions au format du message de demande de rafraîchissement de lien soient définies. La présente spécification ne définit aucune option valide pour le message de demande de rafraîchissement de lien.

Si aucune option réelle n'est présente dans ce message, aucun bourrage n'est nécessaire et le champ Longueur d'en-tête sera réglé à 0.

6.1.3 Message Initiation d'essai de rattachement

Un nœud mobile utilise le message Initiation d'essai de rattachement (HoTI, *Home Test Init*) pour initier la procédure d'acheminement de retour et demander un jeton de génération de clé de rattachement à un nœud correspondant (voir au paragraphe 11.6.1). Le message Initiation d'essai de rattachement utilise la valeur de type MH de 1. Quand cette valeur est indiquée dans le champ Type MH, le format du champ Données de message dans l'en-tête de mobilité est le suivant :



Réservé : champ de 16 bits réservé pour utilisation ultérieure. Cette valeur DOIT être initialisée à zéro par l'envoyeur, et DOIT être ignorée par le receveur.

Mouchard d'initiation de rattachement : champ de 64 bits qui contient une valeur aléatoire.

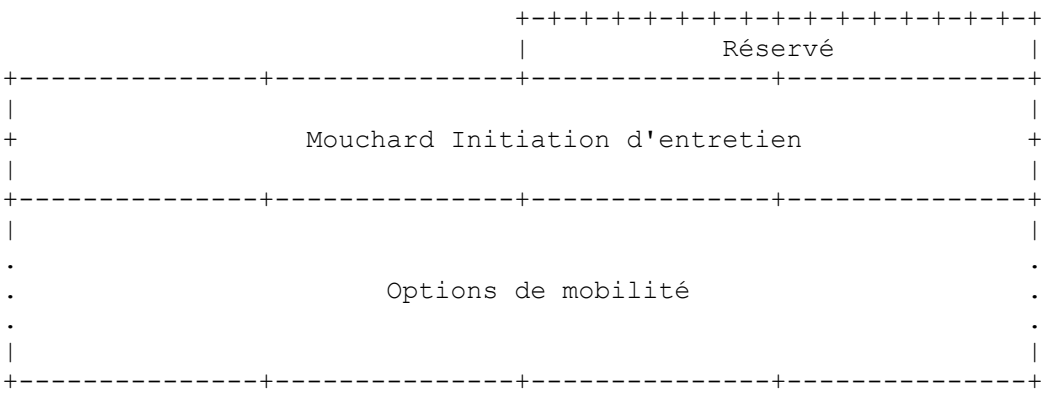
Options de mobilité : champ de longueur variable d'une longueur telle que l'en-tête de mobilité complet soit un multiple entier de 8 octets. Ce champ contient zéro, une ou plusieurs options de mobilité codées comme TLV. Le receveur DOIT ignorer et sauter toute option qu'il ne comprend pas. Cette spécification ne définit aucune option valide pour le message Initiation d'essai de rattachement.

Si aucune option réelle n'est présente dans ce message, aucun bourrage n'est nécessaire et le champ Longueur d'en-tête sera réglé à 1.

Ce message est tunnelé à travers l'agent de rattachement quand le nœud mobile est hors de chez lui. Un tel tunnelage DEVRAIT employer IPsec ESP en mode tunnel entre l'agent de rattachement et le nœud mobile. Cette protection est indiquée par la base de données de politique de sécurité IPsec. La protection des messages Initiation d'essai de rattachement est sans relation avec l'exigence de protéger le trafic régulier de charges utiles, qui PEUT utiliser aussi de tels tunnels.

6.1.4 Message Initiation d'essai d'adresse d'entretien

Un nœud mobile utilise le message Initiation d'essai d'entretien (CoTI, *Care-of Test Init*) pour initier la procédure d'acheminement de retour et demander un jeton de génération de clé d'entretien à un nœud correspondant (voir au paragraphe 11.6.1). Le message Initiation d'essai d'entretien utilise la valeur de type MH de 2. Quand cette valeur est indiquée dans le champ Type MH, le format du champ Données de message dans l'en-tête de mobilité est le suivant :



Réservé : champ de 16 bits réservé pour utilisation ultérieure. La valeur DOIT être initialisée à zéro par l'envoyeur, et DOIT être ignorée par le receveur.

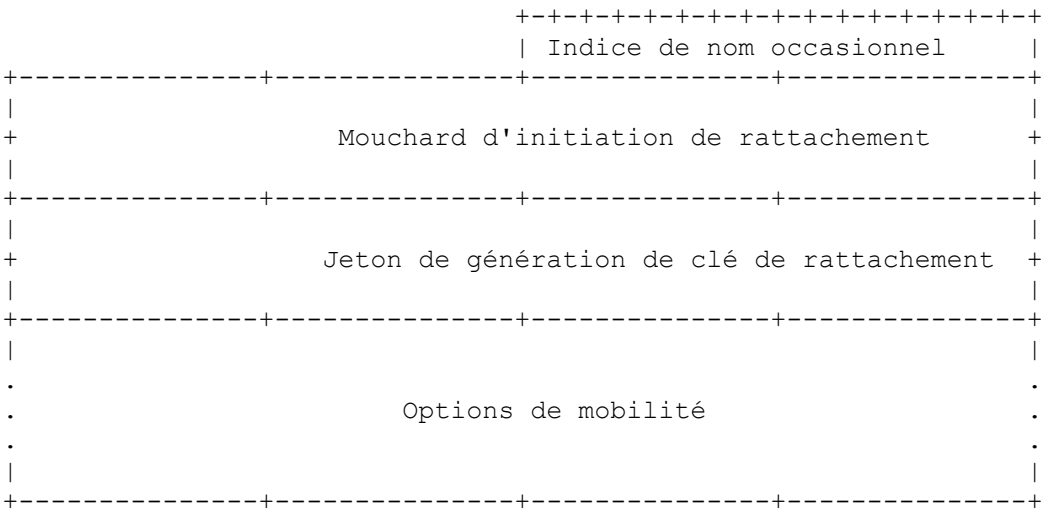
Mouchard d'initiation d'entretien : champ de 64 bits qui contient une valeur aléatoire, le mouchard d'initiation d'entretien.

Options de mobilité : champ de longueur variable d'une longueur telle que 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 receveur DOIT ignorer et sauter toute option qu'il ne comprend pas. La présente spécification ne définit aucune option valide pour le message Initiation d'essai d'entretien.

Si aucune option réelle n'est présente dans ce message, aucun bourrage n'est nécessaire et le champ Longueur d'en-tête sera réglé à 1.

6.1.5 Message Essai de rattachement

Le message Essai de rattachement (HoT, *Home Test*) est une réponse au message Initiation d'essai de rattachement, et est envoyé du nœud correspondant au nœud mobile (voir au paragraphe 5.2.5). Le message Essai de rattachement utilise la valeur de type MH de 3. Quand cette valeur est indiquée dans le champ Type de MH, le format du champ Données de message dans l'en-tête de mobilité est comme suit :



Indice de nom occasionnel de rattachement : ce champ va être renvoyé en écho par le nœud mobile au nœud correspondant dans une mise à jour de lien ultérieure.

Mouchard d'initiation de rattachement : champ de 64 bits qui contient le mouchard d'initiation de rattachement.

Jeton de génération de clé de rattachement : ce champ contient le jeton de génération de clé de rattachement de 64 bits utilisé dans la procédure d'acheminement de retour.

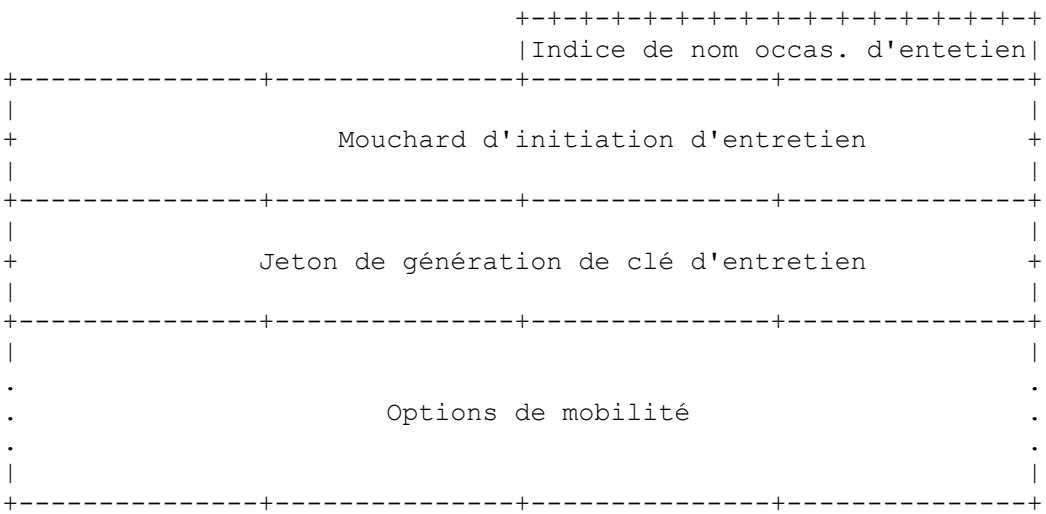
Options de mobilité : champ de longueur variable de longueur telle que l'en-tête de mobilité complet soit un entier multiple de 8 octets. Ce champ contient zéro, une ou plusieurs options de mobilité codées en TLV. Le receveur DOIT ignorer et

sauter toute option qu'il ne comprend pas. La présente spécification ne définit aucune option valide pour le message Essai de rattachement.

Si aucune option réelle n'est présente dans ce message, aucun bourrage n'est nécessaire et le champ Longueur d'en-tête sera réglé à 2.

6.1.6 Message Essai d'entretien

Le message Essai d'entretien (CoT, *Care-of Test*) est une réponse au message Initiation d'essai d'entretien, et est envoyé du nœud correspondant au nœud mobile (voir au paragraphe 11.6.2). Le message Essai d'entretien utilise la valeur de type MH de 4. Quand cette valeur est indiquée dans le champ Type de MH, le format du champ Données de message dans l'en-tête de mobilité est le suivant :



Indice de nom occasionnel d'entretien : cette valeur va être renvoyée en écho par le nœud mobile au nœud correspondant dans une mise à jour de lien suivante.

Mouchard d'initiation d'entretien : champ de 64 bits qui contient le mouchard d'initiation d'entretien.

Jeton de génération de clé d'entretien : ce champ contient le jeton de génération de clé d'entretien de 64 bits utilisé dans la procédure d'acheminement de retour.

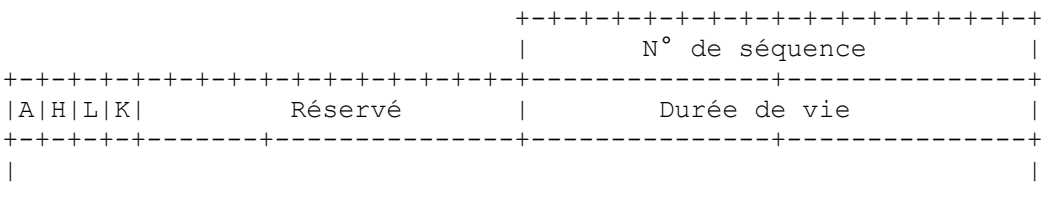
Options de mobilité : champ de longueur variable de longueur telle que l'en-tête de mobilité complet soit un entier multiple de 8 octets. Ce champ contient zéro, une ou plusieurs options de mobilité codées en TLV. Le receveur DOIT ignorer et sauter toute option qu'il ne comprend pas. La présente spécification ne définit aucune option valide pour le message Essai d'entretien.

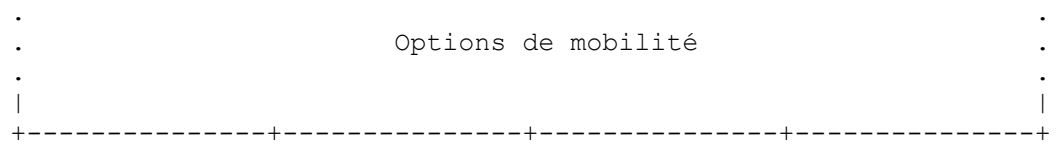
Si aucune option réelle n'est présente dans ce message, aucun bourrage n'est nécessaire et le champ Longueur d'en-tête sera réglé à 2.

6.1.7 Message Mise à jour de lien

Le message Mise à jour de lien (BU, *Binding Update*) est utilisé par un nœud mobile pour notifier aux autres nœuds une nouvelle adresse d'entretien pour lui-même. Les mises à jour de lien sont envoyées comme décrit aux paragraphes 11.7.1 et 11.7.2.

La mise à jour de lien utilise la valeur de type MH de 5. Quand cette valeur est indiquée dans le champ Type de MH, le format du champ Données de message dans l'en-tête de mobilité est comme suit :





A (*Acknowledge*) : le bit A (accusé de réception) est établi par le nœud mobile envoyeur pour demander qu'un accusé de réception de lien (paragraphe 6.1.8) soit retourné à réception de la mise à jour de lien.

H (*Home Registration*) : le bit H (enregistrement de rattachement) est établi par le nœud mobile envoyeur pour demander que le nœud receveur agisse comme agent de rattachement de ce nœud. La destination du paquet qui porte ce message DOIT être celle d'un routeur qui partage le même préfixe de sous réseau que l'adresse de rattachement du nœud mobile dans le lien.

L (*Link-Local Address Compatibility*) : le bit L (Compatibilité d'adresse de liaison locale) est établi quand l'adresse de rattachement rapportée par le nœud mobile a le même identifiant d'interface que l'adresse de liaison locale du nœud mobile.

K (Capacité de mobilité de gestion de clé) : si ce bit est à zéro, le protocole utilisé pour établir l'association de sécurité IPsec entre le nœud mobile et l'agent de rattachement ne survit pas aux mouvements. Il peut alors devoir être relancé. (Noter que les associations de sécurité IPsec elles-mêmes sont supposées survivre aux mouvements.) Si la configuration manuelle de IPsec est utilisée, le bit DOIT être à zéro. Ce bit n'est valide que dans les mises à jour de lien envoyées à l'agent de rattachement, et DOIT être à zéro dans les autres mises à jour de lien. Les nœuds correspondants DOIVENT ignorer ce bit.

Réservé : ces champs ne sont pas utilisés. Ils DOIVENT être initialisés à zéro par l'envoyeur et DOIT être ignorés par le receveur.

N° de séquence : entier non signé de 16 bits utilisé par le nœud receveur pour suivre les mises à jour de lien et par le nœud envoyeur pour confronter un accusé de réception de lien retourné à cette mise à jour de lien.

Durée de vie : entier non signé de 16 bits. Nombre d'unités de temps restantes avant que le lien DOIVE être considéré expiré. Une valeur de zéro indique que l'entrée d'antémémoire de liens pour le nœud mobile DOIT être supprimée. Une unité de temps est de 4 secondes.

Options de mobilité : champ de longueur variable de longueur telle que 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 définies sont décrits au paragraphe 6.2. Le receveur DOIT ignorer et sauter toute option qu'il ne comprend pas.

Les options suivantes sont valides dans une mise à jour de lien :
* option Données d'autorisation de lien (cette option est obligatoire dans les mises à jour de lien envoyées à un nœud correspondant)
* option Indices de nom occasionnel
* option Adresse d'entretien de remplacement

Si aucune option n'est présente dans ce message, 4 octets de bourrage sont nécessaires et le champ Longueur d'en-tête sera réglé à 1.

L'adresse d'entretien est spécifiée soit par le champ Adresse de source dans l'en-tête IPv6, soit par l'option Adresse d'entretien de remplacement, si elle est présente. L'adresse d'entretien DOIT être une adresse d'acheminement en envoi individuel. L'adresse IPv6 de source DOIT être une adresse de source topologiquement correcte. Les mises à jour de lien pour une adresse d'entretien qui n'est pas une adresse d'acheminement en envoi individuel DOIVENT être éliminées en silence.

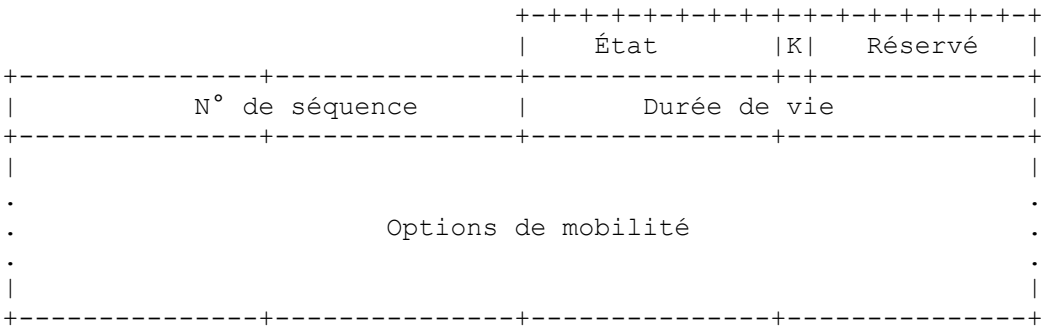
La suppression d'un lien DOIT être indiquée en réglant le champ Durée de vie à 0. Dans une suppression, la génération de la clé de gestion de lien dépend exclusivement du jeton de génération de clé de rattachement, comme expliqué au paragraphe 5.2.5.

Les nœuds correspondants NE DEVRAIENT PAS supprimer les entrées d'antémémoire de liens avant l'expiration de leur durée de vie, si une application hébergée par le nœud correspondant va encore probablement demander une communication avec le nœud mobile. Une entrée d'antémémoire de liens qui est désallouée prématurément peut causer l'élimination de paquets suivants provenant du nœud mobile, si ils contiennent l'option de destination Adresse de rattachement. Cette situation est récupérable, car un message Erreur de lien est envoyé au nœud mobile (voir au paragraphe 6.1.9) ; cependant, cela cause des retards inutiles dans les communications.

6.1.8 Message Accusé de réception de lien

L'accusé de réception de lien est utilisé pour accuser réception d'une mise à jour de lien (paragraphe 6.1.7). Ce paquet est envoyé comme décrit aux paragraphes 9.5.4 et 10.3.1.

L'accusé de réception de lien a la valeur de type MH de 6. Quand cette valeur est indiquée dans le champ Type de MH, le format du champ Données de message dans l'en-tête de mobilité est comme suit :



État : entier non signé de 8 bits indiquant la disposition de la mise à jour de lien. Les valeurs du champ État inférieures à 128 indiquent que la mise à jour de lien a été acceptée par le nœud receveur. Les valeurs supérieures ou égales à 128 indiquent que la mise à jour de lien a été rejetée par le nœud receveur. Les valeurs d'état suivantes sont actuellement définies :

0 Mise à jour de lien acceptée
1 Acceptée mais découverte de préfixe nécessaire
128 Raison non spécifiée
129 Administrativement interdit
130 Ressources insuffisantes
131 Enregistrement de rattachement non pris en charge
132 Pas de sous réseau de rattachement
133 Pas d'agent de rattachement pour ce nœud mobile
134 Échec de détection d'adresse dupliquée
135 Numéro de séquence hors de la fenêtre
136 Indice de nom occasionnel de rattachement expiré
137 Indice de nom occasionnel d'entretien expiré
138 Noms occasionnels expirés
139 Changement de type d'enregistrement interdit
174 Adresse d'entretien invalide

Les valeurs à jour du champ État sont spécifiées dans le registre de l'IANA des numéros alloués [RFC3232].

K (Key Management Mobility Capability) : si ce bit est à zéro, le protocole utilisé pour établir l'association de sécurité IPsec entre le nœud mobile et l'agent de rattachement ne survit pas aux mouvements. Il peut alors devoir être relancé. (Noter que les associations de sécurité IPsec elles-mêmes sont supposées survivre aux mouvements.) Les nœuds correspondants DOIVENT régler le bit K à 0.

Réservé : ce champ n'est pas utilisé. Il DOIT être initialisé à zéro par l'envoyeur et DOIT être ignoré par le receveur.

N° de séquence : le numéro de séquence dans l'accusé de réception de lien est copié du champ Numéro de séquence dans la mise à jour de lien. Il est utilisé par le nœud mobile pour confronter cet accusé de réception de lien avec une mise à jour de lien en instance.

Durée de vie : la durée de vie accordée, en unités de 4 secondes, pour laquelle ce nœud DEVRAIT conserver l'entrée pour ce nœud mobile dans son antémémoire de liens. La valeur de ce champ est indéfinie si le champ État indique que la mise à jour de lien a été rejetée.

Options de mobilité : champ de longueur variable de longueur telle que 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 définies sont décrits au paragraphe 6.2. Le receveur DOIT ignorer et sauter toute option qu'il ne comprend pas.

Il PEUT y avoir des informations supplémentaires associées à cet accusé de réception de lien qui n'ont pas besoin d'être présentes dans tous les accusés de réception de lien envoyés. Les options de mobilité permettent que de futures extensions au format de l'accusé de réception de lien soient définies. Les options suivantes sont valides pour l'accusé de réception de lien :

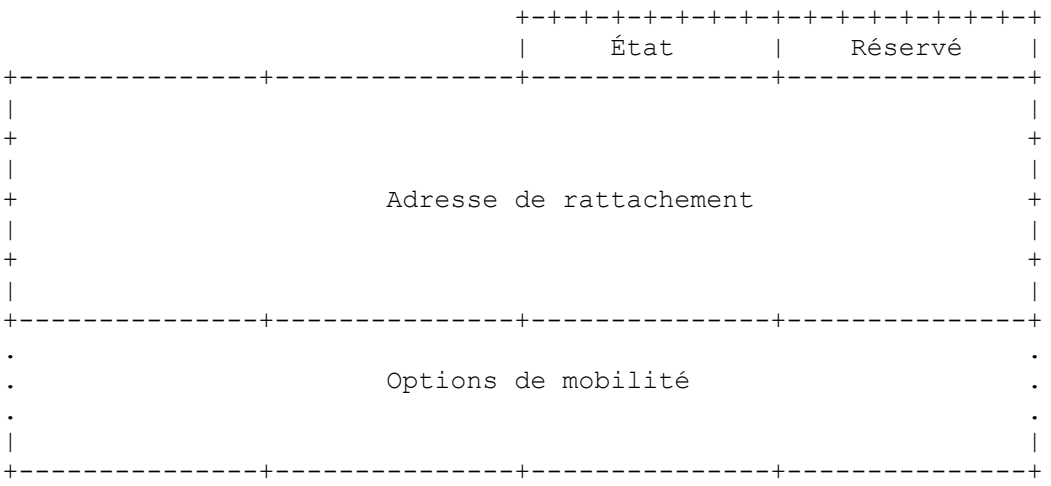
* option Données d'autorisation de lien (cette option est obligatoire dans les accusés de réception de lien envoyés par un nœud correspondant, sauf mention contraire au paragraphe 9.5.4)
* option Avis de rafraîchissement de lien

Si aucune option n'est présente dans ce message, 4 octets de bourrage sont nécessaires et le champ Longueur d'en-tête sera réglé à 1.

6.1.9 Message Erreur de lien

Le message Erreur de lien (BE, *Binding Error*) est utilisé par le nœud correspondant pour signaler une erreur relative à la mobilité, comme une tentative inappropriée d'utiliser l'option de destination Adresse de rattachement sans un lien existant; voir les détails au paragraphe 9.3.3.

Le message Erreur de lien utilise la valeur de type MH de 7. Quand cette valeur est indiquée dans le champ Type de MH, le format du champ Données de message dans l'en-tête de mobilité est le suivant :



État : entier non signé de 8 bits indiquant la raison de ce message. Les valeurs suivantes sont actuellement définies :

1 lien inconnu pour l'option de destination Adresse de rattachement
2 valeur non reconnue de type de MH

Réservé : champ de 8 bits réservé pour utilisation ultérieure. La valeur DOIT être initialisée à zéro par l'envoyeur, et DOIT être ignorée par le receveur.

Adresse de rattachement : l'adresse de rattachement qui était contenue dans l'option de destination Adresse de rattachement. Le nœud mobile utilise cette information pour déterminer que lien n'existe pas, dans les cas où le nœud mobile a plusieurs adresses de rattachement.

Options de mobilité : champ de longueur variable de longueur telle que 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 receveur DOIT ignorer et sauter toute option qu'il ne comprend pas. Il PEUT y avoir des informations supplémentaires associées à ce message Erreur de lien qui n'ont pas besoin d'être présentes dans tous les messages Erreur de lien envoyés. Les options de mobilité permettent que soient définies de futures extensions au format du message Erreur de lien. Le codage et le format des options définies sont décrits au paragraphe 6.2. La présente spécification ne définit aucune option valide pour le message Erreur de lien.

Si aucune option réelle n'est présente dans ce message, aucun bourrage n'est nécessaire et le champ Longueur d'en-tête sera réglé à 2.

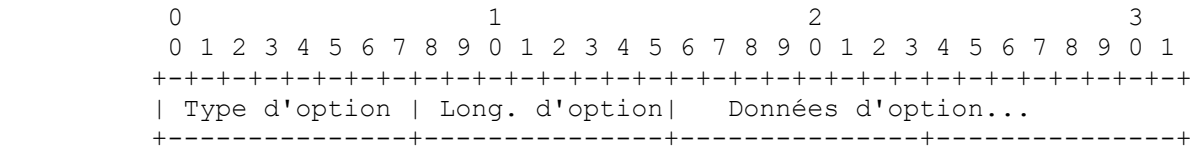
6.2 Options Mobilité

Les messages Mobilité peuvent inclure zéro, une ou plusieurs options de mobilité. Cela permet des champs facultatifs qui peuvent n'être pas nécessaires dans toutes les utilisations d'un en-tête de mobilité particulier, ainsi que de futures extensions au format des messages. De telles options sont incluses dans le champ Données de message du message lui-même, après la portion fixe des données de message spécifiée dans les paragraphes précédents.

La présence de telles options va être indiquée par la longueur d'en-tête de l'en-tête de mobilité. Si elle est incluse, l'option Données d'autorisation de lien (paragraphe 6.2.7) DOIT être la dernière option et NE DOIT PAS avoir de bourrage en queue. Autrement, les options peuvent être placées dans n'importe quel ordre.

6.2.1 Format

Les options de mobilité sont codées dans l'espace restant du champ Données de message d'un message de mobilité, en utilisant un format de type-longueur-valeur (TLV) comme suit :



Type d'option : identifiant de huit bits du type de l'option de mobilité. Quand il traite un en-tête de mobilité qui contient une option pour laquelle la valeur de type d'option n'est pas reconnue par le receveur, celui-ci DOIT ignorer en silence et sauter l'option, traitant correctement toutes les options restantes dans le message.

Longueur d'option : entier non signé de 8 bits, représentant la longueur en octets de l'option de mobilité, non inclus les champs Type d'option et Longueur d'option.

Données d'option : champ de longueur variable qui contient des données spécifiques de l'option.

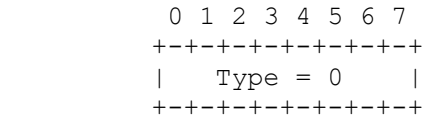
Les paragraphes qui suivent spécifient les types d'option qui sont actuellement définis pour l'usage de l'en-tête de mobilité.

Les mises en œuvre DOIVENT ignorer en silence toutes les options de mobilité qu'elles ne comprennent pas.

Les options de mobilité peuvent avoir des exigences d'alignement. Suivant les conventions de IPv6, ces options sont alignées dans un paquet de telle sorte que les valeurs multi octets dans le champ Données d'option de chaque option tombent sur des limites naturelles (c'est-à-dire, les champs d'une longueur de n octets sont placés dans un multiple entier de n octets à partir du début de l'en-tête, pour n = 1, 2, 4, ou 8) [RFC2460].

6.2.2 Pad1

L'option Pad1 n'a aucune exigence d'alignement. Son format est le suivant :

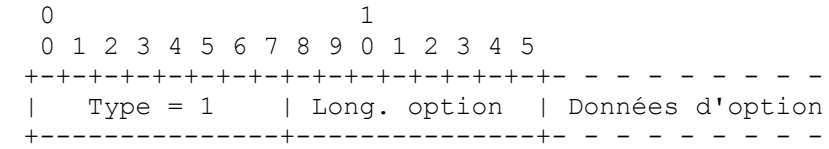


Note : le format de l'option Pad1 est un cas particulier -- il n'a pas de champ Longueur d'option ni de champ Données d'option.

L'option Pad1 est utilisée pour insérer un octet de bourrage dans la zone des options de mobilité d'un en-tête de mobilité. Si plus d'un octet de bourrage est requis, l'option PadN, décrite à la suite, devrait être utilisée plutôt que plusieurs options Pad1.

6.2.3 PadN

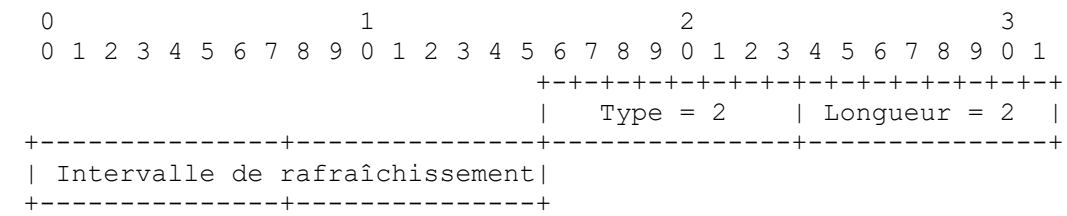
L'option PadN n'a pas d'exigence d'alignement. Son format est le suivant :



L'option PadN est utilisée pour insérer deux octets de bourrage ou plus dans la zone d'options de mobilité d'un message de mobilité. Pour N octets de bourrage, le champ Longueur d'option contient la valeur N-2, et les données d'option consistent en N-2 octets de valeur zéro. Les données de l'option PadN DOIVENT être ignorées par le receveur.

6.2.4 Avis de rafraîchissement de lien

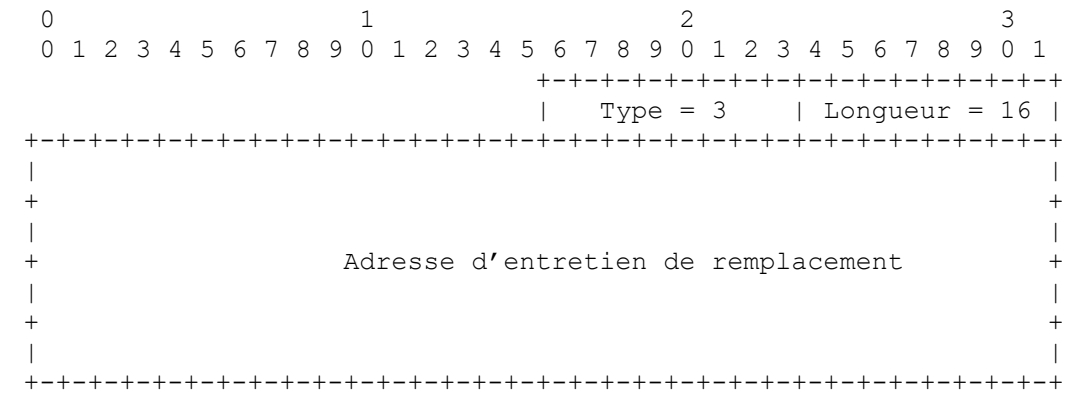
L'option Avis de rafraîchissement de lien a une exigence d'alignement de 2n. Son format est le suivant :



L'option Avis de rafraîchissement de lien n'est valide que dans l'accusé de réception de lien, et seulement sur les accusés de réception de liens envoyés de l'agent de rattachement du nœud mobile en réponse à un enregistrement de rattachement. L'intervalle de rafraîchissement est mesuré en unités de quatre secondes, et indique le temps restant jusqu'à ce que le nœud mobile DEVRAIT envoyer un nouvel enregistrement de rattachement à l'agent de rattachement. L'intervalle de rafraîchissement DOIT être réglé à indiquer un plus petit intervalle de temps que la valeur de durée de vie de l'accusé de réception de lien.

6.2.5 Adresse d'entretien de remplacement

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

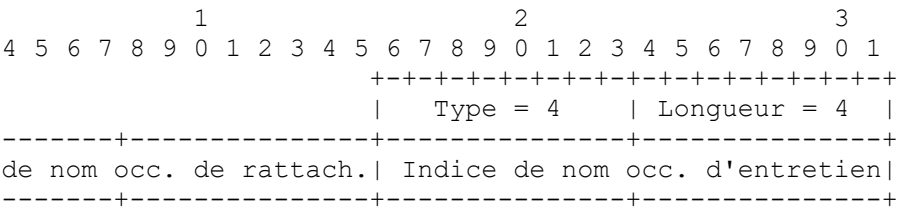


Normalement, une mise à jour de lien spécifie l'adresse d'entretien désirée dans le champ Adresse de source de l'en-tête IPv6. Cependant dans certains cas, ceci n'est pas possible, comme lorsque le nœud mobile souhaite indiquer une adresse d'entretien qu'il ne peut pas utiliser comme adresse de source topologiquement correcte (paragraphes 6.1.7 et 11.7.2) ou quand le mécanisme de sécurité utilisé ne protège pas l'en-tête IPv6 (paragraphe 11.7.1).

L'option Adresse d'entretien de remplacement est fournie pour ces situations. Cette option n'est valide que dans les mises à jour de lien. Le champ Adresse d'entretien de remplacement contient une adresse à utiliser comme adresse d'entretien pour le lien, plutôt que d'utiliser l'adresse de source du paquet comme adresse d'entretien.

6.2.6 Indices de noms occasionnels

L'option Indices de nom occasionnel a une exigence d'alignement de 2n. Son format est le suivant :



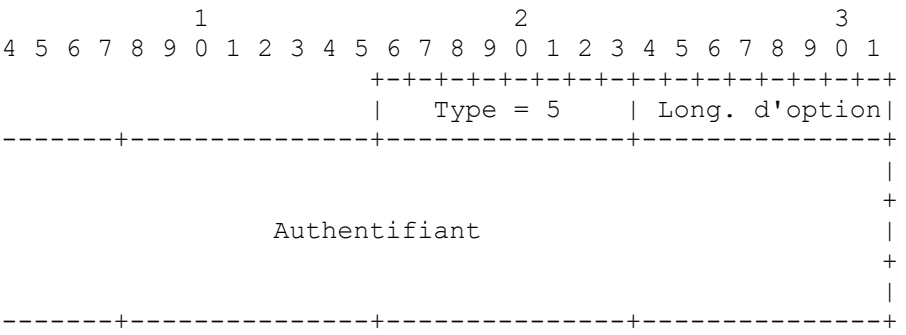
L'option Indices de nom occasionnel n'est valide que dans le message de mise à jour de lien envoyé à un nœud correspondant, et seulement quand il est présent avec une option Données d'autorisation de lien. Quand le nœud correspondant autorise la mise à jour de lien, il doit produire des jetons de génération de clé de rattachement et d'entretien provenant de ses valeurs de nom occasionnel aléatoires mémorisées.

Le champ Indice de nom occasionnel de rattachement dit au nœud correspondant quelle valeur de nom occasionnel utiliser quand il produit le jeton de génération de clé de rattachement.

Le champ Indice de nom occasionnel d'entretien est ignoré dans les demandes de suppression de lien. Autrement, il dit au nœud correspondant quelle valeur de nom occasionnel utiliser quand il produit le jeton de génération de clé d'entretien.

6.2.7 Données d'autorisation de lien

L'option Données d'autorisation de lien n'a pas d'exigence d'alignement en tant que telle. Cependant, comme cette option doit être la dernière option de mobilité, une exigence implicite d'alignement est 8n + 2. Le format de cette option est le suivant :



L'option Données d'autorisation de lien est valide dans la mise à jour de lien et l'accusé de réception de lien.

Le champ Longueur d'option contient la longueur de l'authentifiant en octets.

Le champ Authentifiant contient une valeur cryptographique qui peut être utilisée pour déterminer que le message en question vient de la bonne autorité. Les règles pour calculer cette valeur dépendent de la procédure d'autorisation utilisée.

Pour la procédure d'acheminement de retour, cette option peut apparaître dans la mise à jour de lien et l'accusé de réception de liens. Les règles pour calculer la valeur de l'authentifiant sont les suivantes :

Données de mobilité = adresse d'entretien | correspondant | données de MH
Authentifiant = First (96, HMAC_SHA1 (Kbm, données de mobilité))

Où | note l'enchaînement. "adresse d'entretien" est l'adresse d'entretien qui va être enregistrée pour le nœud mobile si la mise à jour de lien réussit, ou l'adresse de rattachement du nœud mobile si cette option est utilisée dans un désenregistrement. Noter aussi que cette adresse peut être différente de l'adresse de source du message de mise à jour de lien, si l'option de mobilité Adresse d'entretien de remplacement est utilisée, ou quand la durée de vie du lien est réglée à zéro.

Le "correspondant" est l'adresse IPv6 du nœud correspondant. Noter que si le message est envoyé à une destination qui est elle-même mobile, l'adresse du "correspondant" peut n'être pas l'adresse qui se trouve dans le champ Adresse de destination de l'en-tête IPv6 ; l'adresse de rattachement provenant de l'en-tête d'acheminement de type 2 devrait être plutôt utilisée.

"Données de MH" est le contenu de l'en-tête de mobilité, à l'exclusion du champ Authentifiant lui-même. La valeur de l'authentifiant est calculée comme si le champ Somme de contrôle dans l'en-tête de mobilité était zéro. La somme de contrôle dans le paquet transmis est quand même calculée de la façon usuelle, avec l'authentifiant calculé faisant partie du paquet protégé par la somme de contrôle. Kbm est la clé de gestion de lien, qui est normalement créée en utilisant les noms

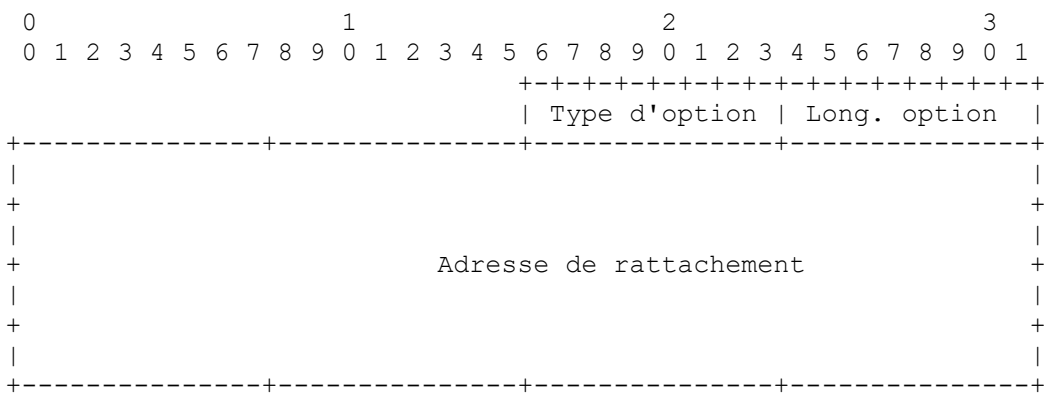
occasionnels fournis par le nœud correspondant (voir au paragraphe 9.4). Noter qu'alors que le contenu d'une potentielle option de destination Adresse de rattachement n'est pas couvert par cette formule, les règles pour le calcul de la Kbm ne prennent pas en compte l'adresse de rattachement. Cela assure que le MAC va être différent pour des adresses de rattachement différentes.

Les 96 premiers bits du résultat du MAC sont utilisés comme champ Authentifiant.

6.3 Option Adresse de rattachement

L'option Adresse de rattachement est portée par l'en-tête d'extension Option de destination (valeur de prochain en-tête = 60). Elle est utilisée dans un paquet envoyé par un nœud mobile lorsque il est hors de chez lui, pour informer le receveur de l'adresse de rattachement du nœud mobile.

L'option Adresse de rattachement est codée en format de TLV comme suit :



Type d'option : 201 (0xC9)

Longueur d'option : entier non signé de 8 bits. Longueur de l'option, en octets, excluant les champs Type d'option et Longueur d'option. Ce champ DOIT être réglé à 16.

Adresse de rattachement : adresse de rattachement du nœud mobile qui envoie le paquet. Cette adresse DOIT être une adresse d'acheminement en envoi individuel.

L'exigence d'alignement [RFC2460] pour l'option Adresse de rattachement est 8n + 6.

Les trois bits de plus fort poids du champ Type d'option sont codés pour indiquer le traitement spécifique de l'option [RFC2460] ; pour l'option Adresse de rattachement, ces trois bits sont réglés à 110. Cela indique les exigences de traitement suivantes :

- Tout nœud IPv6 qui ne reconnaît pas le type d'option doit éliminer le paquet, et si l'adresse de destination du paquet n'était pas une adresse de diffusion groupée, retourner un message ICMP "Problème de paramètre", code 2, à l'adresse de source du paquet. Le champ Pointeur dans le message ICMP DEVRAIT pointer sur le champ Type d'option. Autrement, pour les adresses de diffusion groupée, le message ICMP NE DOIT PAS être envoyé.
- Les données au sein de l'option ne peuvent pas changer en route pour la destination finale du paquet.

L'option Adresse de rattachement DOIT être placée comme suit :

- Après l'en-tête d'acheminement, si cet en-tête est présent
- Avant l'en-tête de fragment, si cet en-tête est présent
  Avant l'en-tête AH ou l'en-tête ESP, si l'un de ces en-têtes est présent.

Pour chaque en-tête de paquet IPv6, l'option Adresse de rattachement NE DOIT PAS apparaître plus d'une fois. Cependant, un paquet encapsulé [RFC2473] PEUT contenir une option Adresse de rattachement séparée associée à chaque en-tête IP encapsulant.

L'inclusion d'une option de destination Adresse de rattachement dans un paquet affecte le traitement par le nœud receveur de ce seul paquet. Aucun état n'est créé ou modifié dans le nœud receveur par suite de la réception d'une option Adresse de rattachement dans un paquet. En particulier, la présence d'une option Adresse de rattachement dans un paquet reçu NE DOIT PAS altérer le contenu de l'antémémoire de liens du receveur et NE DOIT PAS causer de changement de l'acheminement des paquets envoyés ensuite par ce nœud receveur.

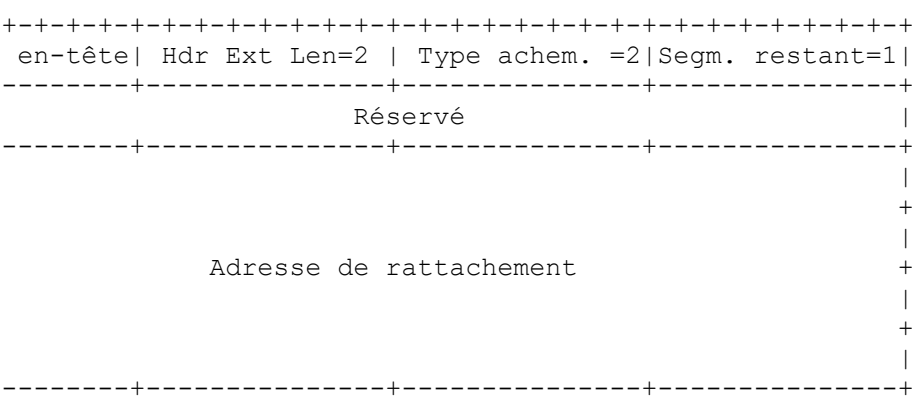
6.4 En-tête d'acheminement de type 2

IPv6 mobile définit une nouvelle variante d'en-tête d'acheminement, l'en-tête d'acheminement de type 2, pour permettre au paquet d'être acheminé directement d'un correspondant à l'adresse d'entretien du nœud mobile. L'adresse d'entretien du nœud mobile est insérée dans le champ Adresse de destination IPv6. Une fois le paquet arrivé à l'adresse d'entretien, le nœud mobile restitue son adresse de rattachement à partir de l'en-tête d'acheminement, et cela est utilisé comme adresse de destination finale pour le paquet.

Le nouvel en-tête d'acheminement utilise un type différent de celui défini pour l'acheminement "régulier" de source IPv6, permettant aux pare-feu d'appliquer des règles différentes de celles de IPv6 mobile aux paquets en acheminement de source. Ce type d'en-tête d'acheminement (type 2) se limite à porter une seule adresse IPv6. Tous les nœuds IPv6 qui traitent cet en-tête d'acheminement DOIVENT vérifier que l'adresse contenue dedans est la propre adresse de rattachement du nœud afin d'empêcher les paquets d'être transmis hors du nœud. L'adresse IP contenue dans l'en-tête d'acheminement, comme elle est l'adresse de rattachement du nœud mobile, DOIT être une adresse d'acheminement en envoi individuel. De plus, si la portée de l'adresse de rattachement est plus petite que celle de l'adresse d'entretien, le nœud mobile DOIT éliminer le paquet (voir au paragraphe 4.6).

6.4.1 Format

L'en-tête d'acheminement de type 2 a le format suivant :



Prochain en-tête : sélecteur de 8 bits. Identifie le type de l'en-tête qui suit immédiatement l'en-tête d'acheminement. Utilise les mêmes valeurs que le champ Prochain en-tête IPv6 [RFC2460].

Hdr Ext Len : 2 (entier non signé de 8 bits) ; longueur de l'en-tête d'acheminement en unités de 8 octets, non inclus les 8 premiers octets.

Type d'acheminement : 2 (entier non signé de 8 bits).

Segment restant : 1 (entier non signé de 8 bits).

Réservé : champ réservé de 32 bits. Valeur initialisée à zéro à l'envoi, et ignorée par le receveur.

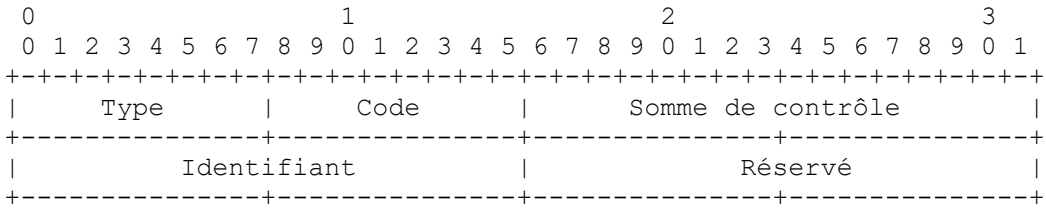
Adresse de rattachement : adresse de rattachement du nœud mobile de destination.

Pour un en-tête d'acheminement de type 2, la longueur de l'extension d'en-tête DOIT être 2. La valeur de "Segments à gauche décrit le nombre de segments de chemin restants, c'est-à-dire, le nombre de nœuds intermédiaires explicitement listés à visiter avant d'atteindre la destination finale. Segments restants DOIT être 1. Les règles d'ordre pour les en-têtes d'extension dans un paquet IPv6 sont décrites au paragraphe 4.1 de la [RFC2460]. L'en-tête d'acheminement de type 2 défini pour IPv6 mobile suit le même ordre que les autres en-têtes d'acheminement. Si un autre en-tête d'acheminement est présent avec un en-tête d'acheminement de type 2, l'en-tête d'acheminement de type 2 devrait suivre l'autre en-tête d'acheminement. Un paquet qui contient une telle encapsulation incorporée devrait être créé comme si l'en-tête d'acheminement interne (type 2) était construit d'abord et ensuite traité comme un paquet original par le processus de construction d'en-tête pour l'autre en-tête d'acheminement.

De plus, les procédures générales définies par IPv6 pour les en-têtes d'acheminement suggèrent que un en-tête d'acheminement reçu PEUT être automatiquement "inversé" pour construire un en-tête d'acheminement à utiliser pour tout paquet de réponse envoyé par les protocoles de couche supérieure, si le paquet reçu est authentifié [RFC2460]. Ceci NE DOIT PAS être fait automatiquement pour les en-têtes d'acheminement de type 2.

6.5 Message ICMP de demande de découverte d'adresse d'agent de rattachement

Le message ICMP Demande de découverte d'adresse d'agent de rattachement est utilisé par un nœud mobile pour initier le mécanisme de découverte dynamique d'adresse d'agent de rattachement, comme décrit au paragraphe 11.4.1. Le nœud mobile envoie le message Demande de découverte d'adresse d'agent de rattachement aux adresses d'envoi à la cantonade d'agents de rattachement IPv6 mobile [RFC2526] pour son propre préfixe de sous réseau de rattachement. (Noter que les adresses d'envoi à la cantonade actuellement définies peuvent ne pas fonctionner avec toutes les longueurs de préfixe autres que celles définies dans les [RFC4291] [RFC3627].)



Type : 144

Code : 0

Somme de contrôle : la somme de contrôle ICMP [RFC4443].

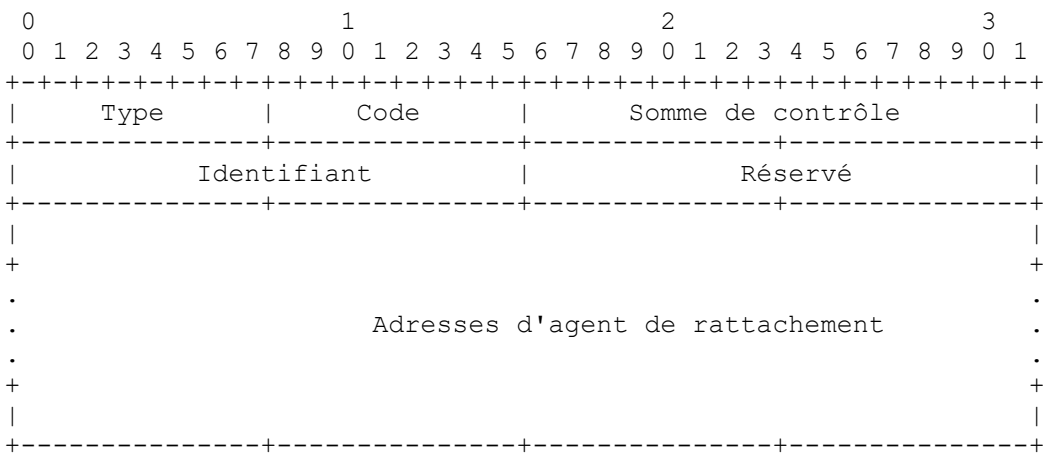
Identifiant : un identifiant pour aider à confronter les messages de réponse de découverte d'adresse d'agent de rattachement à ce message Demande de découverte d'adresse d'agent de rattachement.

Réservé : Ce champ est inutilisé. Il DOIT être initialisé à zéro à l'envoi et DOIT être ignoré par le receveur.

L'adresse de source du paquet de message Demande de découverte d'adresse d'agent de rattachement est normalement une des adresses d'entretien courantes du nœud mobile. Au moment d'effectuer cette procédure de découverte dynamique d'adresse d'agent de rattachement, il est probable que le nœud mobile n'est pas enregistré auprès d'un agent de rattachement. Donc, ni la nature de l'adresse ni l'identité du nœud mobile ne peuvent être établies à ce moment. L'agent de rattachement DOIT alors retourner le message de réponse de découverte d'adresse d'agent de rattachement directement à l'adresse de source choisie par le nœud mobile.

6.6 Message ICMP de réponse de découverte d'adresse d'agent de rattachement

Le message ICMP de réponse de découverte d'adresse d'agent de rattachement est utilisé par un agent de rattachement pour répondre à un nœud mobile qui utilise le mécanisme de découverte dynamique d'adresse d'agent de rattachement, comme décrit au paragraphe 10.5.



Type : 145
Code : 0
Somme de contrôle : somme de contrôle ICMP [RFC4443].

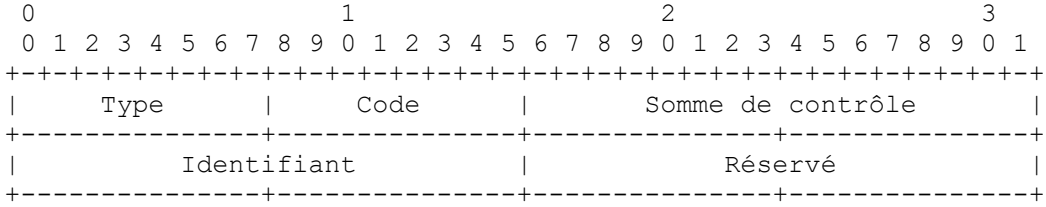
Identifiant : identifiant provenant du message Demande de découverte d'adresse d'agent de rattachement invoquant.

Réservé : Ce champ est inutilisé. Il DOIT être initialisé à zéro par l'envoyeur et DOIT être ignoré par le receveur.

Adresses d'agent de rattachement : liste des adresses des agents de rattachement sur la liaison de rattachement pour le nœud mobile. Le nombre des adresses présentées dans la liste est indiqué par la longueur restante du paquet IPv6 portant le message de réponse de découverte d'adresse d'agent de rattachement.

6.7 Format du message ICMP Sollicitation de préfixe mobile

Le message ICMP Sollicitation de préfixe mobile est envoyé par un nœud mobile à son agent de rattachement lorsque il est hors de chez lui. L'objet de ce message est de solliciter une annonce de préfixe mobile de la part de l'agent de rattachement, ce qui va permettre au nœud mobile de collecter des informations de préfixe sur son réseau de rattachement. Ces informations peuvent être utilisées pour configurer et mettre à jour la ou les adresses de rattachement, conformément aux changements d'informations de préfixe fournies par l'agent de rattachement.



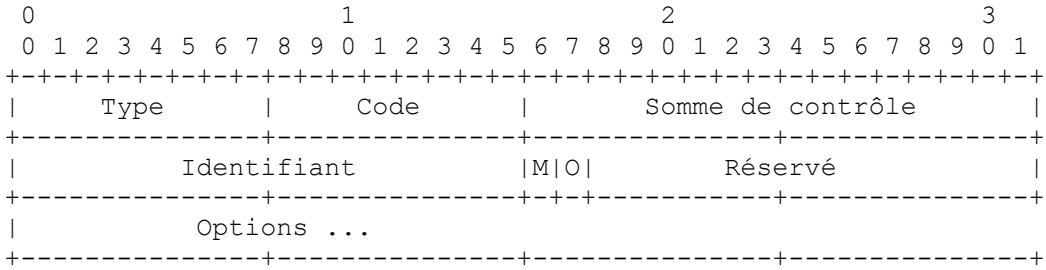
Champs IP :
Adresse de source : adresse d'entretien du nœud mobile.
Adresse de destination : adresse de l'agent de rattachement du nœud mobile. Cet agent de rattachement doit être sur la liaison dont le nœud mobile souhaite apprendre les informations de préfixe.
Limite de bond : réglée à une valeur initiale de limite de bond, comme pour tout autre paquet en envoi individuel envoyé par le nœud mobile.
Option de destination : : une option de destination Adresse de rattachement DOIT être incluse.
En-tête ESP : l'en-tête IPsec DOIT être pris en charge et DEVRAIT être utilisé comme décrit au paragraphe 5.4.

Champs ICMP :
Type : 146
Code : 0
Somme de contrôle : somme de contrôle ICMP [RFC4443].
Identifiant : pour aider à confronter une future annonce de préfixe mobile à cette sollicitation de préfixe mobile.
Réservé : Ce champ est inutilisé. Il DOIT être initialisé à zéro à l'envoi et DOIT être ignoré par le receveur.

Les messages Sollicitation de préfixe mobile peuvent avoir des options. Ces options DOIVENT utiliser le format d'option défini dans la découverte de voisin [RFC4861]. Le présent document ne définit aucun type d'option pour le message Sollicitation de préfixe mobile, mais de futurs documents pourront définir de nouvelles options. Les agents de rattachement DOIVENT ignorer en silence toute option qu'il ne reconnaissent pas et continuer le traitement du message.

6.8 Format du message ICMP Annonce de préfixe mobile

Un agent de rattachement va envoyer une annonce de préfixe mobile à un nœud mobile pour distribuer les informations de préfixes sur la liaison de rattachement lorsque le nœud mobile voyage hors de son réseau de rattachement. Cela va se produire en réponse à une sollicitation de préfixe mobile avec une annonce, ou par une annonce non sollicitée envoyée conformément aux règles du paragraphe 10.6.



Champs IP :
Adresse de source : l'adresse de l'agent de rattachement telle que le nœud mobile s'attend à la voir (c'est-à-dire., même préfixe réseau).
Adresse de destination : si ce message est une réponse à une sollicitation de préfixe mobile, ce champ contient le champ Adresse de source provenant de ce paquet. Pour les messages non sollicités, l'adresse d'entretien du nœud mobile DEVRAIT être utilisée. Noter que les messages non sollicités ne peuvent être envoyés que si le nœud mobile est actuellement enregistré auprès de l'agent de rattachement.
En-tête d'acheminement : un en-tête d'acheminement de type 2 DOIT être inclus.
En-tête ESP : les en-têtes IPsec DOIVENT être pris en charge et DEVRAIENT être utilisés comme décrit en 5.4.

Champs ICMP :
Type : 147
Code : 0
Somme de contrôle : somme de contrôle ICMP [RFC4443].
Identifiant : un identifiant pour aider à confronter cette annonce de préfixe mobile à une précédente sollicitation de préfixe mobile.
M : fanion d'un bit de configuration d'adresse gérée. Quand il est établi, les hôtes utilisent le protocole administré (à états pleins) pour l'autoconfiguration d'adresse en plus de toute adresse autoconfigurée en utilisant l'autoconfiguration d'adresse sans état. L'utilisation de ce fanion est décrite dans les [RFC4861] et [RFC4862].
O : fanion d'un bit d'autre configuration à états pleins. Quand il est établi, les hôtes utilisent le protocole administré (à états pleins) pour l'autoconfiguration des autres informations (non d'adresse). L'utilisation de ce fanion est décrite dans les [RFC4861] et [RFC4862].
Réservé : Ce champ est inutilisé. Il DOIT être initialisé à zéro par l'envoyeur et DOIT être ignoré par le receveur.

Les messages d'annonce de préfixe mobile peuvent avoir des options. Ces options DOIVENT utiliser le format d'option défini dans la découverte de voisin [RFC4861]. Le présent document définit une option qui peut être portée dans un message d'annonce de préfixe mobile, mais de futurs documents pourront définir de nouvelles options. Les nœuds mobiles DOIVENT ignorer en silence toute option qu'il ne reconnaissent pas et continuer le traitement du message.

Informations de préfixe : chaque message contient une ou plusieurs options Informations de préfixe. Chaque option porte le ou les préfixes que le nœud mobile devrait utiliser pour configurer son ou ses adresses de rattachement. Le paragraphe 10.6 décrit quels préfixes devraient être annoncés au nœud mobile.

L'option Informations de préfixe est définie au paragraphe 4.6.2 de la découverte de voisin [RFC4861], avec les modifications définies au paragraphe 7.2 de la présente spécification. L'agent de rattachement DOIT utiliser cette option Informations de préfixe modifiée pour envoyer les préfixes de réseau de rattachement comme défini au paragraphe 10.6.1.

Si l'annonce est envoyée en réponse à une sollicitation de préfixe mobile, l'agent de rattachement DOIT copier la valeur de l'identifiant de ce message dans le champ Identifiant de l'annonce.

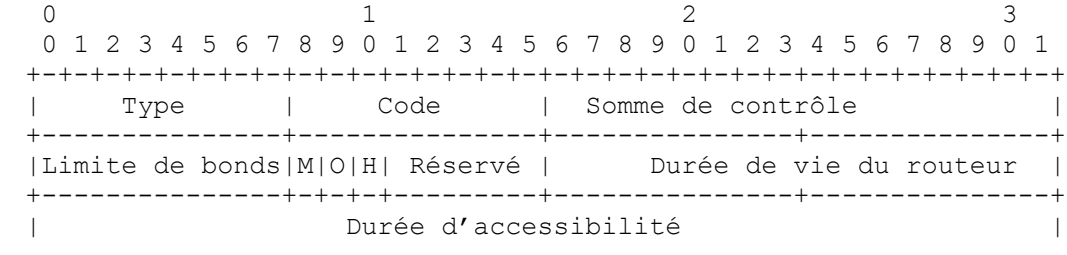
L'agent de rattachement NE DOIT PAS envoyer plus d'un message d'annonce de préfixe mobile par seconde à tout nœud mobile.

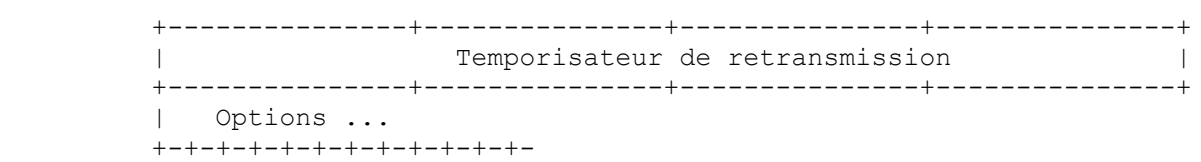
Les bits M et O DOIVENT être à zéro si la prise en charge de l'agent de rattachement DHCPv6 n'est pas fournie. Si cette prise en charge est assurée, ils sont alors réglés en accord avec les réglages administratifs du réseau de rattachement.

7. Modifications à la découverte de voisin IPv6

7.1 Format modifié du message Annonce de routeur

IPv6 mobile modifie le format du message Annonce de routeur [RFC4861] par l'ajout d'un seul fanion pour indiquer que le routeur qui envoie le message d'annonce sert d'agent de rattachement sur cette liaison. Le format du message d'annonce de routeur est le suivant :





Ce format représente les changements suivants par rapport à celui originellement spécifié pour la découverte de voisin [RFC4861] :

H (Agent de rattachement) : le bit H est établi dans une annonce de routeur pour indiquer que le routeur qui envoie cette annonce de routeur fonctionne aussi comme agent de rattachement IPv6 mobile sur cette liaison.

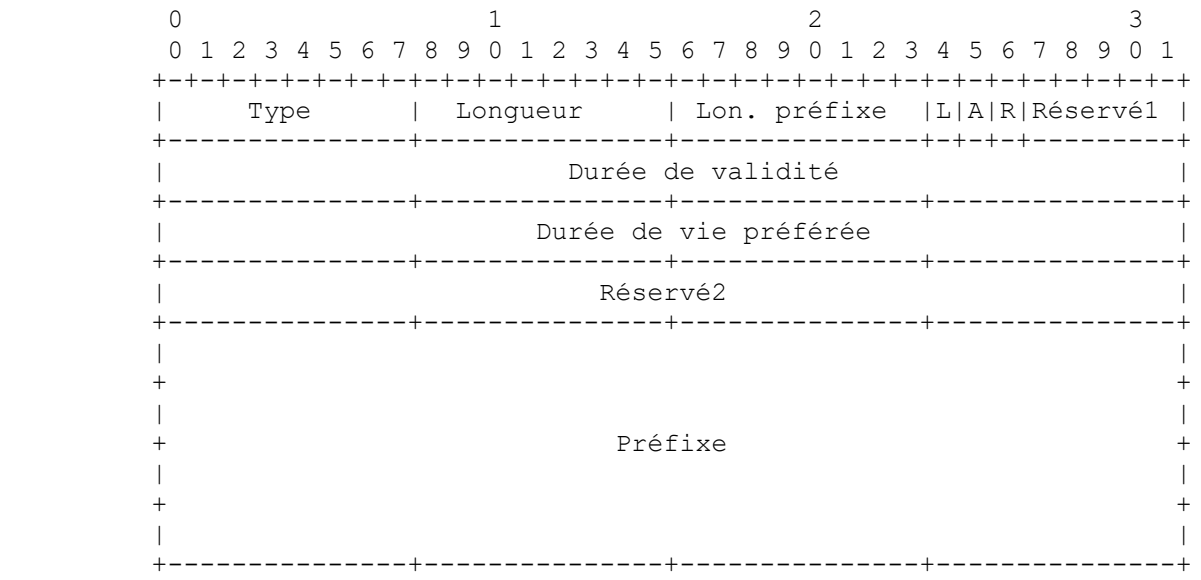
Réservé : réduit d'un champ de 6 bits à un champ de 5 bits pour tenir compte de l'ajout du bit ci-dessus.

7.2 Format modifié d'option Informations de préfixe

IPv6 mobile exige la connaissance de l'adresse mondiale d'un routeur pour construire la liste des agents de rattachement au titre du mécanisme de découverte dynamique d'adresse d'agent de rattachement.

Cependant, la découverte de voisin [RFC4861] annonce seulement l'adresse de liaison locale d'un routeur, en exigeant que cette adresse soit utilisée comme Adresse IP de source de chaque annonce de routeur.

IPv6 mobile étend la découverte de voisin à permettre à un routeur d'annoncer son adresse mondiale, par l'ajout d'un seul bit fanion dans le format d'une option Informations de préfixe à utiliser dans les messages Annonce de routeur. Le format de l'option Informations de préfixe est le suivant :



Ce format représente les changements suivants par rapport au format originellement spécifié pour la découverte de voisin [RFC4861] :

R (adresse de routeur) : fanion d'un bit d'adresse de routeur. Quand il est établi à 1, il indique que le champ Préfixe contient une adresse IP complète allouée au routeur envoyeur. Le préfixe indiqué est donné par les premiers bits de longueur de préfixe du champ Préfixe. L'adresse IP du routeur a la même portée et se conforme aux mêmes valeurs de durée de vie que le préfixe annoncé. Cette utilisation du champ Préfixe est compatible avec son utilisation pour annoncer le préfixe lui-même, car l'annonce de préfixe utilise seulement les bits de tête. L'interprétation de ce bit fanion est donc indépendante du traitement requis pour les bits fanions En-liaison (L) et Configuration d'adresse autonome (A).

Réservé1 : Réduit d'un champ de 6 bits à un champ de 5 bits pour tenir compte de l'ajout du bit ci-dessus.

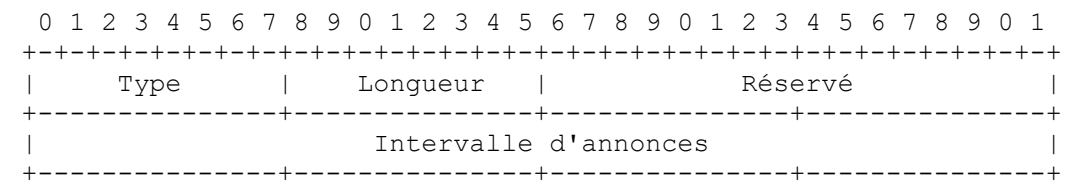
Dans une annonce de routeur, un agent de rattachement DOIT, et tous les autres routeurs PEUVENT, inclure au moins une option Informations de préfixe avec le bit Adresse de routeur (R) établi. La découverte de voisin [RFC4861] spécifie que, quand l'inclusion de toutes les options dans une annonce de routeur cause le dépassement de la MTU de liaison, plusieurs annonces peuvent être envoyées, chacune contenant un sous ensemble des options de découverte de voisin. Aussi, lorsque l'envoi d'annonces de routeur non sollicitées en diffusion groupée est plus fréquent que la limite spécifiée dans la RFC4861,

le routeur envoyeur n'a pas besoin d'inclure toutes les options dans chacune de ces annonces. Cependant, dans les deux cas, le routeur DEVRAIT inclure au moins une option Informations de préfixe avec le bit R (adresse de routeur) établi dans chacune de ces annonces, si ce bit est établi dans une annonce envoyée par le routeur.

De plus, l'exigence suivante peut aider les nœuds mobiles à détecter le mouvement. En interdisant les changements dans les préfixes pour la liaison, les routeurs qui envoient plusieurs annonces de routeur avec le bit R (adresse de routeur) établi dans certaines des options Informations de préfixe incluses DEVRAIT fournir au moins une option et adresse de routeur qui reste la même dans toutes les annonces.

7.3 Nouveau format d'option Intervalle d'annonces

IPv6 mobile définit une nouvelle option Intervalle d'annonces, utilisée dans les messages Annonce de routeur pour annoncer l'intervalle auquel le routeur envoyeur envoie les annonces de routeur non sollicitées en diffusion groupée. Le format de l'option Intervalle d'annonces est le suivant :



Type : 7

Longueur : entier non signé de 8 bits. Longueur de l'option (incluant les champs Type et Longueur) en unités de 8 octets. La valeur de ce champ DOIT être 1.

Réservé : Ce champ est inutilisé. Il DOIT être initialisé à zéro par l'envoyeur et DOIT être ignoré par le receveur.

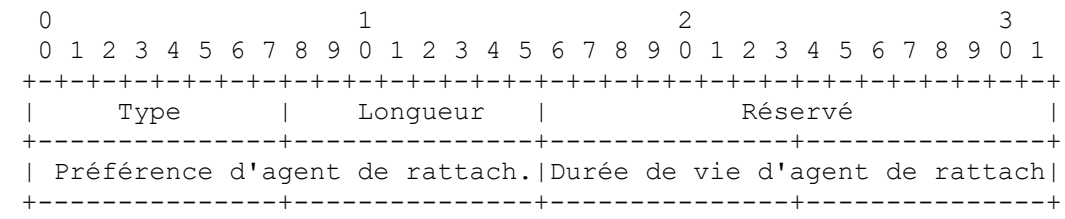
Intervalle d'annonces : entier non signé de 32 bits. Durée maximum, en millisecondes, entre les messages successifs d'annonces de routeur non sollicitées envoyés par ce routeur sur cette interface réseau. En utilisant les variables conceptuelles de configuration de routeur définies par la découverte de voisin [RFC4861], ce champ DOIT être égal à la valeur MaxRtrAdvInterval, exprimée en millisecondes.

Les routeurs PEUVENT inclure cette option dans leurs annonces de routeur. Un nœud mobile qui reçoit une annonce de routeur contenant cette option DEVRAIT utiliser l'intervalle d'annonces spécifié pour ce routeur dans son algorithme de détection de mouvement, comme décrit au paragraphe 11.5.1.

Cette option DOIT être ignorée en silence pour les autres messages de découverte de voisin.

7.4 Nouveau format d'option Informations d'agent de rattachement

IPv6 mobile définit une nouvelle option Informations d'agent de rattachement, utilisée dans les annonces de routeur envoyées par un agent de rattachement pour annoncer des informations spécifiques de cette fonction de routeur comme agent de rattachement. Le format de l'option Informations d'agent de rattachement est le suivant :



Type : 8

Longueur : entier non signé de 8 bits. Longueur de l'option (incluant les champs Type et Longueur) en unités de 8 octets. La valeur de ce champ DOIT être 1.

Réservé : Ce champ est inutilisé. Il DOIT être initialisé à zéro par l'envoyeur et DOIT être ignoré par le receveur.

Préférence d'agent de rattachement : entier non signé de 16 bits. La préférence pour l'agent de rattachement qui envoie cette annonce de routeur, à utiliser pour ordonner les adresses retournées à un nœud mobile dans le champ Adresses d'agent de rattachement d'un message de réponse de découverte d'adresse d'agent de rattachement. Les valeurs les plus fortes signifient qu'elles sont les préférées. Si cette option n'est pas incluse dans une annonce de routeur dans laquelle le bit H (agent de rattachement) est établi, la valeur de préférence pour cet agent de rattachement DOIT être considérée comme étant 0. Les plus grandes valeurs indiquent un agent de rattachement préférable à ceux qui ont des valeurs inférieures.

La configuration manuelle de la valeur de préférence d'agent de rattachement est décrite au paragraphe 8.4. De plus, l'agent de rattachement envoyeur PEUT régler dynamiquement la valeur de préférence d'agent de rattachement, par exemple, en la fondant sur le nombre de nœuds mobiles qu'il dessert actuellement ou sur ses ressources restantes pour servir des nœuds mobiles supplémentaires ; de tels réglages dynamiques sortent du domaine d'application du présent document. Cependant, un tel réglage dynamique de la préférence d'agent de rattachement DOIT régler la préférence de façon appropriée, par rapport à la valeur par défaut de préférence d'agent de rattachement de 0 qui peut être utilisée par certains agents de rattachement sur cette liaison (c'est-à-dire, un agent de rattachement qui n'inclut pas d'option Informations d'agent de rattachement dans ses annonces de routeur va être considéré comme ayant une valeur de préférence d'agent de rattachement de 0).

Durée de vie d'agent de rattachement : entier non signé de 16 bits. Durée de vie associée à l'agent de rattachement en secondes. La valeur par défaut est la même que pour la durée de vie de routeur, comme spécifié dans le corps principal de l'annonce de routeur. La valeur maximum correspond à 18,2 heures. Une valeur de 0 NE DOIT PAS être utilisée. La durée de vie de l'agent de rattachement ne s'applique qu'à l'utilité de ce routeur comme agent de rattachement ; elle ne s'applique pas aux informations contenues dans d'autres champs ou options de message.

Les agents de rattachement PEUVENT inclure cette option dans leurs annonces de routeur. Cette option NE DOIT PAS être incluse dans une annonce de routeur dans laquelle le bit H (agent de rattachement) (voir au paragraphe 7.1) n'est pas établi. Si cette option n'est pas incluse dans une annonce de routeur dans laquelle le bit H (agent de rattachement) est établi, la durée de vie pour cet agent de rattachement DOIT être considérée comme étant la même que la durée de vie de routeur dans l'annonce de routeur. Si plusieurs annonces sont envoyées au lieu d'une seule annonce de routeur en diffusion groupée non sollicitée plus grande, toutes les annonces avec le bit R (adresse de routeur) établi DOIVENT inclure cette option avec le même contenu ; sinon, cette option DOIT être omise dans toutes les annonces.

Cette option DOIT être ignorée en silence pour les autres messages de découverte de voisin.

Si la préférence d'agent de rattachement et la durée de vie d'agent de rattachement sont toutes deux réglées à leurs valeurs par défaut spécifiées ci-dessus, cette option NE DEVRAIT PAS être incluse dans les messages d'annonce de routeur envoyés par cet agent de rattachement.

7.5 Changements à l'envoi d'annonces de routeur

La spécification du protocole de découverte de voisin [RFC4861] limite les routeurs à un intervalle minimum de 3 secondes entre l'envoi de messages d'annonce de routeur non sollicitées en diffusion groupée à partir de toute interface réseau (limité par MinRtrAdvInterval *(intervalle minimum de retransmission d'annonce)* et MaxRtrAdvInterval *(intervalle maximum de retransmission d'annonce)*) en déclarant que "Les routeurs génèrent des annonces de routeur assez fréquemment pour que les hôtes apprennent leur présence en quelques minutes, mais pas assez fréquemment pour s'appuyer sur une absence d'annonce pour détecter une défaillance du routeur ; un algorithme séparé de détection d'inaccessibilité de voisin assure la détection des défaillances".

Cette limitation, ne convient cependant pas pour fournir une détection de mouvement en temps utile pour les nœuds mobiles. Les nœuds mobiles détectent leur propre mouvement en apprenant la présence de nouveaux routeurs lorsque le nœud mobile se déplace dans leur portée de transmission sans fil (ou se connecte physiquement à un nouveau réseau filaire) et en apprenant que les précédents routeurs ne sont plus accessibles. Les nœuds mobiles DOIVENT être capables de détecter rapidement quand ils passent sur une liaison desservie par un nouveau routeur, afin qu'ils puissent acquérir une nouvelle adresse d'entretien et envoyer des mises à jour de lien pour enregistrer cette adresse d'entretien auprès de leur agent de rattachement et le notifier aux nœuds correspondants comme nécessaire.

Une méthode qui peut fournir une plus rapide détection de mouvement est d'augmenter le taux d'envoi des annonces de routeur non sollicitées. IPv6 mobile relâche cette limite de telle façon que les routeurs PEUVENT envoyer plus fréquemment des annonces de routeur non sollicitées en diffusion groupée. Cette méthode peut être appliquée lorsque le routeur est supposé fournir le service aux nœuds mobiles visiteurs (par exemple, les interfaces de réseau sans fil) ou sur lesquels il sert d'agent de rattachement à un ou plusieurs nœuds mobiles (qui peuvent retourner chez eux et ont besoin d'entendre ses annonces).

Les routeurs qui prennent en charge la mobilité DEVRAIENT être capables d'être configurés avec une plus petite valeur de MinRtrAdvInterval et de MaxRtrAdvInterval pour permettre l'envoi plus fréquent d'annonces de routeur non sollicitées en diffusion groupée. Les valeurs minimum permises sont :
- MinRtrAdvInterval 0,03 seconde
- MaxRtrAdvInterval 0,07 seconde

Dans le cas où les intervalles et délais minimum sont utilisés, le temps moyen entre les annonces de routeur non sollicitées en diffusion groupée est de 50 ms. L'utilisation de ces limites modifiées DOIT être configurable (voir aussi la variable de configuration MinDelayBetweenRas *(délai minimum entre annonces de routeur)* à la Section 13 qui peut aussi devoir être modifiée en conséquence). Les systèmes où ces valeurs sont disponibles NE DOIVENT PAS les prendre comme valeurs par défaut, et DEVRAIENT avoir pour valeurs par défaut les valeurs spécifiées dans la découverte de voisin [RFC4861]. La connaissance du type d'interface réseau et de l'environnement de fonctionnement DEVRAIT être prise en compte pour la configuration de ces limites pour chaque interface réseau. C'est important avec certaines liaisons sans fil, où l'augmentation de la fréquence des balises de diffusion groupée peut causer des frais généraux considérables. Les routeurs DEVRAIENT adhérer aux intervalles spécifiés dans la [RFC4861], si ces frais généraux causerait une dégradation du service.

De plus, les possibles faibles valeurs de MaxRtrAdvInterval peuvent causer certains problèmes avec la détection de mouvement dans certains nœuds mobiles. Pour s'assurer que ce n'est pas un problème, les routeurs DEVRAIENT ajouter 20 ms à chaque intervalle d'annonce envoyé dans les annonces de routeur qui sont en dessous de 200 ms, afin de tenir compte des granularités de programmation chez le nœud mobile et chez le routeur.

Noter que les annonces de routeur en diffusion groupée ne sont pas toujours exigées dans certains réseaux sans fil qui ont une bande passante limitée. La détection de la mobilité ou les changements de liaison dans de tels réseaux peut être faite à des couches inférieures. Les annonces de routeur dans de tels réseaux DEVRAIENT n'être envoyées que sollicitées. Dans de tels réseaux, il DEVRAIT être possible de désactiver les annonces de routeur en diffusion groupée non sollicitées sur des interfaces spécifiques. MinRtrAdvInterval et MaxRtrAdvInterval peuvent être réglés dans ce cas à des valeurs supérieures.

Les agents de rattachement DOIVENT inclure l'option Adresse de source de couche de liaison dans toutes les annonces de routeur qu'ils envoient. Cela simplifie le processus de retour au réseau de rattachement, comme expliqué au paragraphe 11.5.5.

Noter que conformément à la découverte de voisin [RFC4861], AdvDefaultLifetime est par défaut fondé sur la valeur de MaxRtrAdvInterval. AdvDefaultLifetime est utilisé dans le champ Durée de vie du routeur des annonces de routeur. Ce champ étant exprimé en secondes, une petite valeur de MaxRtrAdvInterval peut résulter en une valeur de zéro pour ce champ. Pour empêcher cela, les routeurs DEVRAIENT conserver AdvDefaultLifetime au moins une seconde, même si l'utilisation de MaxRtrAdvInterval résulterait en une plus petite valeur.

8. Exigences pour les types de nœuds IPv6

IPv6 mobile pose des exigences particulières pour les fonctions fournies par les différents types de nœuds IPv6. La présente section récapitule ces exigences, et identifie la fonction que chaque exigence est destinée à prendre en charge.

Les exigences sont établies pour les groupes de nœuds suivants :
- Tous les nœuds IPv6.
- Tous les nœuds IPv6 qui prennent en charge l'optimisation de chemin.
- Tous les routeurs IPv6.
- Tous agents de rattachement IPv6 mobile.
- Tous les nœuds mobiles IPv6 mobile.

Il sort du domaine d'application de cette spécification de spécifier lesquels de ces groupes sont obligatoires dans IPv6. On décrit seulement ce qu'il est obligatoire de prendre en charge pour un nœud, par exemple, l'optimisation de chemin. D'autres spécifications sont attendues pour définir l'étendue de IPv6.

8.1 Tous nœuds IPv6

Tout nœud IPv6 peut à tout moment être un nœud correspondant d'un nœud mobile, soit en envoyant un paquet à un nœud mobile, soit en recevant un paquet provenant d'un nœud mobile. Il n'y a pas d'exigence DOIT spécifique de nœud mobile pour de tels nœuds, et les techniques IPv6 de base sont suffisantes. Si un nœud mobile tente d'établir l'optimisation de chemin avec un nœud avec seulement la prise en charge IPv6 de base, une erreur ICMP va signaler que le nœud ne prend

pas en charge de telles optimisations (paragraphe 11.3.5) et les communications vont s'écouler à travers l'agent de rattachement.

Un nœud IPv6 NE DOIT PAS prendre en charge les options de destination Adresse de rattachement, En-tête d'acheminement de type 2, ou En-tête de mobilité si il ne prend pas pleinement en charge les exigences citées dans les paragraphes qui suivent pour les fonctions d'optimisation de chemin, de nœud mobile, ou d'agent de rattachement.

8.2 Nœuds IPv6 qui prennent en charge l'optimisation de chemin

Les nœuds qui mettent en œuvre l'optimisation de chemin sont un sous ensemble de tous les nœuds IPv6 sur l'Internet. La capacité d'un nœud correspondant à participer à l'optimisation de chemin est essentielle pour le fonctionnement efficace de l'Internet IPv6, pour les raisons suivantes :

- o éviter l'encombrement dans le réseau de rattachement, et permettre l'utilisation d'un équipement d'agent de rattachement de moindres performances même pour prendre en charge des milliers de nœuds mobiles ;
- o réduire la charge du réseau sur tout l'Internet, car les appareils mobiles commencent à être prédominants ;
- o réduire la gigue et la latence pour les communications ;
- o augmenter la probabilité de succès de la signalisation de qualité de service (QS) lorsque le tunnelage est évité et, diminuer encore les sources d'encombrement ;
- o améliorer la robustesse aux partitions de réseau, à l'encombrement et autres problèmes, car moins de segments de chemin d'acheminement sont traversés.

Ces effets se combinent pour permettre de bien meilleures performances et robustesse pour les communications entre nœuds mobiles et nœuds IPv6 correspondants. L'optimisation de chemin introduit une petite quantité d'état supplémentaire pour les homologues, quelques messages en plus, et jusqu'à 1,5 délais d'aller-retour avant qu'elle puisse être activée. Cependant, on estime que les avantages dépassent de loin les coûts dans la plupart des cas. Le paragraphe 11.3.1 explique comment les nœuds mobiles peuvent éviter l'optimisation de chemin pour certains des cas restants, comme les communications à très court terme.

Les exigences suivantes s'appliquent à tous les nœuds correspondants qui prennent en charge l'optimisation de chemin :

- o Le nœud DOIT être capable de valider une option Adresse de rattachement en utilisant une entrée d'antémémoire de liens existante, comme décrit au paragraphe 9.3.1.
- o Le nœud DOIT être capable d'insérer un en-tête d'acheminement de type 2 dans les paquets à envoyer à un nœud mobile, comme décrit au paragraphe 9.3.2.
- o Sauf si le nœud correspondant agit aussi comme nœud mobile, il DOIT ignorer les en-têtes d'acheminement de type 2 et éliminer en silence tous les paquets qu'il reçoit avec de tels en-têtes.
- o Le nœud DEVRAIT être capable d'interpréter les messages ICMP comme décrit au paragraphe 9.3.4.
- o Le nœud DOIT être capable d'envoyer des messages Erreur de lien comme décrit au paragraphe 9.3.3.
- o Le nœud DOIT être capable de traiter les en-têtes de mobilité comme décrit au paragraphe 9.2.
- o Le nœud DOIT être capable de participer à une procédure d'acheminement de retour (paragraphe 9.4).
- o Le nœud DOIT être capable de traiter les messages Mise à jour de lien (paragraphe 9.5).
- o Le nœud DOIT être capable de retourner un accusé de réception de lien (paragraphe 9.5.4).
- o Le nœud DOIT être capable de tenir une antémémoire de liens des liens reçus dans les mises à jour de lien acceptées, comme décrit aux paragraphes 9.1 et 9.6.
- o Le nœud DEVRAIT permettre que l'optimisation de chemin soit administrativement activée ou désactivée. Elle DEVRAIT être activée par défaut.

8.3 Tous routeurs IPv6

Tous les routeurs IPv6, même ceux qui ne servent pas comme agent de rattachement pour IPv6 mobile, ont un effet sur la façon dont les nœuds mobiles peuvent communiquer :

- o Chaque routeur IPv6 DEVRAIT être capable d'envoyer une option Intervalle d'annonces (paragraphe 7.3) dans chacune de ses annonces de routeur [RFC4861], pour aider à la détection de mouvement par les nœuds mobiles (comme au paragraphe 11.5.1). L'utilisation de cette option dans les annonces de routeur DEVRAIT être configurable.
- o Chaque routeur IPv6 DEVRAIT être capable de la prise en charge de l'envoi d'annonces de routeur non sollicitées en diffusion groupée au taux plus rapide décrit au paragraphe 7.5. Si le routeur prend en charge un taux plus rapide, le taux utilisé DOIT être configurable.
- o Chaque routeur DEVRAIT inclure au moins un préfixe avec le bit R (adresse de routeur) établi et avec sa pleine adresse IP dans ses annonces de routeur (comme décrit au paragraphe 7.2).
- o Les routeurs qui prennent en charge le filtrage des paquets avec des en-têtes d'acheminement DEVRAIENT prendre en charge des règles différentes pour les en-têtes d'acheminement de type 0 et de type 2 (voir au paragraphe 6.4) afin que le filtrage des paquets en acheminement de source (type 0) ne limite pas nécessairement le trafic IPv6 qui est délivré via les en-têtes d'acheminement de type 2.

8.4 Agents de rattachement IPv6

Afin qu'un nœud mobile fonctionne correctement lorsque il est hors de chez lui, au moins un routeur IPv6 sur la liaison de rattachement du nœud mobile doit fonctionner comme agent de rattachement pour le nœud mobile. Les exigences supplémentaires suivantes s'appliquent à tous les routeurs IPv6 qui servent d'agent de rattachement :

- Chaque agent de rattachement DOIT être capable de maintenir une entrée dans son antémémoire de liens pour chaque nœud mobile pour lequel il sert d'agent de rattachement (paragraphes 10.1 et 10.3.1).
- Chaque agent de rattachement DOIT être capable d'intercepter les paquets (en utilisant la découverte de voisin mandataire [RFC4861]) adressés au nœud mobile pour lequel il sert actuellement d'agent de rattachement, sur la liaison de rattachement de ce nœud mobile, pendant que le nœud mobile est hors de chez lui (paragraphe 10.4.1).
- Chaque agent de rattachement DOIT être capable d'encapsuler [RFC2473] de tels paquets interceptés afin de les tunneler à l'adresse d'entretien principale pour le nœud mobile indiqué dans son lien dans l'antémémoire de liens de l'agent de rattachement (paragraphe 10.4.2).
- Chaque agent de rattachement DOIT prendre en charge la désencapsulation [RFC2473] des paquets en tunnelage inverse qui lui sont envoyés de l'adresse de rattachement du nœud mobile. Chaque agent de rattachement DOIT aussi vérifier que l'adresse de source dans les paquets tunnelés correspond à la localisation actuellement enregistrée du nœud mobile (paragraphe 10.4.5).
- Le nœud DOIT être capable de traiter les en-têtes de mobilité comme décrit au paragraphe 10.2.
- Chaque agent de rattachement DOIT être capable de retourner un accusé de réception de lien en réponse à une mise à jour de lien (paragraphe 10.3.1).
- Chaque agent de rattachement DOIT tenir une liste séparée des agents de rattachement pour chaque liaison sur laquelle il sert d'agent de rattachement, comme décrit aux paragraphes 10.1 et 10.5.1.
- Chaque agent de rattachement DOIT être capable d'accepter les paquets adressés à l'adresse IPv6 mobile d'envoi à la cantonade des agents de rattachement [RFC2526] pour le sous réseau sur lequel il sert d'agent de rattachement, et DOIT être capable de participer à la découverte dynamique d'adresse d'agent de rattachement (paragraphe 10.5).
- Chaque agent de rattachement DEVRAIT prendre en charge un mécanisme de configuration permettant à un administrateur du système de régler manuellement la valeur à envoyer par cet agent de rattachement dans le champ Préférence d'agent de rattachement de l'option Informations d'agent de rattachement dans les annonces de routeur qu'il envoie (paragraphe 7.4).
- Chaque agent de rattachement DEVRAIT prendre en charge l'envoi d'annonces de préfixe ICMP mobile (paragraphe 6.8) et DEVRAIT répondre aux sollicitations de préfixe mobile (paragraphe 6.7). Si il est pris en charge, ce comportement DOIT être configurable, afin que les agents de rattachement puissent être configurés pour éviter d'envoyer de telles annonces de préfixe conformément aux besoins de l'administration de réseau dans le domaine de rattachement.
- Chaque agent de rattachement DOIT prendre en charge IPsec ESP pour la protection des paquets appartenant à la procédure d'acheminement de retour (paragraphe 10.4.6).
- Chaque agent de rattachement DEVRAIT prendre en charge les protocoles de contrôle de l'appartenance au groupe de diffusion groupée comme décrit au paragraphe 10.4.3. Si cette prise en charge est fournie, l'agent de rattachement DOIT être capable de l'utiliser pour déterminer quels paquets de données en diffusion groupée transmettre via le tunnel au nœud mobile.
- Les agents de rattachement PEUVENT prendre en charge l'autoconfiguration d'adresse à états pleins pour les nœuds mobiles comme décrit au paragraphe 10.4.4.

8.5 Nœuds mobiles IPv6

Finalement, les exigences suivantes s'appliquent à tous les nœuds IPv6 capables de fonctionner comme nœuds mobiles :

- Le nœud DOIT tenir une liste de mises à jour de liens (paragraphe 11.1).
- Le nœud DOIT prendre en charge l'envoi de paquets contenant une option Adresse de rattachement (paragraphe 11.3.1), et suivre l'interaction IPsec requise (paragraphe 11.3.2).
- Le nœud DOIT être capable d'effectuer l'encapsulation et la désencapsulation IPv6 [RFC2473].
- Le nœud DOIT être capable de traiter l'en-tête d'acheminement de type 2 comme défini aux paragraphes 6.4 et 11.3.3.
- Le nœud DOIT prendre en charge la réception d'un message Erreur de lien (paragraphe 11.3.6).
- Le nœud DOIT prendre en charge la réception des erreurs ICMP (paragraphe 11.3.5).
- Le nœud DOIT prendre en charge la détection de mouvement, la formation d'adresse d'entretien, et le retour chez lui (paragraphe 11.5).
- Le nœud DOIT être capable de traiter les en-têtes de mobilité comme décrit au paragraphe 11.2.
- Le nœud DOIT prendre en charge la procédure d'acheminement de retour (paragraphe 11.6).
- Le nœud DOIT être capable d'envoyer des mises à jour de lien, comme spécifié aux paragraphes 11.7.1 et 11.7.2.
- Le nœud DOIT être capable de recevoir et traiter les accusés de réception de lien, comme spécifié au paragraphe 11.7.3.
- Le nœud DOIT prendre en charge la réception d'une demande de rafraîchissement de lien (paragraphe 6.1.2) en répondant avec une mise à jour de lien.

- o Le nœud DOIT prendre en charge la réception des annonces de préfixe mobile (paragraphe 11.4.3) et reconfigurer son adresse de rattachement sur la base des informations de préfixe qui y sont contenues.
- o Le nœud DEVRAIT prendre en charge l'utilisation du mécanisme de découverte dynamique d'adresse d'agent de rattachement, comme décrit au paragraphe 11.4.1.
- o Le nœud DOIT permettre que l'optimisation de chemin soit activée ou désactivée administrativement. Elle DEVRAIT être activée par défaut.
- o Le nœud PEUT prendre en charge la partie écouteur d'adresse de diffusion groupée d'un protocole d'appartenance à un groupe de diffusion groupée, comme décrit au paragraphe 11.3.4. Si cette prise en charge est fournie, le nœud mobile DOIT être capable de recevoir des paquets tunnelés en diffusion groupée provenant de l'agent de rattachement.
- o Le nœud PEUT prendre en charge les mécanismes d'autoconfiguration d'adresse à états pleins comme DHCPv6 [RFC3315] sur l'interface représentée par le tunnel à l'agent de rattachement.

9. Fonctionnement du nœud correspondant

9.1 Structures de données conceptuelles

Les nœuds IPv6 qui prennent en charge l'optimisation de chemin tiennent une antémémoire de liens des liens pour les autres nœuds. Une antémémoire de liens séparée DEVRAIT être tenue par chaque nœud IPv6 pour chacune de ses adresses d'acheminement en envoi individuel. L'antémémoire de liens PEUT être mise en œuvre de toute manière cohérente avec le comportement externe décrit dans le présent document, par exemple, en étant combinée avec l'antémémoire de destination du nœud comme tenue par la découverte de voisin [RFC4861]. Quand un paquet est envoyé, l'antémémoire de liens est examinée avant l'antémémoire de destination conceptuelle de découverte de voisin [RFC4861].

Chaque entrée d'antémémoire de liens contient conceptuellement les champs suivants :

- o L'adresse de rattachement du nœud mobile pour lequel c'est l'entrée d'antémémoire de liens. Ce champ est utilisé comme clé pour la recherche dans l'antémémoire de liens pour l'adresse de destination d'un paquet envoyé.
- o L'adresse d'entretien pour le nœud mobile indiqué par le champ Adresse de rattachement dans cette entrée d'antémémoire de liens.
- o Une valeur de durée de vie, indiquant la durée de vie restante pour cette entrée d'antémémoire de liens. La valeur de durée de vie est initialisée pour le champ Durée de vie dans la mise à jour de lien qui a créé ou a pour la dernière fois modifié l'antémémoire de liens. Un nœud correspondant PEUT choisir une plus petite durée de vie pour l'entrée d'antémémoire de liens, et fournir cette valeur au nœud mobile dans le message Accusé de réception de lien.
- o Un fanion indiquant si cette rentrée d'antémémoire de liens est ou non une entrée d'enregistrement de rattachement (applicable seulement sur les nœuds qui prennent en charge la fonction d'agent de rattachement).
- o La valeur maximum du champ Numéro de séquence reçu dans une précédente mise à jour de lien pour cette adresse de rattachement. Le champ Numéro de séquence fait 16 bits. Les valeurs de numéro de séquence DOIVENT être comparées modulo 2**16 comme expliqué au paragraphe 9.5.1.
- o Les informations d'usage pour cette entrée d'antémémoire de liens. Ceci est nécessaire pour mettre en œuvre la politique de remplacement d'antémémoire utilisée dans l'antémémoire de liens. Une utilisation récente d'une entrée d'antémémoire sert aussi d'indication qu'une demande de rafraîchissement de lien devrait être envoyée quand la durée de vie de cette entrée est proche de l'expiration.

Les entrées d'antémémoire de liens non marquées comme enregistrements de rattachement PEUVENT être remplacées à tout moment par toute politique locale raisonnable de remplacement d'antémémoire mais NE DEVRAIENT PAS être supprimées sans nécessité. L'antémémoire de liens pour toute adresse IPv6 d'un nœud peut contenir au plus une entrée pour chaque adresse de rattachement de nœud mobile. Le contenu de l'antémémoire de liens d'un nœud NE DOIT PAS être changé en réponse à une option Adresse de rattachement dans un paquet reçu.

9.2 Traitement des en-têtes de mobilité

Le traitement de l'en-tête de mobilité DOIT observer les règles suivantes :

- o La somme de contrôle doit être vérifiée conformément au paragraphe 6.1. Si elle est invalide, le nœud DOIT éliminer en silence le message.
- o Le champ Type de MH DOIT avoir une valeur connue (paragraphe 6.1.1). Autrement, le nœud DOIT éliminer le message et produire un message Erreur de lien comme décrit au paragraphe 9.3.3, avec le champ État réglé à 2 (valeur de type de MH non reconnue).
- o Le champ Protocole de charge utile DOIT être IPPROTO_NONE (59 en décimal). Autrement, le nœud DOIT éliminer le message et DEVRAIT envoyer un Problème de paramètre ICMP, code 0, directement à l'adresse de source du paquet comme spécifié dans la [RFC4443]. Donc, aucune information d'antémémoire de liens n'est utilisée dans l'envoi du message ICMP. Le champ Pointeur dans le message ICMP DEVRAIT pointer sur le champ Protocole de charge utile.
- o Le champ Longueur d'en-tête dans l'en-tête de mobilité NE DOIT PAS être moins que la longueur spécifiée pour ce type particulier de message au paragraphe 6.1. Autrement, le nœud DOIT éliminer le message et DEVRAIT envoyer un

Problème de paramètre ICMP, code 0, directement à l'adresse de source du paquet comme spécifié dans la [RFC4443]. (Les informations de l'antémémoire de liens ne sont là encore pas utilisées.) Le champ Pointeur dans le message ICMP DEVRAIT pointer sur le champ Longueur d'en-tête.

Les vérifications suivantes dépendent de l'en-tête de mobilité particulier.

9.3 Traitement des paquets

Cette section décrit comment le nœud correspondant envoie les paquets au nœud mobile, et en reçoit les paquets.

9.3.1 Réception des paquets avec l'option Adresse de rattachement

Les paquets qui contiennent une option Adresse de rattachement DOIVENT être éliminés si l'adresse de rattachement donnée n'est pas une adresse d'acheminement en envoi individuel.

Les nœuds mobiles peuvent inclure une option de destination Adresse de rattachement dans un paquet si ils estiment que le nœud correspondant a une entrée d'antémémoire de liens pour l'adresse de rattachement d'un nœud mobile. Si la valeur de prochain en-tête de l'option Destination est une des suivantes : {50 (ESP), 51 (AH), 135 (En-tête de mobilité)}, le paquet DEVRAIT être traité normalement. Autrement, le paquet DOIT être éliminé si il n'y a pas d'entrée correspondante d'antémémoire de liens. Une entrée d'antémémoire de liens correspondante DOIT avoir la même adresse de rattachement que ce qui apparaît dans l'Adresse de rattachement de l'option de destination, et l'adresse d'entretien actuellement enregistrée DOIT être égale à l'adresse de source du paquet.

Si le paquet est éliminé du fait des essais ci-dessus, le nœud correspondant DOIT envoyer le message Erreur de lien comme décrit au paragraphe 9.3.3. Le champ État dans ce message devrait être réglé à 1 (lien inconnu pour l'option de destination Adresse de rattachement).

Le nœud correspondant DOIT traiter l'option d'une manière cohérente avec l'échange du champ Adresse de rattachement provenant de l'option Adresse de rattachement dans l'en-tête IPv6 et en y remplaçant la valeur d'origine du champ Adresse de source. Après que toutes les options IPv6 ont été traitées, il DOIT être possible aux couches supérieures de traiter le paquet sans savoir si il est venu à l'origine d'une adresse d'entretien ou si une option Adresse de rattachement a été utilisée.

L'utilisation de l'en-tête d'authentification (AH) IPsec pour l'option Adresse de rattachement n'est pas exigée, sauf que si l'en-tête IPv6 d'un paquet est couvert par AH, l'authentification DOIT alors aussi couvrir l'option Adresse de rattachement ; cette couverture est réalisée automatiquement par la définition du code de type d'option pour l'option Adresse de rattachement, car il indique que les données au sein de l'option ne peuvent pas changer en route pour la destination finale du paquet, et donc l'option est incluse dans le calcul de AH. En exigeant que toute authentification de l'en-tête IPv6 couvre aussi l'option Adresse de rattachement, la sécurité du champ Adresse de source dans l'en-tête IPv6 n'est pas compromise par la présence d'une option Adresse de rattachement.

Quand il tente de vérifier les données d'authentification AH dans un paquet qui contient une option Adresse de rattachement, le nœud receveur DOIT calculer les données d'authentification AH comme si ce qui suit était vrai : l'option Adresse de rattachement contient l'adresse d'entretien, et le champ Adresse IPv6 de source de l'en-tête IPv6 contient l'adresse de rattachement. Ceci se conforme au calcul spécifié au paragraphe 11.3.2.

9.3.2 Envoi des paquets à un nœud mobile

Avant tout envoi de paquet, le nœud envoyeur DEVRAIT examiner dans son antémémoire de liens si il existe une entrée pour l'adresse de destination à laquelle le paquet est à envoyer. Si il a une entrée d'antémémoire de liens pour cette adresse, il DEVRAIT utiliser un en-tête d'acheminement de type 2 pour acheminer le paquet à ce nœud mobile (le nœud de destination) au moyen de son adresse d'entretien. Cependant, le nœud envoyeur NE DOIT PAS faire cela dans les cas suivants :

- Quand il envoie un paquet IPv6 de découverte de voisin [RFC4861].
- Quand c'est noté autrement au paragraphe 6.1.

Quand il calcule les données d'authentification dans un paquet qui contient un en-tête d'acheminement de type 2, le nœud correspondant DOIT calculer les données d'authentification AH comme si ce qui suit était vrai : l'en-tête d'acheminement contient l'adresse d'entretien, le champ Adresse de destination IPv6 de l'en-tête IPv6 contient l'adresse de rattachement, et le champ Segments restants est zéro. La recherche dans la base de données de politique de sécurité IPsec DOIT se fonder sur l'adresse de rattachement du nœud mobile.

Par exemple, en supposant qu'il n'y a pas d'en-tête d'acheminement supplémentaire dans ce paquet en plus de ceux nécessaires pour IPv6 mobile, le nœud correspondant pourrait régler les champs d'en-tête IPv6 et d'en-tête d'acheminement dans le paquet comme suit :

- L'adresse de destination dans l'en-tête IPv6 du paquet est réglée à l'adresse de rattachement du nœud mobile (l'adresse de destination originale à laquelle le paquet était envoyé).
- L'en-tête d'acheminement est initialisée à contenir un seul segment de chemin, contenant l'adresse d'entretien du nœud mobile copiée de l'entrée d'antémémoire de liens. Le champ Segments restants est, cependant, temporairement réglé à zéro.

La couche IP va insérer l'en-tête d'acheminement avant d'effectuer tout traitement IPsec nécessaire. Une fois tous les traitements IPsec effectués, le nœud remplace le champ Destination IPv6 par le champ Adresse de rattachement dans l'en-tête d'acheminement, règle le champ Segments restants à un, et envoie le paquet. Cela assure que le calcul AH est fait sur le paquet sous la forme qu'il va avoir chez le receveur après l'avancement de l'en-tête d'acheminement.

Suivant la définition d'un en-tête d'acheminement de type 2 au paragraphe 6.4, ce paquet va être acheminé à l'adresse d'entretien du nœud mobile, où il va être livré au nœud mobile (le nœud mobile est associé à l'adresse d'entretien par son interface réseau).

Noter que suivre le modèle conceptuel ci-dessus dans une mise en œuvre crée des exigences supplémentaires pour la découverte de la MTU de chemin car la couche qui détermine la taille du paquet (par exemple, TCP et les applications qui utilisent UDP) a besoin d'être au courant de la taille des en-têtes ajoutés par la couche IP sur le nœud envoyeur.

Si, à la place, le nœud envoyeur n'a pas d'entrée d'antémémoire de liens pour l'adresse de destination à laquelle le paquet est envoyé, le nœud envoyeur envoie simplement le paquet normalement, sans en-tête d'acheminement. Si le nœud de destination n'est pas un nœud mobile (ou est un nœud mobile qui est actuellement chez lui) le paquet va être livré directement à ce nœud et traité normalement par lui. Si, cependant, le nœud de destination est un nœud mobile actuellement hors de chez lui, le paquet va être intercepté par l'agent de rattachement du nœud mobile et tunnelé à l'adresse d'entretien principale actuelle du nœud mobile.

9.3.3 Envoi des messages d'erreur de lien

Les paragraphes 9.2 et 9.3.1 décrivent les conditions qui conduisent au besoin d'envoyer a message Erreur de lien.

Un message Erreur de lien est envoyé directement à l'adresse qui apparaissait dans le champ Adresse IPv6 de source du paquet en cause. Si le champ Adresse de source ne contient pas une adresse d'envoi individuel, le message Erreur de lien NE DOIT PAS être envoyé.

Le champ Adresse de rattachement dans le message Erreur de lien DOIT être copié du champ Adresse de rattachement dans l'option de destination Adresse de rattachement du paquet en cause, ou réglé à l'adresse inspécifiée si aucune option de cette sorte n'apparaissait dans le paquet.

Noter que les valeurs de champ Adresse IPv6 de source et Adresse de rattachement discutées ci-dessus sont les valeurs provenant du réseau, c'est-à-dire, avant toute modification éventuellement effectuée comme spécifié au paragraphe 9.3.1.

Les messages Erreur de lien DEVRAIT être soumis à une limitation de débit de la même façon que pour les messages ICMPv6 [RFC4443].

9.3.4 Réception des messages d'erreur ICMP

Quand le nœud correspondant a une entrée d'antémémoire de liens pour un nœud mobile, tout le trafic destiné au nœud mobile va directement à l'adresse d'entretien actuelle du nœud mobile en utilisant un en-tête d'acheminement. Tout message d'erreur ICMP causé par les paquets sur leur chemin vers l'adresse d'entretien va être retourné de la façon normale au nœud correspondant.

Par ailleurs, si le nœud correspondant n'a pas d'entrée d'antémémoire de liens pour le nœud mobile, le paquet va être acheminé à travers la liaison de rattachement du nœud mobile. Tout message d'erreur ICMP causé par le paquet sur son chemin vers le nœud mobile lorsque il est dans le tunnel, va être transmis à l'agent de rattachement du nœud mobile. Selon la définition de l'encapsulation IPv6 [RFC2473], l'agent de rattachement DOIT relayer certains messages d'erreur ICMP en retour à l'envoyeur original du paquet, qui dans ce cas est le nœud correspondant.

Donc, dans tous les cas, tous les messages d'erreur ICMP significatifs causés par les paquets provenant d'un nœud correspondant à un nœud mobile vont être retournés au nœud correspondant. Si le nœud correspondant reçoit des messages

ICMP Destination injoignable persistants après l'envoi de paquets à un nœud mobile sur la base d'une entrée dans son antémémoire de liens, le nœud correspondant DEVRAIT supprimer cette entrée d'antémémoire de liens. Noter que si le nœud mobile continue d'envoyer des paquets avec l'option de destination Adresse de rattachement à ce nœud correspondant, ils vont être éliminés à cause de l'absence d'un lien. Pour cette raison, il est important que seuls des messages ICMP persistants conduisent à la suppression de l'entrée d'antémémoire de liens.

9.4 Procédure d'acheminement de retour

Ce paragraphe spécifie les actions prises par un nœud correspondant durant la procédure d'acheminement de retour.

9.4.1 Réception des messages Initiation d'essai de rattachement

À réception d'un message Initiation d'essai de rattachement, le nœud correspondant vérifie ce qui suit :
- Le paquet NE DOIT PAS inclure une option de destination Adresse de rattachement.

Tout paquet portant un message Initiation d'essai de rattachement qui échoue à cette vérification DOIT être ignoré en silence.

Autrement, en préparation de l'envoi du message correspondant Essai de rattachement, le nœud correspondant vérifie qu'il a le matériel nécessaire pour engager une procédure d'acheminement de retour, comme spécifié au paragraphe 5.2. Le nœud correspondant DOIT avoir une Kcn secrète et un nom occasionnel. Si il n'a pas déjà ce matériel, il DOIT le produire avant de continuer la procédure d'acheminement de retour.

Le paragraphe 9.4.3 spécifie la suite du traitement.

9.4.2 Réception des messages Initiation d'essai d'entretien

À réception d'un message Initiation d'essai d'entretien, le nœud correspondant vérifie ce qui suit :
- Le paquet NE DOIT PAS inclure une option de destination Adresse de rattachement.

Tout paquet qui porte un message Initiation d'essai d'entretien qui échoue à cette vérification DOIT être ignoré en silence.

Autrement, en préparation de l'envoi du message correspondant Essai d'entretien, le nœud correspondant vérifie qu'il a le matériel nécessaire pour s'engager dans une procédure d'acheminement de retour de la manière décrite au paragraphe 9.4.1.

Le paragraphe 9.4.4 spécifie la suite du traitement.

9.4.3 Envoi des messages d'essai de rattachement

Le nœud correspondant crée un jeton de génération de clé de rattachement et utilise l'indice actuel de nom occasionnel comme Indice de nom occasionnel de rattachement. Il crée alors un message Essai de rattachement (paragraphe 6.1.5) et l'envoie au nœud mobile à l'adresse de rattachement de ce dernier.

9.4.4 Envoi des messages Essai d'entretien

Le nœud correspondant crée un jeton de génération de clé d'entretien et utilise l'indice actuel de nom occasionnel comme indice de nom occasionnel d'entretien. Il crée ensuite un message Essai d'entretien (paragraphe 6.1.6) et l'envoie au nœud mobile à l'adresse d'entretien de ce dernier.

9.5 Traitement des liens

Ce paragraphe explique comment le nœud correspondant traite les messages relatifs aux liens. Ces messages sont :
- Mise à jour de lien
- Demande de rafraîchissement de lien
- Accusé de réception de lien
- Erreur de lien

9.5.1 Réception de mises à jour de lien

Avant d'accepter une mise à jour de lien, le nœud receveur DOIT valider la mise à jour de lien conformément aux essais suivants :

- Le paquet DOIT contenir une adresse de rattachement acheminable en envoi individuel, soit dans l'option Adresse de rattachement, soit dans l'adresse de source, si l'option Adresse de rattachement n'est pas présente.
- Le champ Numéro de séquence dans la mise à jour de lien est supérieur au numéro de séquence reçu dans la précédente mise à jour de lien valide pour cette adresse de rattachement, si il en est une.

Si le nœud receveur n'a pas d'entrée d'antémémoire de liens pour l'adresse de rattachement indiquée, il DOIT accepter toute valeur de numéro de séquence dans une mise à jour de lien reçue de ce nœud mobile.

Cette comparaison de numéro de séquence DOIT être effectuée modulo 2**16, c'est-à-dire que le numéro est un compteur de fonctionnement libre représenté modulo 65536. Un numéro de séquence dans une mise à jour de lien reçue est considéré inférieur ou égal au dernier numéro reçu si sa valeur se tient dans la gamme du dernier numéro reçu et des 32768 valeurs précédentes, incluses. Par exemple, si le dernier numéro de séquence reçu était 15, alors les messages avec les numéros de séquence de 0 à 15, ainsi que de 32783 à 65535, vont être considérés inférieurs ou égaux.

Quand le bit H (enregistrement de rattachement) n'est pas établi, ce qui suit est aussi exigé :

- Une option de mobilité Indices de nom occasionnel DOIT être présente, et les valeurs d'indice de nom occasionnel de rattachement et d'entretien dans cette option DOIVENT être assez récentes pour être reconnues par le nœud correspondant. (Les valeurs d'indices de nom occasionnel d'entretien ne sont pas inspectées pour les demandes de suppression de lien.)
- Le nœud correspondant DOIT re-générer le jeton de génération de clé de rattachement et le jeton de génération de clé d'entretien à partir des informations contenues dans le paquet. Il génère alors la clé de gestion de lien Kbm et l'utilise pour vérifier le champ Authentifiant dans la mise à jour de lien comme spécifié au paragraphe 6.1.7.
- L'option de mobilité Données d'autorisation de lien DOIT être présente, et son contenu DOIT satisfaire aux règles présentées au paragraphe 5.2.6. Noter qu'une adresse d'entretien différente de l'adresse de source PEUT avoir été spécifiée en incluant une option de mobilité Adresse d'entretien de remplacement dans la mise à jour de lien. Quand un tel message est reçu et que la procédure d'acheminement de retour est utilisée comme méthode d'autorisation, le nœud correspondant DOIT vérifier l'authentifiant en utilisant l'adresse au sein de l'adresse d'entretien de remplacement dans le calcul.
- L'option de mobilité Données d'autorisation de lien DOIT être la dernière option et NE DOIT PAS avoir de bourrage en queue.

Si le bit H (enregistrement de rattachement) est établi, l'option de mobilité Indices de nom occasionnel NE DOIT PAS être présente.

Si le nœud mobile envoie un numéro de séquence qui n'est pas supérieur au numéro de séquence provenant de la dernière mise à jour de lien valide pour cette adresse de rattachement, alors le nœud receveur DOIT renvoyer un accusé de réception de lien avec le code d'état 135, et le dernier numéro de séquence accepté dans le champ Numéro de séquence de l'accusé de réception de lien.

Si un lien existe déjà pour l'adresse de rattachement donnée et si le fanion enregistrement de rattachement a une valeur différente de celle du bit H (enregistrement de rattachement) dans la mise à jour de lien, alors le nœud receveur DOIT renvoyer un accusé de réception de lien avec le code d'état 139 (changement de type d'enregistrement interdit). Le fanion Enregistrement de rattachement mémorisé dans l'entrée d'antémémoire de liens NE DOIT PAS être changé.

Si le nœud receveur ne reconnaît plus la valeur d'indice de nom occasionnel de rattachement, la valeur d'indice de nom occasionnel d'entretien, ou les deux valeurs provenant de la mise à jour de lien, il DOIT renvoyer un accusé de réception de lien avec le code d'état 136, 137, ou 138, respectivement.

Les paquets qui portent des mises à jour de lien qui ne satisfont pas à toutes ces vérifications pour toute raison autre que l'insuffisance du numéro de séquence, un changement de type d'enregistrement, ou des valeurs d'indice de nom occasionnel expirées, DOIVENT être éliminés en silence.

Si la mise à jour de lien est valide conformément aux essais ci-dessus, la mise à jour de lien est alors traité comme suit :

- La valeur du numéro de séquence reçu d'un nœud mobile dans une mise à jour de lien est mémorisée par le nœud receveur dans son entrée d'antémémoire de liens pour l'adresse de rattachement donnée.
- Si la durée de vie spécifiée dans la mise à jour de lien n'est pas zéro, c'est alors une demande de mise en antémémoire d'un lien pour l'adresse de rattachement. Si le bit H (enregistrement de rattachement) est établi dans la mise à jour de lien, la mise à jour de lien est traitée conformément à la procédure spécifiée au paragraphe 10.3.1 ; sinon, elle est traitée conformément à la procédure spécifiée au paragraphe 9.5.2.

- Si la durée de vie spécifiée dans la mise à jour de lien est zéro, c'est alors une demande de suppression du lien en antémémoire pour l'adresse de rattachement. Dans ce cas, la mise à jour de lien DOIT inclure un indice de nom occasionnel de rattachement valide, et l'indice de nom occasionnel d'entretien DOIT être ignoré par le nœud correspondant. La génération de la clé de gestion de lien dépend alors exclusivement du jeton de génération de clé de rattachement (paragraphe 5.2.5). Si le bit H (enregistrement de rattachement) est établi dans la mise à jour de lien, elle est traitée conformément à la procédure spécifiée au paragraphe 10.3.2 ; sinon, elle est traitée conformément à la procédure spécifiée au paragraphe 9.5.3.

L'adresse d'entretien spécifiée DOIT être déterminée comme suit :
- Si l'option Adresse d'entretien de remplacement est présente, l'adresse d'entretien est celle de cette option.
- Autrement, l'adresse d'entretien est celle du champ Adresse de source dans l'en-tête IPv6 du paquet.

L'adresse de rattachement pour le lien DOIT être déterminée comme suit :
- Si l'option de destination Adresse de rattachement est présente, l'adresse de rattachement est l'adresse dans cette option.
- Autrement, l'adresse de rattachement est celle du champ Adresse de source dans l'en-tête IPv6 du paquet.

9.5.2 Demande de mise en antémémoire d'un lien

Ce paragraphe décrit le traitement d'une mise à jour de lien valide qui demande à un nœud de mettre un lien en antémémoire, pour lequel le bit H (enregistrement de rattachement) n'est pas établi dans la mise à jour de lien.

Dans ce cas, le nœud receveur DEVRAIT créer une nouvelle entrée dans son antémémoire de liens pour cette adresse de rattachement, ou mettre à jour une entrée d'antémémoire de liens existante pour cette adresse de rattachement, si une telle entrée existe déjà. La durée de vie pour l'entrée d'antémémoire de liens est initialisée à partir du champ Durée de vie spécifié dans la mise à jour de lien, bien que cette durée de vie PUISSE être réduite par le nœud qui met le lien en antémémoire ; la durée de vie pour l'entrée d'antémémoire de liens NE DOIT PAS être supérieure à la valeur de durée de vie spécifiée dans la mise à jour de lien. Toute entrée d'antémémoire de liens DOIT être supprimée après l'expiration de sa durée de vie.

Noter que si le nœud mobile n'a pas demandé d'accusé de réception de lien, il ne connaît alors pas la plus courte durée de vie choisie. Le nœud mobile peut donc utiliser l'optimisation de chemin et envoyer des paquets avec l'option de destination Adresse de rattachement. Comme expliqué au paragraphe 9.3.1, de tels paquets vont être éliminés si il n'y a pas de lien. Cette situation est récupérable, mais peut causer une perte temporaire de paquets.

Le nœud correspondant PEUT refuser d'accepter une nouvelle entrée d'antémémoire de liens si il n'a pas des ressources suffisantes. Une nouvelle entrée PEUT aussi être refusée si le nœud correspondant estime que ses ressources seront utilisée plus efficacement à un autre objet, comme de servir un autre nœud mobile avec une quantité de trafic supérieure. Dans les deux cas, le nœud correspondant DEVRAIT retourner un accusé de réception de lien avec la valeur d'état 130.

9.5.3 Demande de suppression d'un lien

Ce paragraphe décrit le traitement d'une mise à jour de lien valide qui demande à un nœud de supprimer un lien quand le bit H (enregistrement de rattachement) n'est pas établi dans la mise à jour de lien.

Tout lien existant pour l'adresse de rattachement donnée DOIT être supprimé. Une entrée d'antémémoire de liens pour l'adresse de rattachement NE DOIT PAS être créée en réponse à la réception de la mise à jour de lien.

Si l'entrée d'antémémoire de liens a été créée par l'utilisation de noms occasionnels d'acheminement de retour, le nœud correspondant DOIT s'assurer que les mêmes noms occasionnels ne sont pas utilisés à nouveau avec les adresses particulières de rattachement et d'entretien. Si les deux noms occasionnels sont encore valides, le nœud correspondant doit mémoriser la combinaison particulière d'indice de nom occasionnel, d'adresses, et de numéro de séquence comme illégale jusqu'à ce qu'au moins un des noms occasionnels soit périmé.

9.5.4 Envoi des accusés de réception de lien

Un accusé de réception de lien peut être envoyé pour indiquer la réception d'une mise à jour de lien comme suit :
- Si la mise à jour de lien a été éliminée comme décrit aux paragraphes 9.2 ou 9.5.1, un accusé de réception de lien NE DOIT PAS être envoyé. Autrement, le traitement dépend des règles suivantes.
- Si le bit A (accusé de réception) est établi dans la mise à jour de lien, un accusé de réception de lien DOIT être envoyé. Autrement, le traitement dépend de la règle suivante.

- o Si le nœud rejette la mise à jour de lien à cause de l'expiration d'un indice de nom occasionnel, d'un numéro de séquence hors fenêtre (paragraphe 9.5.1) ou de ressources insuffisantes (paragraphe 9.5.2) un accusé de réception de lien DOIT être envoyé. Si le nœud accepte la mise à jour de lien, l'accusé de réception de lien NE DEVRAIT PAS être envoyé.

Si le nœud accepte la mise à jour de lien et crée ou met à jour une entrée pour ce lien, le champ État dans l'accusé de réception de lien DOIT être réglé à une valeur inférieure à 128. Autrement, le champ État DOIT être réglé à une valeur supérieure ou égale à 128. Les valeurs pour le champ État sont décrites au paragraphe 6.1.8 et dans le registre IANA des numéros alloués [RFC3232].

Si le champ État dans l'accusé de réception de lien contient la valeur 136 (indice de nom occasionnel de rattachement expiré) 137 (indice de nom occasionnel d'entretien expiré) ou 138 (noms occasionnels expirés) le message NE DOIT alors PAS inclure l'option de mobilité Données d'autorisation de lien. Autrement, l'option de mobilité Données d'autorisation de lien DOIT être incluse, et DOIT satisfaire aux exigences d'authentification spécifiques pour l'accusé de réception de liens comme définies au paragraphe 5.2.

Si le champ Adresse de source de l'en-tête IPv6 qui portait la mise à jour de lien ne contient pas une adresse en envoi individuel, l'accusé de réception de lien NE DOIT PAS être envoyé et le paquet de mise à jour de lien DOIT être éliminé en silence. Autrement, l'accusé de réception DOIT être envoyé à l'adresse de source. À la différence du traitement des paquets réguliers, cette procédure d'adressage n'utilise pas d'informations provenant de l'antémémoire de liens. Cependant, un en-tête d'acheminement est nécessaire dans certains cas. Si l'adresse de source est l'adresse de rattachement du nœud mobile, c'est-à-dire, si la mise à jour de lien ne contient pas d'option de destination Adresse de rattachement, l'accusé de réception de lien DOIT alors être envoyé à cette adresse et l'en-tête d'acheminement NE DOIT PAS être utilisé. Autrement, l'accusé de réception de lien DOIT être envoyé en utilisant un en-tête d'acheminement de type 2 qui contient l'adresse de rattachement du nœud mobile.

9.5.5 Envoi des demandes de rafraîchissement de lien

Si une entrée d'antémémoire de liens en cours de suppression est encore en utilisation active lors de l'envoi de paquets à un nœud mobile, le prochain paquet envoyé au nœud mobile va être acheminé normalement à la liaison de rattachement du nœud mobile. La communication avec le nœud mobile continue, mais le tunnelage à partir du réseau de rattachement crée des frais généraux et de la latence supplémentaires dans la livraison des paquets au nœud mobile.

Si l'envoyeur sait que l'entrée d'antémémoire de liens est encore utilisée activement, il PEUT envoyer un message Demande de rafraîchissement de lien au nœud mobile pour tenter d'éviter ces frais généraux et cette latence dus à la suppression et la recréation de l'entrée d'antémémoire de liens. Ce message est toujours envoyé à l'adresse de rattachement du nœud mobile.

Le nœud correspondant PEUT retransmettre des messages Demande de rafraîchissement de lien dans la mesure de l'application de la limitation de taux d'envoi. Le nœud correspondant DOIT arrêter de retransmettre quand il reçoit une mise à jour de lien.

9.6 Politique de remplacement d'antémémoire

Idéalement, un nœud tient un temporisateur séparé pour chaque entrée dans son antémémoire de liens. Quand il crée ou met à jour une entrée d'antémémoire de liens en réponse à une mise à jour de lien reçue et acceptée, le nœud lance le temporisateur pour cette entrée pour la période de durée de vie spécifiée. Toute entrée dans l'antémémoire de liens d'un nœud DOIT être supprimée à l'expiration de la durée de vie spécifiée dans la mise à jour de lien à partir de laquelle l'entrée a été créée ou mise à jour.

Chaque antémémoire de liens de nœud va, par nécessité, avoir une taille finie. Un nœud PEUT utiliser toute politique locale raisonnable pour gérer l'espace dans son antémémoire de liens.

Un nœud PEUT choisir d'éliminer toute entrée de son antémémoire de liens afin de faire de l'espace pour une nouvelle entrée. Par exemple, une stratégie de "moins récemment utilisée" pour le remplacement des entrées d'antémémoire devrait bien fonctionner, sauf si la taille de l'antémémoire de liens est substantiellement insuffisante. Quand des entrées sont supprimées, le nœud correspondant DOIT suivre les règles du paragraphe 5.2.8 afin de conserver la procédure d'acheminement de retour contre les attaques en répétition.

Si le nœud envoie un paquet à une destination pour laquelle il a éliminé l'entrée de son antémémoire de liens, le paquet va être acheminé à travers la liaison de rattachement du nœud mobile. Le nœud mobile peut le détecter et établir un nouveau lien si nécessaire.

Cependant, si le nœud mobile pense que le lien existe encore, il peut utiliser l'optimisation de chemin et envoyer des paquets avec l'option de destination Adresse de rattachement. Cela peut créer une perte temporaire de paquets, comme expliqué plus haut, dans le contexte de la réduction de la durée de vie de lien effectuée par le nœud correspondant (paragraphe 9.5.2).

10. Fonctionnement de l'agent de rattachement

10.1 Structures de données conceptuelles

Chaque agent de rattachement DOIT tenir une antémémoire de liens et une liste d'agents de rattachement.

Les règles de tenue d'une antémémoire de liens sont les mêmes pour les agents de rattachement et les nœuds correspondants et ont déjà été décrites au paragraphe 9.1.

La liste des agents de rattachement est tenue par chaque agent de rattachement, enregistrant les informations sur chaque routeur sur la même liaison qui agit comme agent de rattachement. Cette liste est utilisée par le mécanisme de découverte dynamique d'adresse d'agent de rattachement. Un routeur est connu pour agir comme agent de rattachement si il envoie une annonce de routeur dans laquelle le bit H (agent de rattachement) est établi. Quand la durée de vie pour une entrée de la liste (définie ci-dessous) expire, cette entrée est supprimée de la liste des agents de rattachement. La liste des agents de rattachement est similaire à la structure de données conceptuelles de liste des routeurs par défaut tenue par chaque hôte pour la découverte de voisin [RFC4861]. La liste des agents de rattachement PEUT être mise en œuvre de nombreuses façons avec le comportement externe décrit dans le présent document.

Chaque agent de rattachement tient une liste séparée des agents de rattachement pour chaque liaison sur laquelle il sert d'agent de rattachement. Une nouvelle entrée est créée ou une entrée existante est mise à jour en réponse à la réception d'une annonce de routeur valide dans laquelle le bit H (agent de rattachement) est établi. Chaque entrée de liste des agents de rattachement contient les champs suivants :

- L'adresse IP de liaison locale d'un agent de rattachement sur la liaison. Cette adresse est apprise de l'adresse de source des annonces de routeur [RFC4861] reçues du routeur.
- Une ou plusieurs adresses IP mondiales pour cet agent de rattachement. Les adresses mondiales sont apprises des options Informations de préfixe avec le bit R (Adresse de routeur) établi et reçues dans les annonces de routeur provenant de cette adresse de liaison locale. Les adresses mondiales pour le routeur dans une entrée de liste des agents de rattachement DOIVENT être supprimées une fois que le préfixe associé à cette adresse n'est plus valide [RFC4861].
- La durée de vie restante de cette entrée de liste des agents de rattachement. Si une option Informations d'agent de rattachement est présente dans une annonce de routeur reçue d'un agent de rattachement, la durée de vie de l'entrée de liste des agents de rattachement représentant cet agent de rattachement est initialisée à partir du champ Durée de vie provenant de l'agent de rattachement dans l'option (si elle est présente) ; autrement, la durée de vie est initialisée à partir du champ Durée de vie de routeur dans l'annonce de routeur reçue. Si la durée de vie de l'entrée de liste des agents de rattachement tombe à zéro, l'entrée DOIT être supprimée de la liste des agents de rattachement.
- La préférence pour cet agent de rattachement ; les plus hautes valeurs indiquent un agent de rattachement préféré. La valeur de préférence est prise du champ Préférence d'agent de rattachement dans l'annonce de routeur reçue, si l'annonce de routeur contient une option Informations d'agent de rattachement et est autrement réglée à la valeur par défaut de 0. Un agent de rattachement utilise cette préférence pour ordonner la liste des agents de rattachement quand il envoie un message ICMP Découverte d'adresse d'agent de rattachement.

10.2 Traitement des en-têtes de mobilité

Tous les agents de rattachement IPv6 DOIVENT observer les règles décrites au paragraphe 9.2 lors du traitement des en-têtes de mobilité.

10.3 Traitement des liens

10.3.1 Enregistrement de l'adresse d'entretien principale

Quand un nœud reçoit une mise à jour de lien, il DOIT la valider et déterminer le type de mise à jour de lien conformément aux étapes décrites au paragraphe 9.5.1. De plus, il DOIT authentifier la mise à jour de lien comme décrit au paragraphe 5.1. Une étape d'autorisation spécifique pour l'agent de rattachement est aussi nécessaire pour s'assurer que seul le bon nœud peut contrôler une adresse de rattachement particulière. Ceci est fourni par l'adresse de rattachement qui identifie de façon non équivoque l'association de sécurité qui doit être utilisée.

Ce paragraphe décrit le traitement d'une mise à jour de lien valide et autorisée quand elle demande l'enregistrement de l'adresse d'entretien principale du nœud mobile.

Pour commencer le traitement de la mise à jour de lien, l'agent de rattachement DOIT effectuer la séquence de vérifications suivante :

- Si le nœud met seulement en œuvre la fonction de nœud correspondant, ou n'a pas été configuré à agir comme agent de rattachement, il DOIT rejeter la mise à jour de lien. Le nœud DOIT aussi retourner un accusé de réception de lien au nœud mobile, dans lequel le champ État est réglé à 131 (enregistrement de rattachement non pris en charge).
- Autrement, si l'adresse de rattachement pour le lien (le champ Adresse de rattachement dans l'option Adresse de rattachement du paquet) n'est pas une adresse IPv6 en liaison par rapport à la liste de préfixes actuelle de l'agent de rattachement, l'agent de rattachement DOIT alors rejeter la mise à jour de lien et DEVRAIT retourner un accusé de réception de lien au nœud mobile, dans lequel le champ État est réglé à 132 (pas de sous réseau de rattachement).
- Autrement, si l'agent de rattachement choisit de rejeter la mise à jour de lien pour toute autre raison (par exemple, ressources insuffisantes pour servir un autre nœud mobile comme agent de rattachement) l'agent de rattachement DEVRAIT alors retourner un accusé de réception de lien au nœud mobile, dans lequel le champ État est réglé à une valeur appropriée pour indiquer la raison du rejet.
- Une option de destination Adresse de rattachement DOIT être présente dans le message. Elle DOIT être validée comme décrit au paragraphe 9.3.1 avec la règle supplémentaire suivante. L'essai d'existence d'entrée d'antémémoire de liens NE DOIT PAS être faite pour les paquets IPsec quand l'option Adresse de rattachement contient une adresse pour laquelle le nœud receveur pourrait agir comme agent de rattachement.

Si l'agent de rattachement accepte la mise à jour de lien, il DOIT alors créer une nouvelle entrée dans son antémémoire de liens pour ce nœud mobile ou mettre à jour une entrée d'antémémoire de liens existante, si une telle entrée existe déjà. Le champ Adresse de rattachement tel que reçu dans l'option Adresse de rattachement fournit l'adresse de rattachement du nœud mobile.

L'agent de rattachement DOIT marquer cette entrée d'antémémoire de liens comme enregistrement de rattachement pour indiquer que le nœud sert d'agent de rattachement pour ce lien. Les entrées d'antémémoire de liens marquées comme enregistrement de rattachement DOIVENT être exclues de la politique normale de remplacement d'antémémoire utilisée pour l'antémémoire de liens (paragraphe 9.6) et NE DOIVENT PAS être retirées de l'antémémoire de liens jusqu'à l'expiration de la période de durée de vie.

Sauf si cet agent de rattachement a déjà un lien pour cette adresse de rattachement, il DOIT effectuer la détection d'adresse dupliquée [RFC4862] sur la liaison de rattachement de nœud mobile avant de retourner l'accusé de réception de lien. Cela assure qu'aucun autre nœud sur la liaison de rattachement n'utilise l'adresse de rattachement du nœud mobile quand la mise à jour de lien arrive. Si cette détection d'adresse dupliquée échoue pour cette adresse de rattachement ou une adresse de liaison locale associée, l'agent de rattachement DOIT alors rejeter la mise à jour de lien complète et DOIT retourner un accusé de réception de lien au nœud mobile, dans lequel le champ État est réglé à 134 (échec de détection d'adresse dupliquée). Quand l'agent de rattachement envoie un accusé de réception de lien de succès au nœud mobile, l'agent de rattachement assure au nœud mobile que sa ou ses adresses seront conservées uniques par l'agent de rattachement pour toute la durée de vie accordée pour le lien.

Les adresses spécifiques, qui vont être vérifiées avant d'accepter la mise à jour de lien et plus tard être défendues en effectuant une détection d'adresse dupliquée, dépendent du réglage du bit L (compatibilité d'adresse de liaison locale) comme suit :

- L = 0 : défend seulement cette adresse. Ne déduit pas d'adresse de liaison locale.
- L = 1 : défend à la fois l'adresse d'envoi individuel (de rattachement) donnée non de liaison locale et l'adresse déduite de liaison locale. L'adresse de liaison locale est déduite en remplaçant le préfixe de sous réseau dans l'adresse de rattachement du nœud mobile par le préfixe de liaison locale.

La durée de vie de l'entrée d'antémémoire de liens dépend d'un certain nombre de facteurs :

- La durée de vie pour l'entrée d'antémémoire de liens NE DOIT PAS être supérieure à la valeur de durée de vie spécifiée dans la mise à jour de lien.
- La durée de vie pour l'entrée d'antémémoire de liens NE DOIT PAS être supérieure à la durée de vie valide restante pour le préfixe de sous réseau dans l'adresse de rattachement du nœud mobile spécifiée avec la mise à jour de lien. La durée de vie valide restante pour ce préfixe est déterminée par l'agent de rattachement sur la base de sa propre entrée de liste de préfixes [RFC4861].
  La durée de vie préférée restante NE DEVRAIT PAS avoir d'impact sur la durée de vie pour l'entrée d'antémémoire de liens.
  L'agent de rattachement DOIT supprimer un lien quand la durée de vie valide du préfixe qui lui est associé expire.
- L'agent de rattachement PEUT diminuer encore la durée de vie spécifiée pour le lien, par exemple, sur la base d'une politique locale. La durée de vie résultante est mémorisée par l'agent de rattachement dans l'entrée d'antémémoire de

liens, et cette entrée d'antémémoire de liens DOIT être supprimée par l'agent de rattachement après l'expiration de cette durée de vie.

Sans considération du réglage du bit A (accusé de réception) dans la mise à jour de lien, l'agent de rattachement DOIT retourner un accusé de réception de lien au nœud mobile, construit comme suit :

- Le champ État DOIT être réglé à une valeur qui indique le succès. La valeur 1 (accepté mais découverte de préfixe nécessaire) DOIT être utilisée si le préfixe de sous-réseau de l'adresse de rattachement spécifiée est déconseillé, ou devient déconseillé durant la durée de vie du lien, ou devient invalide à la fin de la durée de vie. La valeur 0 DOIT être utilisée autrement. Pour les besoins de la comparaison des durées de vie du lien et du préfixe, la durée de vie du préfixe est d'abord convertie en unités de quatre secondes en ignorant les deux bits de moindre poids.
- Le bit K (capacité de mobilité de gestion de clé) est établi si les conditions suivantes sont toutes satisfaites, et mis à zéro autrement :
  * Le bit K (capacité de mobilité de gestion de clé) était établi dans la mise à jour de lien.
  * Les associations de sécurité IPsec entre le nœud mobile et l'agent de rattachement ont été établies dynamiquement.
  * L'agent de rattachement a la capacité de mettre à jour son point d'extrémité dans le protocole de gestion de clés utilisé à la nouvelle adresse d'entretien chaque fois qu'il se déplace.

Selon la valeur finale du bit dans l'accusé de réception de lien, l'agent de rattachement DEVRAIT effectuer les actions suivantes :

K = 0 : éliminer les connexions de gestion de clés, si il y en a, à la vieille adresse d'entretien. Si le nœud mobile n'avait pas de lien avant l'envoi de cette mise à jour de lien, éliminer les connexions à l'adresse de rattachement.

K = 1 : déplacer le point d'extrémité homologue de la connexion de protocole de gestion de clés, si il en est, à la nouvelle adresse d'entretien.

- Le champ Numéro de séquence DOIT être copié du numéro de séquence donné dans la mise à jour de lien.

- Le champ Durée de vie DOIT être réglé à la durée de vie restante pour le lien comme réglé par l'agent de rattachement dans son entrée d'enregistrement de rattachement d'antémémoire de liens pour le nœud mobile, comme décrit ci-dessus.

- Si l'agent de rattachement mémorise l'entrée d'antémémoire de liens sur un support non volatile, l'option de mobilité Avis de rafraîchissement de lien DOIT être omise. Autrement, l'agent de rattachement PEUT inclure cette option pour suggérer que le nœud mobile rafraîchisse son lien avant la fin réelle de la durée de vie du lien.

Si l'option de mobilité Avis de rafraîchissement de lien est présente, le champ Intervalle de rafraîchissement dans l'option DOIT être réglé à une valeur inférieure à la valeur de durée de vie retournée dans l'accusé de réception de lien. Cela indique que le nœud mobile DEVRAIT tenter de rafraîchir son enregistrement de rattachement au plus court intervalle indiqué. L'agent de rattachement DOIT quand même conserver l'enregistrement pour toute la période de durée de vie, même si le nœud mobile ne rafraîchit pas son enregistrement dans la période de rafraîchissement.

Les règles de choix de l'adresse IP de destination (et éventuellement de construction de l'en-tête d'acheminement) pour l'accusé de réception de lien au nœud mobile sont les mêmes qu'au paragraphe 9.5.4.

De plus, l'agent de rattachement DOIT suivre la procédure définie au paragraphe 10.4.1 pour intercepter les paquets sur la liaison de rattachement du nœud mobile adressés au nœud mobile, alors que l'agent de rattachement sert d'agent de rattachement pour ce nœud mobile. L'agent de rattachement DOIT aussi être prêt à accepter les paquets en tunnelage inverse provenant de la nouvelle adresse d'entretien du nœud mobile, comme décrit au paragraphe 10.4.5. Finalement, l'agent de rattachement DOIT aussi propager les nouveaux préfixes de réseau de rattachement, comme décrit au paragraphe 10.6.

10.3.2 Désenregistrement de l'adresse d'entretien principale

Un lien peut devoir être désenregistré quand le nœud mobile retourne chez lui ou quand le nœud mobile sait qu'il n'aura pas d'adresse d'entretien dans le réseau visité.

Une mise à jour de lien est validée et autorisée de la manière décrite au paragraphe précédent ; noter que quand le nœud mobile se désenregistre alors qu'il est chez lui, il PEUT choisir d'omettre l'option de destination Adresse de rattachement, et dans ce cas, l'adresse de rattachement du nœud mobile est l'adresse IP de source de la mise à jour de lien de désenregistrement. Ce paragraphe décrit le traitement d'une mise à jour de lien valide qui demande au nœud receveur de ne plus lui servir d'agent de rattachement, désenregistrant son adresse d'entretien principale.

Pour commencer le traitement de la mise à jour de lien, l'agent de rattachement DOIT effectuer les vérifications suivantes :

- Si le nœud receveur n'a pas d'entrée marquée comme enregistrement de rattachement dans son antémémoire de liens pour ce nœud mobile, alors ce nœud DOIT rejeter la mise à jour de lien et DEVRAIT retourner un accusé de réception de lien au nœud mobile, dans lequel le champ État est réglé à 133 (pas d'agent de rattachement pour ce nœud mobile). Si l'agent de rattachement ne rejette pas la mise à jour de lien comme décrit ci-dessus, il DOIT retourner un accusé de réception de lien au nœud mobile, construit comme suit :
  - Le champ État DOIT être réglé à la valeur 0, indiquant le succès.
  - Le bit K (capacité de mobilité de gestion de clé) est établi ou à zéro et les actions fondées sur sa valeur sont effectuées comme décrit au paragraphe précédent. L'adresse de rattachement du nœud mobile est utilisée comme sa nouvelle adresse d'entretien pour les besoins du déplacement de la connexion de gestion de clés à un nouveau point d'extrémité.
  - Le champ Numéro de séquence DOIT être copié du numéro de séquence donné dans la mise à jour de lien.
  - Le champ Durée de vie DOIT être réglé à zéro.
  - L'option de mobilité Avis de rafraîchissement de lien DOIT être omise.

Les règles pour choisir l'adresse de destination IP (et, si nécessaire, la construction de l'en-tête d'acheminement) pour l'accusé de réception de lien au nœud mobile sont les mêmes qu'au paragraphe précédent. Quand le champ État dans l'accusé de réception de lien est supérieur ou égal à 128 et que l'adresse de source de la mise à jour de lien est sur la liaison de rattachement, et que la mise à jour de lien vient d'un nœud mobile sur la même liaison, l'agent de rattachement DOIT l'envoyer à l'adresse de couche de liaison du nœud mobile (restituée de la mise à jour de lien ou par une sollicitation de voisin).

Quand un nœud mobile envoie une mise à jour de lien pour rafraîchir le lien provenant de la liaison visitée et que peu après il vient sur la liaison de rattachement et envoie une mise à jour de désenregistrement de lien, une condition de conflit peut se produire si la première mise à jour de lien se trouve retardée. La mise à jour de lien retardée peut causer la création par l'agent de rattachement d'une nouvelle entrée d'antémémoire de liens pour un nœud mobile qui vient juste de se rattacher à la liaison de rattachement et a réussi a supprimer le lien. Cela empêcherait le nœud mobile d'utiliser son adresse de rattachement sur la liaison de rattachement.

Afin d'empêcher cela, l'agent de rattachement NE DEVRAIT PAS supprimer l'entrée d'antémémoire de liens immédiatement après avoir reçu la mise à jour de désenregistrement de lien pour le nœud mobile. Il DEVRAIT marquer l'entrée d'antémémoire de liens comme invalide, et DOIT arrêter d'intercepter les paquets sur la liaison de rattachement du nœud mobile qui sont adressés au nœud mobile (paragraphe 10.4.1). L'agent de rattachement devrait attendre pendant MAX_DELETE_BCE_TIMEOUT (Section 12) secondes avant de supprimer l'entrée d'antémémoire de liens complètement. Dans le scénario décrit ci-dessus, si l'agent de rattachement reçoit la mise à jour de lien retardée que le nœud mobile a envoyé de la liaison visitée, il rejetterait le message car le numéro de séquence serait inférieur à la dernière mise à jour de désenregistrement de lien provenant de la liaison de rattachement. L'agent de rattachement enverrait alors un accusé de réception de lien avec l'état "135" (Numéro de séquence hors de la fenêtre) à l'adresse d'entretien sur la liaison visitée. Le nœud mobile peut continuer à utiliser l'adresse de rattachement provenant de la liaison de rattachement.

10.4 Traitement des paquets

10.4.1 Interception de paquets pour un nœud mobile

Lorsque un nœud sert d'agent de rattachement pour un nœud mobile, il DOIT tenter d'intercepter sur la liaison de rattachement du nœud mobile les paquets qui sont adressés au nœud mobile.

Afin de le faire, quand un nœud commence à servir d'agent de rattachement, il DOIT avoir effectué la détection d'adresse dupliquée (comme spécifié au paragraphe 10.3.1) et ensuite, il DOIT envoyer en diffusion groupée sur la liaison de rattachement un message Annonce de voisin [RFC4861] au nom du nœud mobile. Pour l'adresse de rattachement spécifiée dans la mise à jour de lien, l'agent de rattachement envoie un message Annonce de voisin [RFC4861] à l'adresse de diffusion groupée Tous-les-nœuds sur la liaison de rattachement pour annoncer la propre adresse de couche de liaison de l'agent de rattachement pour cette adresse IP au nom du nœud mobile. Si le bit fanion L (compatibilité d'adresse de couche de liaison) a été spécifié dans la mise à jour de lien, l'agent de rattachement DOIT faire de même pour l'adresse de liaison locale du nœud mobile.

Tous les champs de chaque message Annonce de voisin DEVRAIENT être réglés de la même façon qu'ils le seraient par le nœud mobile si il envoyait cette annonce de voisin [RFC4861] lorsque il est chez lui, avec les exceptions suivantes :

- L'adresse cible dans l'annonce de voisin DOIT être réglée à l'adresse IP spécifique pour le nœud mobile.
- L'annonce DOIT inclure une option Adresse de couche liaison cible spécifiant l'adresse de couche de liaison de l'agent de rattachement.
- Le bit R (Routeur) dans l'annonce DOIT être réglé à zéro.

- o Le fanion S (Sollicité) dans l'annonce NE DOIT PAS être établi, car il n'a pas été sollicité par une sollicitation de voisin.
- o Le fanion O (Outrepasser) dans l'annonce DOIT être établi, indiquant que l'annonce DEVRAIT outrepasser toute entrée existante d'antémémoire de voisin chez tout nœud qui la reçoit.
- o L'adresse de source dans l'en-tête IPv6 DOIT être réglée à l'adresse IP de l'agent de rattachement sur l'interface utilisée pour envoyer l'annonce.

Tout nœud sur la liaison de rattachement qui reçoit un des messages d'annonce de voisin (décrits ci-dessus) va mettre à jour son antémémoire de voisin pour associer l'adresse du nœud mobile à l'adresse de couche de liaison de l'agent de rattachement, pour qu'il transmette tous les futurs paquets normalement destinés au nœud mobile à l'agent de rattachement du nœud mobile. Comme la diffusion groupée sur la liaison locale (comme Ethernet) n'est normalement pas d'une fiabilité garantie, l'agent de rattachement PEUT retransmettre cette annonce de voisin jusqu'à MAX_NEIGHBOR_ADVERTISEMENT (voir la [RFC4861]) fois pour augmenter sa fiabilité. Il est encore possible que certains nœuds sur la liaison de rattachement ne reçoivent aucune des annonces de voisin, mais ces nœuds vont finalement être capables de détecter le changement d'adresse de couche de liaison pour l'adresse du nœud mobile par l'utilisation de la détection de voisin injoignable [RFC4861].

Lorsque un nœud sert d'agent de rattachement pour un nœud mobile, l'agent de rattachement utilise la découverte de voisin IPv6 [RFC4861] pour intercepter les paquets en envoi individuel sur la liaison de rattachement adressés au nœud mobile. Afin d'intercepter les paquets de cette façon, l'agent de rattachement DOIT agir comme mandataire pour ce nœud mobile et répondre à toutes les sollicitations de voisin reçues pour lui. Quand un agent de rattachement reçoit une sollicitation de voisin, il DOIT vérifier si l'adresse cible spécifiée dans le message correspond à l'adresse d'un nœud mobile pour lequel il a une entrée d'antémémoire de liens marquée comme enregistrement de rattachement.

Si une telle entrée existe dans l'antémémoire de liens de l'agent de rattachement, l'agent de rattachement DOIT répondre à la sollicitation de voisin par une annonce de voisin donnant la propre adresse de couche de liaison de l'agent de rattachement comme adresse de couche de liaison pour l'adresse cible spécifiée. De plus, le bit R (Routeur) dans l'annonce DOIT être réglé à zéro. Agissant comme mandataire de cette façon permet aux autres nœuds sur la liaison de rattachement du nœud mobile de résoudre l'adresse du nœud mobile et pour l'agent de rattachement de défendre ces adresses sur la liaison de rattachement pour la détection d'adresse dupliquée [RFC4861].

10.4.2 Traitement des paquets interceptés

Pour tout paquet envoyé à un nœud mobile depuis l'agent de rattachement du nœud mobile (et dans ce cas l'agent de rattachement est l'envoyeur original du paquet) l'agent de rattachement fonctionne comme un nœud correspondant du nœud mobile pour ce paquet et les procédures décrites au paragraphe 9.3.2 s'appliquent. L'agent de rattachement utilise alors un en-tête d'acheminement pour acheminer le paquet au nœud mobile au moyen de l'adresse d'entretien principale dans l'antémémoire de liens de l'agent de rattachement.

Pendant que le nœud mobile est hors de chez lui, l'agent de rattachement intercepte tous les paquets sur la liaison de rattachement qui sont adressés à l'adresse de rattachement du nœud mobile, comme décrit au paragraphe 10.4.1. Afin de transmettre chaque paquet intercepté au nœud mobile, l'agent de rattachement DOIT tunneler le paquet au nœud mobile en utilisant l'encapsulation IPv6 [RFC2473]. Quand un agent de rattachement encapsule un paquet intercepté pour le transmettre au nœud mobile, l'agent de rattachement règle l'adresse de source dans le nouvel en-tête de tunnel IP à la propre adresse IP de l'agent de rattachement et règle l'adresse de destination dans l'en-tête de tunnel IP à l'adresse d'entretien principale du nœud mobile. Quand il est reçu par le nœud mobile, le traitement normal de l'en-tête de tunnel [RFC2473] va résulter en la désencapsulation et le traitement du paquet original par le nœud mobile.

Cependant, les paquets adressés à l'adresse de liaison locale du nœud mobile NE DOIVENT PAS être tunnelés au nœud mobile. À la place, ces paquets DOIVENT être éliminés et l'agent de rattachement DEVRAIT retourner un message ICMP Destination injoignable, code 3, à l'adresse de source du paquet (sauf si cette adresse de source est une adresse de diffusion groupée).

L'interception et le tunnelage des paquets suivants adressés en diffusion groupée sur le réseau de rattachement ne sont faits que si l'agent de rattachement prend en charge les messages de contrôle d'appartenance à un groupe de diffusion groupée provenant du nœud mobile comme décrit au paragraphe suivant. Le tunnelage de paquets en diffusion groupée à un nœud mobile suit des limitations similaires à celles définies ci-dessus pour les paquets en envoi individuel adressés à l'adresse de liaison locale du nœud mobile. Les paquets en diffusion groupée adressés à une adresse de diffusion groupée avec une portée de liaison locale [RFC4291], auxquels le nœud mobile est abonné, NE DOIVENT PAS être tunnelés au nœud mobile. Ces paquets DEVRAIENT être éliminés en silence (après livraison aux autres receveurs locaux de diffusion groupée). Les paquets en diffusion groupée adressés à une adresse de diffusion groupée d'une portée plus large que la liaison locale, mais plus petite que mondiale (par exemple, limitée au site et limitée à l'organisation [RFC4291]) auxquels

le nœud mobile est abonné, NE DEVRAIENT PAS être tunnelés au nœud mobile. Les paquets en diffusion groupée adressés avec une portée mondiale, auxquels le nœud mobile s'est abonné avec succès, DOIVENT être tunnelés au nœud mobile.

Avant de tunneler un paquet au nœud mobile, l'agent de rattachement DOIT effectuer tous le traitement IPsec indiqué par la base de données de politique de sécurité.

10.4.3 Contrôle de l'appartenance au groupe de diffusion groupée

Ce paragraphe est un préalable à la transmission de paquet de données en diffusion groupée, décrite au paragraphe précédent. Si cette prise en charge n'est pas assurée, les messages de contrôle d'appartenance au groupe de diffusion groupée sont ignorés en silence.

Afin de transmettre les paquets de données en diffusion groupée provenant du réseau de rattachement à tous les nœuds mobiles appropriés, l'agent de rattachement DEVRAIT être capable de recevoir des informations tunnelées de contrôle d'appartenance à un groupe de diffusion groupée provenant du nœud mobile afin de déterminer à quels groupes le nœud mobile s'est abonné. Ces messages d'appartenance à un groupe de diffusion groupée sont les messages de rapport d'écoutant spécifiés dans la découverte d'écoutant de diffusion groupée (MLD, *Multicast Listener Discovery*) [RFC2710] ou dans d'autres protocoles tels que la [RFC3810].

Les messages sont produits par le nœud mobile, mais envoyés à travers le tunnel inverse à l'agent de rattachement. Ces messages sont produits chaque fois que le nœud mobile décide d'activer la réception des paquets pour un groupe de diffusion groupée ou en réponse à une interrogation de MLD provenant de l'agent de rattachement. Le nœud mobile va aussi produire des messages de contrôle de groupe de diffusion groupée pour désactiver la réception des paquets en diffusion groupée quand il n'est plus intéressé à recevoir de diffusions groupées pour un certain groupe.

Pour obtenir l'appartenance actuelle du nœud mobile à des groupes de diffusion groupée, l'agent de rattachement doit périodiquement transmettre des messages d'interrogation MLD à travers le tunnel au nœud mobile. Ces transmissions MLD périodiques vont assurer que l'agent de rattachement a un enregistrement précis des groupes auxquels le nœud mobile est intéressé en dépit des pertes de paquet de messages d'appartenance à des groupes de diffusion groupée MLD du nœud mobile.

Tous les paquets MLD sont envoyés directement entre le nœud mobile et l'agent de rattachement. Comme tous ces paquets sont destinés à une adresse de diffusion groupée de portée de liaison et ont une limite de bond de 1, il n'y a pas de transmission directe de ces paquets entre le réseau de rattachement et le nœud mobile. Les paquets MLD entre le nœud mobile et l'agent de rattachement sont encapsulés dans le même en-tête de tunnel qu'utilisé pour les autres flux de paquets entre le nœud mobile et l'agent de rattachement.

Noter que pour l'instant, même si une source de liaison locale est utilisée sur les paquets MLD, aucune fonctionnalité ne dépend de ce que ces adresses soient uniques, ni qu'elles appellent de réponse directe. Tous les messages MLD sont envoyés à des destinations de diffusion groupée. Pour éviter toute ambiguïté chez l'agent de rattachement, du fait que les nœuds mobiles peuvent choisir des adresses de source de liaison locale identiques pour leur fonction MLD, il est nécessaire que l'agent de rattachement identifie quel nœud mobile est réellement le producteur d'un message MLD particulier. Ceci peut être réalisé en notant sur quel tunnel un tel MLD est arrivé, quelle association de sécurité (SA) IPsec a été utilisée, ou par d'autres moyens distinctifs.

La présente spécification n'impose aucune exigence aux fonctions de ce paragraphe et à la façon dont la transmission de diffusion groupée du paragraphe 10.4.2 va être réalisée. Au moment de cette rédaction, on pense qu'une pleine fonction de routeur IPv6 de diffusion groupée serait nécessaire chez l'agent de rattachement, mais il est possible d'arriver au même effet par une application de "mandataire MLD" couplée avec un noyau de transmission de diffusion groupée. Ceci peut être le sujet de futures spécifications.

10.4.4 Autoconfiguration d'adresse à états pleins

Ce paragraphe décrit comment les agents de rattachement prennent en charge l'utilisation des mécanismes d'autoconfiguration d'adresse à états pleins comme DHCPv6 [RFC3315] à partir des nœuds mobiles. Si cette prise en charge n'est pas fournie, les bits M et O doivent alors rester à zéro sur les messages d'annonce de préfixe mobile. Tout nœud mobile qui envoie des messages DHCPv6 à l'agent de rattachement sans cette prise en charge ne va pas recevoir de réponse.

Si DHCPv6 est utilisé, les paquets sont envoyés avec des adresses de source de liaison locale soit à une adresse de diffusion groupée de portée de liaison, soit à une adresse de liaison locale. Les nœuds mobiles qui désirent emprunter un service

DHCPv6 peuvent inverser les paquets dans le tunnel standard DHCPv6 à l'agent de rattachement. Comme ces paquets de portée de liaison ne peuvent pas être transmis au réseau de rattachement, il est nécessaire que l'agent de rattachement mette lui-même en œuvre soit une fonction d'agent de relais DHCPv6, soit de serveur DHCPv6. Le tunnel d'arrivée ou la SA IPsec des messages DHCPv6 de portée de liaison provenant du nœud mobile doit être noté afin que les réponses DHCPv6 puissent être renvoyées au nœud mobile approprié. Les messages DHCPv6 envoyés au nœud mobile avec une destination de liaison locale doivent être tunnelés dans le même en-tête de tunnel qu'utilisé pour les autres flux de paquets.

10.4.5 Traitement des paquets en tunnelage inverse

Sauf quand un lien a été établi entre le nœud mobile et un nœud correspondant, le trafic du nœud mobile au nœud correspondant passe à travers un tunnel inverse. Les agents de rattachement DOIVENT prendre en charge le tunnelage inverse comme suit :

- Le trafic tunnelé arrive à l'adresse de l'agent de rattachement en utilisant l'encapsulation IPv6 [RFC2473].
- Selon les politiques de sécurité utilisées par l'agent de rattachement, les paquets en tunnelage inverse PEUVENT être éliminés si ils ne sont pas accompagnés par un en-tête ESP valide. La prise en charge du tunnelage inverse authentifié permet à l'agent de rattachement de protéger le réseau de rattachement et les nœuds correspondants de nœuds malveillants qui se font passer pour un nœud mobile.
- Autrement, quand un agent de rattachement désencapsule un paquet tunnelé provenant du nœud mobile, l'agent de rattachement DOIT vérifier que l'adresse de source dans l'en-tête de tunnel IP est l'adresse d'entretien principale du nœud mobile. Autrement, tout nœud dans l'Internet pourrait envoyer du trafic à travers l'agent de rattachement et échapper aux limitations de filtrage d'entrée. Cette simple vérification force l'attaquant à connaître la localisation actuelle réelle du nœud mobile et d'être capable de vaincre le filtrage d'entrée. Cette vérification n'est pas nécessaire si le paquet en tunnel inverse est protégé par ESP en mode tunnel.

10.4.6 Protection des paquets d'acheminement de retour

La procédure d'acheminement de retour, décrite au paragraphe 5.2.5, suppose que la confidentialité des messages Initiation d'essai de rattachement et Essai de rattachement est protégée lorsque ils sont tunnelés entre l'agent de rattachement et le nœud mobile. Donc, l'agent de rattachement DOIT prendre en charge IPsec ESP en mode tunnel pour la protection des paquets qui appartiennent à la procédure d'acheminement de retour. La prise en charge d'un algorithme de transformation de chiffrement non nul et d'authentification DOIT être disponible. Il n'est pas nécessaire de distinguer les différentes sortes de paquets durant la procédure d'acheminement de retour.

Des associations de sécurité sont nécessaires pour fournir cette protection. Quand l'adresse d'entretien pour le nœud mobile change par suite d'une mise à jour de lien acceptée, un traitement particulier est nécessaire pour les prochains paquets envoyés en utilisant ces associations de sécurité. L'agent de rattachement DOIT régler la nouvelle adresse d'entretien comme adresse de destination de ces paquets, comme si l'en-tête externe d'adresse de destination dans l'association de sécurité avait changé.

La protection ci-dessus DEVRAIT être utilisée avec tous les nœuds mobiles. L'utilisation est contrôlée par la configuration de la base de données de politique de sécurité IPsec chez le nœud mobile et chez l'agent de rattachement.

Comme décrit précédemment, les messages Mise à jour de lien et Accusé de réception de lien exigent une protection entre l'agent de rattachement et le nœud mobile. Le protocole d'en-tête de mobilité porte ces deux messages ainsi que les messages d'acheminement de retour. Du point de vue de la base de données de politique de sécurité, ces messages sont indistinguables. Quand IPsec est utilisé pour protéger la signalisation d'acheminement de retour ou les paquets de charge utile, cette protection DOIT seulement être appliquée aux paquets d'acheminement de retour qui entrent dans l'interface de tunnel encapsulé IPv6 entre le nœud mobile et l'agent de rattachement. Ceci peut être réalisé, par exemple, en définissant les entrées de base de données de politique de sécurité spécifiquement pour l'interface de tunnel. C'est-à-dire que les entrées de politique ne sont généralement pas appliquées sur tout le trafic sur la ou les interfaces physiques des nœuds, mais plutôt seulement sur le trafic qui entre dans le tunnel. Cela utilise des entrées de base de données de politique de sécurité par interface [RFC4301] spécifiques de l'interface du tunnel (le rattachement du nœud au tunnel [RFC2460]).

10.5 Découverte dynamique de l'adresse d'agent de rattachement

Ce paragraphe décrit un mécanisme facultatif par lequel un agent de rattachement peut aider les nœuds mobiles à découvrir les adresses des autres agents de rattachement sur le réseau de rattachement du nœud mobile. L'agent de rattachement garde trace des autres agents de rattachement sur la même liaison et répond aux interrogations envoyées par le nœud mobile.

10.5.1 Réception des messages d'annonce de routeur

Pour chaque liaison sur laquelle un routeur fournit le service d'agent de rattachement, le routeur tient une liste des agents de rattachement enregistrant des informations sur tous les autres agents de rattachement sur cette liaison. Cette liste est utilisée dans le mécanisme de découverte dynamique d'adresse d'agent de rattachement ; le nœud mobile utilise la liste comme décrit au paragraphe 11.4.1. Les informations pour la liste sont apprises par la réception des annonces de routeur en diffusion groupée périodiques non sollicitées, d'une manière similaire à la structure de données conceptuelles de liste des routeurs par défaut tenue par chaque hôte pour la découverte de voisin [RFC4861]. Dans la construction de la liste des agents de rattachement, les annonces de routeur sont de chaque (autre) agent de rattachement sur la liaison et le bit H (agent de rattachement) y est établi.

À réception d'une annonce de routeur valide, comme défini dans l'algorithme de traitement spécifié pour la découverte de voisin [RFC4861], l'agent de rattachement effectue les étapes suivantes en plus de toutes celles déjà requises par la découverte de voisin :

- Si le bit H (agent de rattachement) dans l'annonce de routeur n'est pas établi, supprimer l'entrée du nœud envoyeur dans la liste courante des agents de rattachement (si il en existe une). Sauter toutes les étapes suivantes.
- Autrement, extraire l'adresse de source de l'en-tête IP de l'annonce de routeur. C'est l'adresse IP de liaison locale sur cette liaison de l'agent de rattachement qui envoie cette annonce [RFC4861].
- Déterminer la préférence pour cet agent de rattachement. Si l'annonce de routeur contient une option Informations d'agent de rattachement, la préférence est alors prise dans le champ Préférence d'agent de rattachement de l'option ; autrement, la préférence par défaut de 0 DOIT être utilisée.
- Déterminer la durée de vie pour cet agent de rattachement. Si l'annonce de routeur contient une option Informations d'agent de rattachement, la durée de vie est alors prise du champ Durée de vie d'agent de rattachement dans l'option ; sinon, la durée de vie spécifiée par le champ Durée de vie de routeur dans l'annonce de routeur DEVRAIT être utilisée.
- Si l'adresse de liaison locale de l'agent de rattachement qui envoie cette annonce est déjà présente dans la liste des agents de rattachement de cet agent de rattachement et si la valeur de durée de vie d'agent de rattachement reçue est zéro, supprimer immédiatement cette entrée dans la liste des agents de rattachement.
- Autrement, si l'adresse de liaison locale de l'agent de rattachement qui envoie cette annonce est déjà présente dans la liste des agents de rattachement de l'agent de rattachement receveur, rétablir sa durée de vie et sa préférence aux valeurs déterminées ci-dessus.
- Si l'adresse de liaison locale de l'agent de rattachement qui envoie cette annonce n'est pas déjà présente dans la liste des agents de rattachement tenue par l'agent de rattachement receveur, et si la durée de vie pour l'agent de rattachement envoyeur n'est pas zéro, créer une nouvelle entrée dans la liste, et initialiser sa durée de vie et sa préférence aux valeurs déterminées ci-dessus.
- Si l'entrée de la liste des agents de rattachement pour l'adresse de liaison locale de l'agent de rattachement qui envoie cette annonce n'a pas été supprimée comme décrit ci-dessus, déterminer toutes les adresses mondiales de l'agent de rattachement sur la base de chaque option Informations de préfixe reçue dans cette annonce dans laquelle le bit R (adresse de routeur) est établi (paragraphe 7.2). Ajouter toutes ces adresses mondiales à la liste des adresses mondiales dans cette entrée de liste des agents de rattachement.

Un agent de rattachement DEVRAIT tenir une entrée dans sa liste des agents de rattachement pour chaque adresse valide d'agent de rattachement jusqu'à ce que la durée de vie de cette entrée expire, après quoi l'entrée DOIT être supprimée.

Comme décrit au paragraphe 11.4.1, un nœud mobile tente la découverte dynamique d'adresse d'agent de rattachement en envoyant un message ICMP Demande de découverte d'adresse d'agent de rattachement à l'adresse d'envoi à la cantonade Agents-de-rattachement-IPv6-mobile [RFC2526] pour son préfixe de sous réseau IP de rattachement. Un agent de rattachement qui reçoit un message Demande de découverte d'adresse d'agent de rattachement qui dessert ce sous réseau DEVRAIT retourner un message ICMP de réponse de découverte d'adresse d'agent de rattachement au nœud mobile avec l'adresse de source du paquet de réponse réglée à une des adresses mondiales d'envoi individuel de l'agent de rattachement. Le champ Adresse d'agent de rattachement dans le message de réponse est construit comme suit :

- Le champ Adresses d'agent de rattachement DEVRAIT contenir toutes les adresses IP mondiales pour chaque agent de rattachement figurant actuellement sur la propre liste des agents de rattachement de cet agent de rattachement (paragraphe 10.1).
- Les adresses IP dans le champ Adresses d'agent de rattachement DEVRAIENT être dans l'ordre des valeurs décroissantes de préférence, sur la base de la préférence annoncée à partir d'une option Informations d'agent de rattachement ou de la préférence par défaut de 0 si aucune préférence n'est annoncée (ou sur la préférence configurée d'agent de rattachement pour cet agent de rattachement lui-même).
- Parmi les agents de rattachement d'égale préférence, leurs adresses IP dans le champ Adresses d'agent de rattachement DEVRAIENT être dans un ordre rendu aléatoire par rapport aux autres agents de rattachement d'égale préférence chaque fois qu'un message de réponse de découverte d'adresse d'agent de rattachement est retourné par cet agent de rattachement.
- Si plus d'une adresse IP mondiale est associée à un agent de rattachement, ces adresses DEVRAIENT être mises dans un ordre aléatoire sur la liste.

- L'agent de rattachement DEVRAIT réduire le nombre d'adresses IP d'agent de rattachement afin que le paquet tienne dans la MTU IPv6 minimum [RFC2460]. Les adresses d'agent de rattachement choisies pour être incluses dans le paquet DEVRAIT être celles de la liste complète qui ont la plus forte préférence. Cette limitation évite le danger que le paquet de message de réponse soit fragmenté (ou rejeté par un routeur intermédiaire avec un message ICMP Paquet trop gros [RFC4443]).

10.6 Envoi des informations de préfixe au nœud mobile

10.6.1 Liste des préfixes de réseau de rattachement

IPv6 mobile s'arrange pour propager les informations de préfixe pertinentes au nœud mobile quand il est hors de chez lui afin qu'elles puissent être utilisées dans la configuration d'adresse de rattachement du nœud mobile et dans les renumérotations de réseau. Dans ce mécanisme, les nœuds mobiles hors de chez eux reçoivent des messages d'annonce de préfixe mobile. Ces messages incluent des options Informations de préfixe pour les préfixes configurés sur la ou les interfaces de sous réseau de rattachement de l'agent de rattachement.

Si il y a plusieurs agents de rattachement, des différences dans les annonces envoyées par les différents agents de rattachement peuvent conduire à une incapacité d'utiliser une adresse de rattachement particulière quand on change pour un autre agent de rattachement. Afin d'assurer que les nœuds mobiles obtiennent les mêmes informations des différents agents de rattachement, il est préférable que tous les agents de rattachement sur la même liaison soient configurés de la même manière.

Pour prendre cela en charge, l'agent de rattachement surveille les préfixes annoncés par lui-même et par les autres agents de rattachement sur la liaison de rattachement. Dans la découverte de voisin [RFC4861] il est acceptable que deux routeurs annoncent des ensembles différents de préfixes sur la même liaison. Pour les agents de rattachement, les différences devraient être détectées pour une certaine adresse de rattachement parce que le nœud mobile communique seulement avec un agent de rattachement à la fois et que le nœud mobile a besoin de savoir l'ensemble complet de préfixes alloués à la liaison de rattachement. Toutes les autres comparaisons d'annonces de routeur sont comme spécifié au paragraphe 6.2.7 de la RFC 4861.

10.6.2 Programmation de la livraison des préfixes

Un agent de rattachement qui dessert un nœud mobile va programmer la livraison des nouvelles informations de préfixe à ce nœud mobile quand une des conditions suivantes se produit :

DOIT :
- L'état des fanions change pour le préfixe de l'adresse de rattachement enregistrée du nœud mobile.
- La durée de vie valide ou préférée est reconfigurée ou change pour toute raison autre que l'avancement de l'heure.
- Le nœud mobile demande les informations avec une sollicitation de préfixe mobile (voir au paragraphe 11.4.2).

DEVRAIT :
- Un nouveau préfixe est ajouté à la ou aux interfaces du sous réseau de rattachement de l'agent de rattachement.

PEUT :
- La durée de vie valide ou préférée ou l'état des fanions change pour un préfixe qui n'est pas utilisé dans une entrée d'antémémoire de liens pour ce nœud mobile.

L'agent de rattachement utilise l'algorithme suivant pour déterminer quand envoyer les informations de préfixe au nœud mobile :
- Si un nœud mobile envoie une sollicitation, répondre immédiatement.
- Si aucune annonce de préfixe mobile n'a été envoyée au nœud mobile dans les dernières MaxMobPfxAdvInterval secondes (voir la Section 13) s'assurer alors qu'une transmission est programmée. L'heure réelle de transmission est rendue aléatoire comme décrit lus loin.
- Si un préfixe correspondant à l'enregistrement de rattachement du nœud mobile est ajouté sur l'interface du sous réseau de rattachement ou si ses informations changent d'une façon qui ne déconseille pas l'adresse du nœud mobile, s'assurer qu'une transmission est programmée. L'heure réelle de transmission est rendue aléatoire comme décrit plus loin.
- Si un enregistrement de rattachement expire, annuler toute annonce programmée au nœud mobile.

La liste des préfixes est envoyée en entier dans tous les cas.

Si l'agent de rattachement a déjà programmé la transmission d'une annonce de préfixe mobile au nœud mobile, l'agent de rattachement va alors remplacer l'annonce par une nouvelle à envoyer au moment programmé.

Autrement, l'agent de rattachement calcule une valeur fraîche pour RAND_ADV_DELAY qui se décale de l'heure actuelle pour la transmission programmée. D'abord, calculer le délai maximum pour l'annonce programmée :

MaxScheduleDelay = min (MaxMobPfxAdvInterval, Durée de vie préférée),

où MaxMobPfxAdvInterval est comme défini à la Section 12. Puis, calculer le délai final pour l'annonce :

RAND_ADV_DELAY = MinMobPfxAdvInterval + (rand() % abs(MaxScheduleDelay - MinMobPfxAdvInterval))

Ici, rand() retourne une valeur d'entier aléatoire dans la gamme de 0 à la valeur d'entier maximum possible. Ce calcul est supposé diminuer les salves d'annonces quand les informations de préfixe changent. De plus, un agent de rattachement PEUT réduire encore le taux de transmission de paquets en retardant les annonces individuelles, quand nécessaire pour éviter de submerger les ressources réseau locales. L'agent de rattachement DEVRAIT périodiquement continuer de retransmettre un annonce non sollicitée au nœud mobile, jusqu'à ce qu'elle soit acquittée par la réception d'une sollicitation de préfixe mobile provenant du nœud mobile.

L'agent de rattachement DOIT attendre PREFIX_ADV_TIMEOUT (voir la Section 12) avant la première retransmission et doubler le temps d'attente de retransmission pour chaque retransmission réussie jusqu'à un nombre maximum de PREFIX_ADV_RETRIES tentatives (voir la Section 12). Si le lien du nœud mobile expire avant que la mise à jour de lien correspondante ait été reçue, l'agent de rattachement NE DOIT alors PAS tenter d'autres retransmissions, même si toutes les PREFIX_ADV_RETRIES n'ont pas été retransmises. Dans l'intervalle, si le nœud mobile envoie une autre mise à jour de lien sans rentrer chez lui, l'agent de rattachement DEVRAIT alors recommencer à transmettre les annonces non sollicitées.

Si une condition, comme décrit ci-dessus, se produit sur la liaison de rattachement et cause l'envoi d'une autre annonce de préfixe au nœud mobile, avant l'accusé de réception par le nœud mobile d'une transmission antérieure, l'agent de rattachement DEVRAIT combiner toutes les options Informations de préfixe de l'annonce de préfixe mobile non acquittée dans une nouvelle annonce. L'agent de rattachement élimine alors la vieille annonce.

10.6.3 Envoi des annonces

Quand il envoie une annonce de préfixe mobile au nœud mobile, l'agent de rattachement DOIT construire le paquet comme suit :

- L'adresse de source dans l'en-tête IPv6 du paquet DOIT être réglée à l'adresse IP de l'agent de rattachement auquel le nœud mobile a adressé son enregistrement de rattachement actuel ou son adresse mondiale d'agent de rattachement par défaut si il n'existe pas de lien.
- Si l'annonce était sollicitée, elle DOIT être destinée à l'adresse de source de la sollicitation. Si elle a été déclenchée par un changement de préfixe ou de numérotation, la destination de l'annonce sera l'adresse de rattachement du nœud mobile dans le lien qui a déclenché la règle.
- Un en-tête d'acheminement de type 2 DOIT être inclus avec l'adresse de rattachement du nœud mobile.
- Les en-têtes IPsec DOIVENT être pris en charge et DEVRAIENT être utilisés.
- L'agent de rattachement DOIT envoyer le paquet comme il le ferait de tout autre paquet IPv6 en envoi individuel qu'il génère.
- Établir le fanion M (Configuration d'adresse gérée) si le fanion correspondant a été établi dans toute annonce de routeur de laquelle ont été apprises des informations de préfixe (incluant celles envoyées par cet agent de rattachement).
- Établir le fanion O (Autres configurations à états pleins) si le fanion correspondant était établi dans une des annonces de routeur desquelles ont été apprises des informations de préfixe (incluant celles envoyées par cet agent de rattachement).

10.6.4 Durée de vie des préfixes changés

Comme décrit au paragraphe 10.3.1, la durée de vie retournée par l'agent de rattachement dans un accusé de réception de lien NE DOIT PAS être supérieure à la durée de vie valide restante pour le préfixe de sous réseau dans l'adresse de rattachement du nœud mobile. Cette limite sur la durée de vie du lien sert à interdire l'utilisation d'une adresse de rattachement du nœud mobile devenue invalide.

11. Fonctionnement du nœud mobile

11.1 Structures de données conceptuelles

Chaque nœud mobile DOIT tenir une liste des mises à jour de liens.

La liste des mises à jour de liens enregistre les informations sur chaque mise à jour de lien envoyée par ce nœud mobile, dans laquelle la durée de vie du lien n'est pas encore expirée. La liste des mises à jour de lien inclut tous les liens envoyés par le nœud mobile à son agent de rattachement ou à ses nœuds correspondants. Elle contient aussi les mises à jour de lien qui attendent l'achèvement de la procédure d'acheminement de retour avant qu'elles puissent être envoyées. Cependant, pour des mises à jour de lien multiples envoyées à la même adresse de destination, la liste des mises à jour de lien contient seulement la plus récente mise à jour de lien (c'est-à-dire, avec la plus forte valeur de numéro de séquence) envoyée à cette destination. La liste des mises à jour de lien PEUT être mise en œuvre de toute façon cohérente avec le comportement externe décrit dans le présent document.

Chaque entrée de liste de mises à jour de lien contient conceptuellement les champs suivants :
- o L'adresse IP du nœud auquel une mise à jour de lien a été envoyée.
- o L'adresse de rattachement pour laquelle cette mise à jour de lien a été envoyée.
- o L'adresse d'entretien envoyée dans cette mise à jour de lien. Cette valeur est nécessaire pour que le nœud mobile détermine si il a envoyé une mise à jour de lien quand il a envoyé sa nouvelle adresse d'entretien à cette destination après avoir changé son adresse d'entretien.
- o La valeur initiale du champ Durée de vie envoyé dans cette mise à jour de lien.
- o La durée de vie restante de ce lien. Cette durée de vie est initialisée à partir de la valeur de durée de vie envoyée dans la mise à jour de lien et est décrémentée jusqu'à ce qu'elle atteigne zéro, moment où cette entrée DOIT être supprimée de la liste des mises à jour de lien.
- o La valeur maximum du champ Numéro de séquence envoyé dans les précédentes mises à jour de lien à cette destination. Le champ Numéro de séquence fait 16 bits et toute comparaison entre valeurs de numéro de séquence DOIT être effectuée modulo 2**16 (voir au paragraphe 9.5.1).
- o Le moment auquel une mise à jour de lien a été envoyée pour la dernière fois à cette destination, comme nécessaire pour mettre en œuvre la restriction de limitation de taux pour l'envoi des mises à jour de lien.
- o L'état de toutes les retransmissions nécessaires pour cette mise à jour de lien. Cet état inclut le temps restant jusqu'à la prochaine tentative de retransmission pour la mise à jour de lien et l'état actuel du mécanisme de retard exponentiel pour les retransmissions.
- o Un fanion spécifiant si de futures mises à jour de lien devraient ou non être envoyées à cette destination. Le nœud mobile établit ce fanion dans l'entrée de liste des mises à jour de lien quand il reçoit un message ICMP Erreur de paramètre, code 1, en réponse à un message d'acheminement de retour ou à une mise à jour de lien envoyée à cette destination, comme décrit au paragraphe 11.3.5.

La liste des mises à jour de lien est utilisée pour déterminer si un paquet particulier est envoyé directement au nœud correspondant ou tunnelé via l'agent de rattachement (voir au paragraphe 11.3.1).

La liste des mises à jour de lien contient aussi conceptuellement les données suivantes relatives à la procédure d'acheminement de retour. Ces données ne sont pertinentes que pour les mises à jour de lien envoyées aux nœuds correspondants.
- o L'heure à laquelle le dernier message Initiation d'essai de rattachement ou Initiation d'essai d'entretien a été envoyé à cette destination, comme nécessaire pour mettre en œuvre la restriction de limitation de taux d'envoi pour la procédure d'acheminement de retour.
- o L'état de toute retransmission nécessaire pour cette procédure d'acheminement de retour. Cet état inclut le temps restant jusqu'à la prochaine tentative de retransmission et l'état actuel du mécanisme de retard exponentiel des retransmissions.
- o Les valeurs de mouchards utilisées dans les messages Initiation d'essai de rattachement et Initiation d'essai d'entretien.
- o Les jetons de génération de clé de rattachement et d'entretien reçus du nœud correspondant.
- o Les indices de nom occasionnel de rattachement et d'entretien reçus du nœud correspondant.
- o L'heure à laquelle chacun des jetons et noms occasionnels ont été reçus du nœud correspondant, comme nécessaire pour mettre en œuvre la réutilisation lors d'un déplacement.

11.2 Traitement des en-têtes de mobilité

Tous les nœuds IPv6 mobiles DOIVENT observer les règles décrites au paragraphe 9.2 dans le traitement d'en-tête de mobilité.

11.3 Traitement des paquets

11.3.1 Envoi des paquets durant l'itinérance

Lorsque un nœud mobile est hors de chez lui, il continue d'utiliser son adresse de rattachement, ainsi aussi que d'utiliser une ou plusieurs adresses d'entretien. Quand il envoie un paquet lorsque il est hors de chez lui, un nœud mobile PEUT choisir parmi elles en sélectionnant l'adresse qu'il va utiliser comme source du paquet, comme suit :

- Les protocoles en couche sur IP vont généralement traiter l'adresse de rattachement du nœud mobile comme son adresse IP de source pour la plupart des paquets. Pour les paquets envoyés qui font partie de connexions de niveau transport établies lorsque le nœud mobile était chez lui, le nœud mobile DOIT utiliser son adresse de rattachement. De même, pour les paquets envoyés qui font partie de connexions de niveau transport que le nœud mobile peut encore utiliser après s'être déplacé dans une nouvelle localisation, le nœud mobile DEVRAIT utiliser son adresse de rattachement de cette façon. Si un lien existe, le nœud mobile DEVRAIT envoyer les paquets directement au nœud correspondant. Autrement, si il n'existe pas de lien, le nœud mobile DOIT utiliser le tunnelage inverse.
- Le nœud mobile PEUT choisir d'utiliser directement une de ses adresses d'entretien comme source du paquet, en n'exigeant pas l'utilisation d'une option Adresse de rattachement dans le paquet. Ceci est particulièrement utile pour une communication à court terme qui peut facilement être réessayée en cas d'échec. Utiliser l'adresse d'entretien du nœud mobile comme source pour de telles interrogations va généralement avoir de plus faibles frais généraux que d'utiliser l'adresse de rattachement du nœud mobile, car aucune option supplémentaire n'a besoin d'être utilisée ni dans l'interrogation ni dans sa réponse. De tels paquets peuvent être acheminés normalement, directement entre leur source et leur destination sans s'appuyer sur IPv6 mobile. Si l'application qui fonctionne sur le nœud mobile n'a pas de connaissance particulière que la communication envoyée tient dans ce type général de communication, le nœud mobile ne devrait cependant pas utiliser de cette façon son adresse d'entretien comme source du paquet. Le choix de la méthode la plus efficace de communications est spécifique de l'application, et sort du domaine d'application de la présente spécification. Les API nécessaires pour contrôler le choix sortent aussi de ce domaine d'application. Un exemple d'une telle API est décrit dans la [RFC5014] "API de prises IPv6 pour la sélection d'adresse de source".
- Lorsque il n'est pas sur sa liaison de rattachement, le nœud mobile NE DOIT PAS utiliser l'option de destination Adresse de rattachement quand il communique avec des homologues sur la liaison locale.

De même, le nœud mobile NE DOIT PAS utiliser l'option de destination Adresse de rattachement pour des paquets IPv6 de découverte de voisin [RFC4861].

Le fonctionnement détaillé de ces cas est décrit plus loin dans cette section et aussi discuté dans la [RFC3484].

Pour les paquets envoyés par un nœud mobile lorsque il est chez lui, aucun traitement spécial IPv6 mobile n'est requis. De même, si le nœud mobile utilise une adresse autre qu'une de ses adresses de rattachement comme source d'un paquet envoyé lorsque il est hors de chez lui, aucun traitement spécial IPv6 mobile n'est requis. Dans l'un et l'autre cas, le paquet est simplement adressé et transmis de la même façon que tout paquet IPv6 normal.

Pour les paquets envoyés par le nœud mobile lorsque il est hors de chez lui en utilisant l'adresse de rattachement du nœud mobile comme source, un traitement IPv6 mobile spécial du paquet est requis. Ceci peut être fait d'une des deux façons suivantes :

Optimisation de chemin : cette manière de livrer les paquets n'exige pas de passer par le réseau de rattachement, et permet normalement une transmission plus rapide et plus fiable.

Le nœud mobile doit s'assurer qu'une entrée d'antémémoire de liens existe pour son adresse de rattachement afin que le nœud correspondant puisse traiter le paquet (le paragraphe 9.3.1 spécifie les règles pour le traitement de l'option de destination Adresse de rattachement chez un nœud correspondént). Le nœud mobile DEVRAIT examiner sa liste de mises à jour de lien pour une entrée satisfaisant aux conditions suivantes :

* Le champ Adresse de source du paquet envoyé est égal à l'adresse de rattachement dans l'entrée.
* Le champ Adresse de destination du paquet envoyé est égal à l'adresse du nœud correspondant dans l'entrée.
* Une des adresses d'entretien courantes du nœud mobile apparaît comme adresse d'entretien dans l'entrée.
* L'entrée indique qu'un lien a bien été créé.
* La durée de vie restante du lien est supérieure à zéro.

Quand ces conditions sont satisfaites, le nœud mobile sait que le nœud correspondant a une entrée d'antémémoire de liens convenable.

Un nœud mobile DEVRAIT s'arranger pour fournir l'adresse de rattachement dans une option Adresse de rattachement, et DOIT régler le champ Adresse de source de l'en-tête IPv6 à l'adresse d'entretien que le nœud mobile a enregistré pour être utilisée avec ce nœud correspondant. Le nœud correspondant va alors utiliser l'adresse fournie dans l'option Adresse de rattachement pour servir la fonction traditionnellement effectuée par l'adresse IP de source dans l'en-tête IPv6. L'adresse de rattachement du nœud mobile est alors fournie aux protocoles et applications de couches supérieures.

Spécifiquement :

* Construire le paquet en utilisant l'adresse de rattachement du nœud mobile comme adresse de source du paquet, de la même façon que si le nœud mobile était chez lui. Cela inclut de calculer la comme de contrôle de couche supérieure en utilisant l'adresse de rattachement comme valeur de la source.

* Insérer une option Adresse de rattachement dans le paquet avec le champ Adresse de rattachement copié de la valeur originale du champ Adresse de source dans le paquet.
* Changer le champ Adresse de source dans l'en-tête IPv6 du paquet en une des adresses d'entretien du nœud mobile. Ceci va normalement être l'adresse d'entretien principale actuelle du nœud mobile, mais DOIT être une adresse allouée à l'interface sur la liaison utilisée.

En utilisant l'adresse d'entretien comme adresse de source dans l'en-tête IPv6, avec l'adresse de rattachement du nœud mobile à la place de l'option Adresse de rattachement, le paquet va être capable de passer en toute sécurité à travers tout routeur qui met en œuvre le filtrage d'entrée [RFC2827].

Tunnelage inverse :
C'est le mécanisme qui tunnelle les paquets via l'agent de rattachement. Ce n'est pas aussi efficace que le mécanisme précédent, mais il est nécessaire si il n'y a pas encore de lien avec le nœud correspondant.
Ce mécanisme est utilisé pour les paquets qui ont l'adresse de rattachement du nœud mobile comme adresse de source dans l'en-tête IPv6, ou avec les paquets de protocole de contrôle de diffusion groupée comme décrit au paragraphe 11.3.4.
Spécifiquement :

* Le paquet est envoyé à l'agent de rattachement en utilisant l'encapsulation IPv6 [RFC2473].
* L'adresse de source dans le paquet tunnelé est l'adresse d'entretien principale comme enregistrée auprès de l'agent de rattachement.
* L'adresse de destination dans le paquet tunnelé est l'adresse de l'agent de rattachement.

Ensuite, l'agent de rattachement va passer le paquet encapsulé au nœud correspondant.

11.3.2 Interaction avec le traitement IPsec sortant

Ce paragraphe décrit l'interaction entre le traitement IPv6 mobile sortant et le traitement de sécurité IP (IPsec) sortant pour les paquets envoyés par un nœud mobile hors de chez lui. Toute mise en œuvre spécifique PEUT utiliser des algorithmes et structures de données autres que ce qui est suggéré ici, mais son traitement DOIT être cohérent avec l'effet de l'opération décrite ici et avec les spécifications IPsec pertinentes. Dans les étapes décrites ci-dessous, on suppose que IPsec est utilisé en mode transport [RFC4301] et que le nœud mobile utilise son adresse de rattachement comme source pour le paquet (du point de vue des couches de protocole supérieures ou applications, comme décrit au paragraphe 11.3.1) :

o Le paquet est créé par les protocoles et applications de couche supérieure (par exemple, TCP) comme si le nœud mobile était chez lui et qu'IPv6 mobile n'était pas utilisé.
o Déterminer l'interface sortante pour le paquet. (Noter que le choix entre tunnelage inverse et optimisation de chemin peut impliquer des interfaces différentes, en particulier si les tunnels sont considérés aussi comme des interfaces.)
o Au titre du traitement du paquet sortant dans IP, le paquet est comparé à la base de données de politique de sécurité IPsec pour déterminer quel traitement est requis pour le paquet [RFC4301].
o Si le traitement IPsec est requis, le paquet est transposé en une association de sécurité (ou bouquet de SA) existante, ou une nouvelle SA (ou bouquet de SA) est créé pour le paquet, conformément aux procédures définies pour IPsec.
o Comme le nœud mobile est hors de chez lui, le mobile utilise le tunnelage inverse ou l'optimisation de chemin pour joindre le nœud correspondant.

Si le tunnelage inverse est utilisé, le paquet est construit de la manière normale et ensuite tunnelé à travers l'agent de rattachement.

Si l'optimisation de chemin est utilisée, le nœud mobile insère une option de destination Adresse de rattachement dans le paquet, remplaçant l'adresse de source dans l'en-tête IP du paquet par l'adresse d'entretien utilisée avec ce nœud correspondant, comme décrit au paragraphe 11.3.1. L'en-tête d'options de destination dans lequel est insérée l'option de destination Adresse de rattachement DOIT apparaître dans le paquet après l'en-tête d'acheminement, si présent, et avant l'en-tête IPsec (AH [RFC4302] ou ESP [RFC4303]) de sorte que l'option de destination Adresse de rattachement est traitée par le nœud de destination avant l'en-tête IPsec.

Finalement une fois que le paquet est pleinement assemblé, la nécessaire authentification IPsec (et le chiffrement, si exigé) est effectuée sur le paquet, initialisant les données authentification dans l'en-tête IPsec.

Le traitement des options de destination décrit dans la RFC 4302 est étendu comme suit. Les données d'authentification AH DOIVENT être calculées comme si ce qui suit était vrai :

* l'adresse IPv6 de source dans l'en-tête IPv6 contient l'adresse de rattachement du nœud mobile, et
* le champ Adresse de rattachement de l'option de destination Adresse de rattachement (paragraphe 6.3) contient la nouvelle adresse d'entretien.

o Cela permet, mais n'exige pas, que le receveur du paquet contenant une option de destination Adresse de rattachement échange les deux champs du paquet entrant pour arriver à la situation ci-dessus, simplifiant le traitement pour tous les

en-têtes suivants du paquet. Cependant, un tel échange n'est pas exigé, pour autant que le résultat du calcul de l'authentification reste le même.

Quand un protocole automatisé de gestion de clés est utilisé pour créer une nouvelle associations de sécurité pour un homologue, il est important de s'assurer que l'homologue peut envoyer les paquets de protocole de gestion de clés au nœud mobile. Ce n'est pas possible si l'homologue est l'agent de rattachement du nœud mobile et l'objet des associations de sécurité serait d'envoyer une mise à jour de lien à l'agent de rattachement. Les paquets adressés à l'adresse de rattachement du nœud mobile ne peuvent pas être utilisés avant que la mise à jour de lien ait été traitée. Pour le cas par défaut de l'utilisation de IKEv2 [RFC5996] comme protocole automatisé de gestion de clés, ces problèmes peuvent être évités par les exigences suivantes lorsque la communication est avec son agent de rattachement :

- Quand le nœud mobile est hors de chez lui, il DOIT utiliser son adresse d'entretien comme adresse de source de tous les paquets qu'il envoie au titre du protocole de gestion de clés (sans l'utilisation de IPv6 mobile pour ces paquets, comme suggéré au paragraphe 11.3.1).

Le bit K (capacité de mobilité de gestion de clé) dans les mises à jour de lien et les accusés de réception peuvent être utilisés pour éviter d'avoir besoin de relancer IKEv2 lors des mouvements.

11.3.3 Réception des paquets durant l'itinérance

Quand il est hors de chez lui, un nœud mobile va recevoir des paquets adressés à son adresse de rattachement, par une des deux méthodes suivantes :

- Les paquets envoyés par un nœud correspondant qui n'a pas une entrée d'antémémoire de liens pour le nœud mobile vont être envoyés à l'adresse de rattachement, capturés par l'agent de rattachement et tunnelés au nœud mobile.
- Les paquets envoyés par un nœud correspondant qui a une entrée d'antémémoire de liens pour le nœud mobile qui contient l'adresse d'entretien courante du nœud mobile vont être envoyés par le nœud correspondant en utilisant un en-tête d'acheminement de type 2. Le paquet va être adressé à l'adresse d'entretien du nœud mobile, avec le bond final dans l'en-tête d'acheminement qui dirige le paquet sur l'adresse de rattachement du nœud mobile ; le traitement de ce dernier bond de l'en-tête d'acheminement est entièrement interne au nœud mobile, car l'adresse d'entretien et l'adresse de rattachement sont toutes deux des adresses au sein du nœud mobile.

Pour les paquets reçus par la première méthode, le nœud mobile DOIT vérifier que l'adresse IPv6 de source du paquet tunnelé est l'adresse IP de son agent de rattachement. Dans cette méthode, le nœud mobile peut aussi envoyer une mise à jour de lien à l'envoyeur original du paquet comme décrit au paragraphe 11.7.2 et sous réserve de la limitation de débit définie au paragraphe 11.8. Le nœud mobile DOIT aussi traiter le paquet reçu de la manière définie pour l'encapsulation IPv6 [RFC2473], qui va résulter en le traitement normal du paquet encapsulé (interne) par les protocoles de couche supérieure au sein du nœud mobile comme si il avait été (seulement) adressé à l'adresse de rattachement du nœud mobile.

Pour les paquets reçus par la seconde méthode, les règles suivantes vont résulter en le traitement du paquet normalement par les protocoles de couche supérieure au sein du nœud mobile comme si il avait été adressé à l'adresse de rattachement du nœud mobile.

Un nœud qui reçoit un paquet adressé à lui-même (c'est-à-dire que une des adresses du nœud est dans le champ Destination IPv6) suit le prochain en-tête de la chaîne des en-têtes et les traite. Quand il rencontre un en-tête d'acheminement de type 2 durant ce traitement, il effectue les vérifications suivantes. Si une de ces vérifications échoue, le nœud DOIT éliminer le paquet en silence.

- Le champ Longueur dans l'en-tête d'acheminement est exactement 2.
- Le champ Segments restants dans l'en-tête d'acheminement est 1 sur le réseau. (Mais les mises en œuvre peuvent traiter l'en-tête d'acheminement de telle sorte que la valeur peut devenir 0 après le traitement de l'en-tête d'acheminement, mais avant que le reste du paquet soit traité.)
- Le champ Adresse de rattachement dans l'en-tête d'acheminement est une des adresses de rattachement du nœud, si le champ Segments restants était 1. Donc, en particulier, il est exigé du champ Adresse qu'il soit celui d'une adresse d'acheminement en envoi individuel.

Une fois effectuées les vérifications ci-dessus, le nœud échange le champ destination IPv6 avec le champ Adresse de rattachement dans l'en-tête d'acheminement, décrémente les segments restants de un par rapport à la valeur qu'il avait sur le réseau, et resoumet le paquet à IP pour traiter le prochain en-tête. Conceptuellement, cela suit le même modèle que dans la RFC 2460. Cependant, dans le cas de l'en-tête d'acheminement de type 2, cela peut être simplifié car il est connu que le paquet ne sera pas transmis à un nœud différent.

La définition de AH exige que l'envoyeur calcule la valeur de vérification d'intégrité AH d'un en-tête d'acheminement de la même façon qu'il apparaît chez le receveur après qu'il a traité l'en-tête. Comme les en-têtes IPsec suivent l'en-tête

d'acheminement, tout traitement IPsec va opérer sur le paquet avec l'adresse de rattachement dans le champ Destination IP et Segments restant à zéro. Donc, les calculs AH chez l'envoyeur et le receveur vont avoir une vue identique du paquet.

11.3.4 Acheminement des paquets en diffusion groupée

Un nœud mobile qui est connecté à sa liaison de rattachement fonctionne de la même façon que tout autre nœud (stationnaire). Donc, quand il est chez lui, un nœud mobile fonctionne de façon identique aux autres envoyeurs et receveurs de diffusion groupée. Donc, ce paragraphe décrit le comportement d'un nœud mobile qui n'est pas sur sa liaison de rattachement.

Afin de recevoir les paquets envoyés à un groupe de diffusion groupée, un nœud mobile doit se joindre à ce groupe de diffusion groupée. Une méthode, dans laquelle un nœud mobile PEUT se joindre au groupe, est via un routeur (local) de diffusion groupée sur la liaison étrangère visitée. Dans ce cas, le nœud mobile DOIT utiliser son adresse d'entretien et NE DOIT PAS utiliser l'option de destination Adresse de rattachement quand il envoie des paquets MLD [RFC2710].

Autrement, un nœud mobile PEUT se joindre à des groupes de diffusion groupée via un tunnel bidirectionnel à son agent de rattachement. Le nœud mobile tunnelle ses paquets de contrôle d'appartenance à un groupe de diffusion groupée (comme ceux définis dans la [RFC2710] ou dans la [RFC3810]) à son agent de rattachement, et l'agent de rattachement transmet les paquets de diffusion groupée sur le tunnel au nœud mobile. Un nœud mobile NE DOIT PAS tunneler de paquets de contrôle d'appartenance à un groupe de diffusion groupée tant que (1) le nœud mobile a un lien en place chez l'agent de rattachement, et (2) ce dernier envoie au moins un paquet de contrôle d'appartenance à un groupe de diffusion groupée via le tunnel. Une fois que cette condition est vraie, le nœud mobile DEVRAIT supposer qu'elle ne change pas tant que le lien n'arrive pas à expiration.

Un nœud mobile qui souhaite envoyer des paquets à un groupe de diffusion groupée a aussi deux options :

1. Envoyer directement sur la liaison étrangère visitée.
Pour faire cela, l'application utilise l'adresse d'entretien comme adresse de source pour le trafic en diffusion groupée, tout comme elle utiliserait une adresse stationnaire. Cela exige que l'application connaisse l'adresse d'entretien, ou utilise une API comme la spécification d'API de prises IPv6 pour la sélection d'adresse de source [RFC5014] pour demander que l'adresse d'entretien soit utilisée comme adresse de source dans les paquets transmis. Le nœud mobile NE DOIT PAS utiliser l'option de destination Adresse de rattachement dans un tel trafic.

2. Envoyer via un tunnel à son agent de rattachement.
Comme en général l'acheminement de la diffusion groupée dépend de l'adresse de source utilisée dans l'en-tête IPv6 du paquet en diffusion groupée, un nœud mobile qui tunnelle un paquet en diffusion groupée à son agent de rattachement DOIT utiliser son adresse de rattachement comme adresse IPv6 de source du paquet interne en diffusion groupée.

Noter que l'envoi direct à partir de la liaison étrangère n'est applicable que lorsque le nœud mobile est sur cette liaison étrangère. C'est parce que l'arborescence de diffusion groupée associée est spécifique de cette localisation de source et que tout changement de localisation et d'adresse de source va invalider l'arborescence spécifique de source et le contexte d'application des autres membres du groupe de diffusion groupée.

La présente spécification ne fournit pas de mécanisme pour permettre à une telle session de diffusion groupée locale de survivre à l'itinérance et de continuer sans coupure à partir d'une nouvelle adresse d'entretien sur chaque nouvelle liaison étrangère. Un tel mécanisme, développé comme extension à la présente spécification, devrait tenir compte de l'impact du déplacement rapide des nœuds mobiles sur les protocoles d'acheminement de diffusion groupée de l'Internet et leur capacité à conserver l'intégrité des arborescences spécifiques de la source de diffusion groupée.

Alors que l'utilisation du tunnelage bidirectionnel peut assurer que les arborescences de diffusion groupée sont indépendantes des mouvements des nœuds mobiles, dans certains cas un tel tunnelage peut avoir des effets contraires. La latence de types spécifiques d'applications de diffusion groupée (tels que les protocoles de découverte fondés sur la diffusion groupée) va être affectée quand le délai aller-retour entre le sous réseau étranger et l'agent de rattachement est significatif comparé à celui de la topologie à découvrir. De plus, l'arborescence de livraison à partir de l'agent de rattachement dans de telles circonstances repose sur l'encapsulation en envoi individuel de l'agent au nœud mobile. Donc, l'usage de la bande passante est inefficace comparé à la transmission native en diffusion groupée dans le système étranger de diffusion groupée.

11.3.5 Réception des messages d'erreur ICMP

Tout nœud qui ne reconnaît pas l'en-tête Mobilité va retourner un message ICMP Problème de paramètre, code 1, à l'envoyeur du paquet. Si le nœud mobile reçoit un tel message d'erreur ICMP en réponse à une procédure d'acheminement

de retour ou de mise à jour de lien, il DEVRAIT enregistrer dans sa liste de mise à jour de liens que les futures mises à jour de lien NE DEVRAIENT PAS être envoyées à cette destination. De telles entrées de liste de mise à jour de liens DEVRAIENT être supprimées après un certain temps afin de permettre de réessayer l'optimisation de chemin.

Une nouvelle entrée de liste de mise à jour de liens NE DOIT PAS être créée par suite de la réception d'un message d'erreur ICMP.

Les nœuds correspondants qui ont participé à la procédure d'acheminement de retour DOIVENT mettre en œuvre la capacité de traiter correctement les paquets reçus qui contiennent une option de destination Adresse de rattachement. Donc, les nœuds correspondants mis en œuvre correctement devraient toujours être capables de reconnaître les options Adresse de rattachement. Si un nœud mobile reçoit un message ICMP Problème de paramètre, code 2, pour un nœud qui indique qu'il ne prend pas en charge l'option Adresse de rattachement, le nœud mobile DEVRAIT enregistrer l'erreur et ensuite éliminer le message ICMP.

11.3.6 Réception des messages d'erreur de lien

Quand un nœud mobile reçoit un paquet contenant un message Erreur de lien, il devrait d'abord vérifier si le nœud mobile a une entrée de liste de mises à jour de lien pour la source du message Erreur de lien. Si le nœud mobile n'a pas une telle entrée, il DOIT ignorer le message. Ceci est nécessaire pour empêcher un gaspillage des ressources, par exemple, sur une procédure d'acheminement de retour due à des messages d'erreur de lien falsifiés.

Autrement, si le champ État du message était 1 (lien inconnu pour l'option de destination Adresse de rattachement) le nœud mobile devrait effectuer une des trois actions suivantes

- Si le message Erreur de lien a été envoyé par l'agent de rattachement, le nœud mobile DEVRAIT envoyer une mise à jour de lien à l'agent de rattachement conformément au paragraphe 11.7.1.
- Si le nœud mobile a des informations récentes des progrès à la couche supérieure, qui indiquent que les communications avec le nœud correspondant progressent, il PEUT ignorer le message. Ceci peut être fait afin de limiter les dommages que des messages Erreur de lien falsifiés peuvent causer aux communications en cours.
- Si le nœud mobile n'a pas d'information des progrès à la couche supérieure, il DOIT supprimer l'entrée et acheminer la suite de la communication à travers l'agent de rattachement. Il PEUT aussi commencer une procédure d'acheminement de retour (voir au paragraphe 5.2).

Si le champ État de message était 2 (valeur non reconnue de type de MH) le nœud mobile devrait effectuer une des deux actions suivantes :

- Si le nœud mobile n'attend pas d'accusé de réception ou de réponse du nœud correspondant, le nœud mobile DEVRAIT ignorer ce message.
- Autrement, le nœud mobile DEVRAIT cesser d'utiliser toutes les extensions à la présente spécification. Si aucune extension n'a été utilisée, le nœud mobile devrait cesser de tenter d'utiliser l'optimisation de chemin.

11.4 Gestion de l'agent et du préfixe de rattachement

11.4.1 Découverte dynamique de l'adresse d'agent de rattachement

Parfois, quand le nœud mobile a besoin d'envoyer une mise à jour de lien à son agent de rattachement pour enregistrer sa nouvelle adresse d'entretien principale, comme décrit au paragraphe 11.7.1, le nœud mobile peut ne pas connaître l'adresse d'un routeur sur sa liaison de rattachement qui puisse lui servir d'agent de rattachement. Par exemple, certains nœuds sur sa liaison de rattachement peuvent avoir été reconfigurés pendant que le nœud mobile était hors de chez lui, de telle sorte que le routeur qui fonctionnait comme agent de rattachement du nœud mobile a été remplacé par un routeur différent pour assurer ce rôle.

Dans ce cas, le nœud mobile PEUT tenter de découvrir l'adresse d'un agent de rattachement convenable sur sa liaison de rattachement. Pour ce faire, le nœud mobile envoie un message ICMP Demande de découverte d'adresse d'agent de rattachement à l'adresse d'envoi à la cantonade Agents de rattachement IPv6 mobile [RFC2526] pour son préfixe de sous réseau de rattachement. Comme décrit au paragraphe 10.5, l'agent de rattachement sur sa liaison de rattachement qui reçoit ce message de demande va retourner un message ICMP de réponse de découverte d'adresse d'agent de rattachement. Ce message donne les adresses des agents de rattachement fonctionnant sur la liaison de rattachement.

À réception de ce message de réponse de découverte d'adresse d'agent de rattachement, le nœud mobile PEUT alors envoyer sa mise à jour de lien d'enregistrement de rattachement à toutes les adresses IP d'envoi individuel mentionnées dans le champ Adresses d'agent de rattachement de la réponse. Par exemple, le nœud mobile PEUT tenter son enregistrement de rattachement sur chacune de ces adresses, tout à tour, jusqu'à ce que son enregistrement soit accepté. Le nœud mobile envoie une mise à jour de lien à une adresse et attend l'accusé de réception de lien correspondant, passant à la

prochaine adresse si il n'y a pas de réponse. Le nœud mobile DOIT, cependant, attendre au moins InitialBindackTimeoutFirstReg secondes (voir à la Section 13) avant d'envoyer une mise à jour de lien à l'agent de rattachement suivant. En essayant chacune des adresses d'agent de rattachement retournées, le nœud mobile DEVRAIT essayer chacune d'elles dans l'ordre où elles apparaissent dans le champ Adresses d'agent de rattachement dans le message de réponse de découverte d'adresse d'agent de rattachement reçu. Pour ce faire, le nœud mobile DEVRAIT mémoriser la liste des agents de rattachement pour une utilisation ultérieure au cas où l'agent de rattachement qui gère actuellement la transmission à l'adresse d'entretien du nœud mobile deviendrait indisponible. La liste PEUT être mémorisée, ainsi que toutes les informations de durée de vie disponibles pour les adresses d'agent de rattachement, dans une mémoire non volatile pour survivre aux réamorçages par le nœud mobile.

Si le nœud mobile a un enregistrement actuel auprès d'un agent de rattachement (la durée de vie pour cet enregistrement n'a pas encore expiré) le nœud mobile DOIT alors tenter tout nouvel enregistrement d'abord auprès de cet agent de rattachement. Si cette tentative d'enregistrement échoue (par exemple, fin de temporisation ou rejet) le nœud mobile DEVRAIT alors tenter à nouveau cet enregistrement auprès d'un autre agent de rattachement. Si le nœud mobile ne connaît pas d'autre agent de rattachement convenable, il PEUT alors tenter la découverte dynamique d'adresse d'agent de rattachement décrite précédemment.

Si, après qu'un nœud mobile a transmis un message Demande de découverte d'adresse d'agent de rattachement à l'adresse d'envoi à la cantonade des agents de rattachement, il ne reçoit pas de message de réponse de découverte d'adresse d'agent de rattachement correspondant dans les INITIAL_DHAAD_TIMEOUT (voir à la Section 12) secondes, le nœud mobile PEUT retransmettre le même message de demande à la même adresse d'envoi à la cantonade. Cette retransmission PEUT être répétée jusqu'au maximum de DHAAD_RETRIES (voir la Section 12) tentatives. Chaque retransmission DOIT être retardée de deux fois l'intervalle de temps de la retransmission précédente.

11.4.2 Envoi de sollicitations de préfixe mobile

Quand un nœud mobile a une adresse de rattachement qui est sur le point de devenir invalide, il DEVRAIT envoyer une sollicitation de préfixe mobile à son agent de rattachement pour tenter d'acquérir des informations de préfixe d'acheminement fraîches. Les nouvelles informations permettent aussi au nœud mobile de participer à des opérations de renumérotation affectant le réseau de rattachement, comme décrit au paragraphe 10.6.

Le nœud mobile DOIT utiliser l'option de destination Adresse de rattachement pour porter son adresse de rattachement. Le nœud mobile DOIT prendre en charge et DEVRAIT utiliser IPsec pour protéger la sollicitation. Le nœud mobile DOIT régler le champ Identifiant dans l'en-tête ICMP à une valeur aléatoire.

Comme décrit au paragraphe 11.7.2, les mises à jour de lien envoyées par le nœud mobile aux autres nœuds DOIVENT utiliser une durée de vie qui ne soit pas supérieure à la durée de vie restante de son enregistrement de rattachement de son adresse d'entretien principale. Le nœud mobile DEVRAIT encore limiter les durées de vie qu'il envoie sur toute mise à jour de lien à être dans la durée de vie valide restante (voir au paragraphe 10.6.2) pour le préfixe dans son adresse de rattachement.

Quand la durée de vie diminue pour un préfixe changé, et que le changement cause la mémorisation des liens en antémémoire aux nœuds correspondants dans la liste des mises à jour de lien après la durée de vie qui vient d'être raccourcie, le nœud mobile DOIT produire une mise à jour de lien à tous ces nœuds correspondants.

Ces limites sur la durée de vie de lien servent à interdire l'utilisation d'une adresse de rattachement du nœud mobile après qu'elle est devenue invalide.

11.4.3 Réception d'annonces de préfixe mobile

Le paragraphe 10.6 décrit le fonctionnement d'un agent de rattachement pour la prise en charge de la configuration au moment de l'amorçage et le changement de numéro du sous réseau de rattachement d'un nœud mobile lorsque il est hors de chez lui. L'agent de rattachement envoie des annonces de préfixe mobile au nœud mobile lorsque il est hors de chez lui, donnant les options Informations de préfixe "importantes" qui décrivent les changements des préfixes utilisés sur la liaison de rattachement du nœud mobile.

La sollicitation de préfixe mobile est similaire à la sollicitation de routeur utilisée dans la découverte de voisin [RFC4861], excepté qu'elle est acheminée à partir du nœud mobile sur le réseau visité à l'agent de rattachement sur le réseau de rattachement par les règles usuelles d'acheminement en envoi individuel.

Quand un nœud mobile reçoit une annonce de préfixe mobile, il DOIT la valider conformément à l'essai suivant :

- o L'adresse de source du paquet IP qui porte l'annonce de préfixe mobile est la même que l'adresse de l'agent de rattachement auquel le nœud mobile a envoyé la dernière mise à jour de lien d'enregistrement de rattachement acceptée pour enregistrer son adresse d'entretien principale. Autrement, si il n'a pas été fait un tel enregistrement, ce DEVRAIT être l'adresse mémorisée d'agent de rattachement du nœud mobile, si il en existe une. Autrement, si le nœud mobile n'a pas encore découvert l'adresse de son agent de rattachement, il NE DOIT PAS accepter les annonces de préfixe mobile.
- o Le paquet DOIT avoir un en-tête d'acheminement de type 2 et DEVRAIT être protégé par un en-tête IPsec comme décrit aux paragraphes 5.4 et 6.8.
- o Si la valeur d'identifiant ICMP correspond à la valeur d'identifiant ICMP de la sollicitation de préfixe mobile la plus récemment envoyée et qu'aucune autre annonce n'a encore été reçue pour cette valeur, l'annonce va alors être considérée comme sollicitée et va être traitée en conséquence.

Autrement, l'annonce est non sollicitée, et DOIT être éliminée. Dans ce cas, le nœud mobile DEVRAIT envoyer une sollicitation de préfixe mobile.

Toute annonce de préfixe mobile reçue qui échoue à ces vérifications DOIT être éliminée en silence.

Pour une annonce de préfixe mobile acceptée, le nœud mobile DOIT traiter les options M (configuration d'adresse gérée) O (autre configuration à états pleins), et Informations de préfixe comme si elles étaient arrivées dans une annonce de routeur [RFC4861] sur la liaison de rattachement du nœud mobile. (La présente spécification ne décrit cependant pas comment acquérir les adresses de rattachement par des protocoles à états pleins.) Un tel traitement peut résulter en la configuration par le nœud mobile d'une nouvelle adresse de rattachement, bien que, à cause de la séparation entre durée de vie préférée et durée de vie valide, de tels changements ne devraient pas affecter la plupart des communications du nœud mobile, de la même façon que pour les nœuds qui sont chez eux.

La présente spécification suppose que toutes les associations de sécurité et les entrées de politique de sécurité qui peuvent être nécessaires pour les nouveaux préfixes, ont été pré configurées dans le nœud mobile. Noter qu'alors que la gestion dynamique de clés évite le besoin de configurer de nouvelles associations de sécurité, il est toujours nécessaire d'ajouter des entrées de politique pour protéger les communications qui impliquent des adresses de rattachement. Les mécanismes pour établir ces entrées sortent du domaine d'application de la présente spécification.

11.5 Mouvement

11.5.1 Détection de mouvement

Le but principal de la détection de mouvement est de détecter les transferts inter cellulaires de couche 3. Ce paragraphe ne cherche pas à spécifier un algorithme rapide de détection de mouvement qui fonctionnerait de façon optimale pour tous les types d'applications, couches de liaison, et scénarios de déploiement ; il décrit plutôt une méthode générique qui utilise les facilités de la découverte de voisin IPv6, incluant la découverte de routeur et la détection de voisin injoignable. Au moment de la rédaction de ce document, cette méthode est considérée comme assez bien comprise pour la recommander pour la normalisation ; cependant, on s'attend à ce que les futures versions de cette spécification ou d'autres spécifications puissent contenir des versions mises à jour de l'algorithme de détection de mouvement avec de meilleures performances.

La détection de mouvement générique utilise la détection de voisin injoignable pour détecter quand le routeur par défaut n'est plus accessible en bidirectionnel, auquel cas le nœud mobile doit découvrir un nouveau routeur par défaut (généralement sur une nouvelle liaison). Cependant, cette détection ne se produit que quand le nœud mobile a des paquets à envoyer, et en l'absence de fréquentes annonces de routeur ou d'indications provenant de la couche de liaison, le nœud mobile peut ignorer qu'un transfert inter-cellulaire de couche 3 s'est produit. Donc, le nœud mobile devrait compléter cette méthode avec d'autres informations chaque fois qu'elles sont à la disposition du nœud mobile (par exemple, provenant de couches de protocole inférieures).

Quand le nœud mobile détecte un transfert inter-cellulaire de couche 3, il effectue une détection d'adresse dupliquée [RFC4862] sur son adresse de liaison locale, choisit un nouveau routeur par défaut par suite de la découverte de routeur, et effectue ensuite la découverte de préfixe avec ce nouveau routeur pour former une ou des nouvelles adresses d'entretien, comme décrit au paragraphe 11.5.3. Il enregistre alors sa nouvelle adresse d'entretien principale auprès de son agent de rattachement comme décrit au paragraphe 11.7.1. Après la mise à jour de son enregistrement de rattachement, le nœud mobile met alors à jour les liens de mobilité associés dans les nœuds correspondants avec qui il effectue l'optimisation de chemin comme spécifié au paragraphe 11.7.2.

Du fait de l'interruption temporaire du flux de paquets et des surcharges de signalisation impliquées par la mise à jour des liens de mobilité, le nœud mobile devrait éviter d'effectuer un transfert inter cellulaire de couche 3 quand ce n'est pas strictement nécessaire.

Précisément, quand le nœud mobile reçoit de la part d'un nouveau routeur une annonce de routeur qui contient un ensemble différent de préfixes en liaison, si le nœud mobile détecte que le routeur par défaut actuellement choisi sur la vieille liaison est toujours accessible bidirectionnellement, il devrait généralement continuer d'utiliser le vieux routeur sur la vieille liaison plutôt que de s'en déconnecter pour utiliser un nouveau routeur par défaut.

Les nœuds mobiles peuvent utiliser les informations reçues des annonces de routeur pour détecter les transferts inter cellulaires de couche 3. Ce faisant, le nœud mobile doit prendre en considération les questions suivantes :

- Il peut y avoir plusieurs routeurs sur la même liaison. Donc, entendre un nouveau routeur ne constitue pas nécessairement un transfert inter cellulaire de couche 3.
- Quand il y a plusieurs routeurs sur la même liaison, ils peuvent annoncer des préfixes différents. Donc, entendre un nouveau routeur avec un nouveau préfixe peut n'être pas une indication fiable d'un transfert inter cellulaire de couche 3.
- Les adresses de liaison locale des routeurs ne sont pas uniques au monde, donc après avoir réalisé un transfert inter cellulaire de couche 3, le nœud mobile peut continuer de recevoir des annonces de routeur avec la même adresse de source de liaison locale. Ce peut être courant si les routeurs utilisent la même adresse de liaison locale sur plusieurs interfaces. Ce problème peut être évité quand les routeurs utilisent le bit R (Adresse de routeur) car cela donne une adresse mondiale du routeur. De plus, le nœud mobile devrait considérer les événements suivants comme l'indication qu'un transfert inter cellulaire de couche 3 peut s'être produit. À réception d'une telle indication, le nœud mobile doit effectuer une découverte de routeur pour découvrir les routeurs et les préfixes sur la nouvelle liaison, comme décrit au paragraphe 6.3.7 de la découverte de voisin [RFC4861].
- Si les annonces de routeur que le nœud mobile reçoit incluent une option Intervalle d'annonces, le nœud mobile peut utiliser son champ Intervalle d'annonces comme l'indication de la fréquence à laquelle il devrait s'attendre à continuer de recevoir les futures annonces de ce routeur. Ce champ spécifie le taux minimum (la durée maximum entre les annonces successives) que le nœud mobile devrait attendre. Si ce délai s'écoule sans que le nœud mobile reçoive aucune annonce de ce routeur, il peut être sûr qu'au moins une annonce envoyée par le routeur a été perdue. Le nœud mobile peut alors mettre en œuvre sa propre politique pour déterminer combien d'annonces perdues de son routeur par défaut actuel constituent une indication de transfert inter cellulaire.
- La détection de voisin injoignable détermine que le routeur par défaut n'est plus accessible.
- Sur certains types de réseaux, la notification qu'un transfert inter cellulaire de couche 2 s'est produit peut être obtenue des protocoles de couche inférieure ou du logiciel de pilote d'appareil au sein du nœud mobile. Bien que les détails du traitement des indications de couche 2 comme indications de mouvement soient un sujet d'études futures, au moment de la rédaction de la présente spécification, ce qui suit est considéré comme raisonnable : une indication de transfert inter cellulaire de couche 2 peut ou non impliquer un mouvement de couche 2 et un mouvement de couche 2 peut ou non impliquer un mouvement de couche 3 ; les corrélations peuvent être fonction du type de L2 mais aussi être une fonction du déploiement réel de la topologie sans fil.

Sauf si il est bien connu qu'une indication de transfert inter cellulaire de couche 2 implique probablement un mouvement de couche 3, au lieu d'envoyer immédiatement une sollicitation de routeur en diffusion groupée, il peut être meilleur de tenter de vérifier si le routeur par défaut est toujours accessible en bidirectionnel. Ceci peut être accompli par l'envoi d'une sollicitation de voisin en envoi individuel et d'attendre une annonce de voisin avec le fanion Sollicité établi. Noter que ceci est similaire à la détection d'inaccessibilité de voisin, mais cela n'a pas le même automate à états, comme l'état PÉRIMÉ.

Si le routeur par défaut ne répond pas à la sollicitation de voisin, il paraît raisonnable de procéder à la diffusion groupée d'une sollicitation de routeur.

11.5.2 Détection de liaison de rattachement

Quand un MN détecte qu'il est arrivé sur une nouvelle liaison en utilisant l'algorithme de détection de mouvement (paragraphe 11.5.1) ou à l'amorçage, il effectue les étapes suivantes pour déterminer si il est sur la liaison de rattachement.

- Le MN effectue la procédure décrite au paragraphe 11.5.3 et configure une adresse. Il garde aussi trace de tous les préfixes en liaison reçus dans la RA avec leurs longueurs de préfixe.
- Si le préfixe de rattachement n'a pas encore été configuré statiquement, le MN utilise une forme de procédure d'amorçage (par exemple, de la [RFC5026] pour déterminer le préfixe de rattachement.
- Le préfixe de rattachement étant disponible, le MN vérifie si il correspond ou non à un des préfixes reçus dans la RA. Si il correspond, le MN en conclut qu'il est connecté à la liaison de rattachement.

11.5.3 Formation de nouvelles adresses d'entretien

Après avoir détecté qu'il bougé, un nœud mobile DEVRAIT générer une nouvelle adresse d'entretien principale en utilisant les mécanismes IPv6 normaux. Ceci DEVRAIT aussi être fait quand l'adresse d'entretien principale actuelle devient déconseillée. Un nœud mobile PEUT former une nouvelle adresse d'entretien principale à tout moment, mais un nœud mobile NE DOIT PAS envoyer une mise à jour de lien sur une nouvelle adresse d'entretien à son agent de rattachement plus de MAX_UPDATE_RATE fois par seconde.

De plus, un nœud mobile PEUT former une nouvelle adresse d'entretien non principale même quand il n'est pas passé sur un nouveau routeur par défaut. Un nœud mobile peut avoir seulement une adresse d'entretien principale à la fois (qui est enregistrée auprès de son agent de rattachement) mais il PEUT avoir une adresse d'entretien supplémentaire pour un ou tous les préfixes sur sa liaison actuelle. De plus, comme une interface de réseau sans fil peut en fait permettre à un nœud mobile d'être accessible sur plus d'une liaison à la fois (c'est-à-dire, au sein d'une gamme de routeurs transmetteurs sans fil sur plus d'une liaison séparée) un nœud mobile PEUT avoir des adresses d'entretien sur plus d'une liaison à la fois. L'utilisation de plus d'une adresse d'entretien à la fois est décrite au paragraphe 11.5.4.

Comme décrit à la Section 4, afin de former une nouvelle adresse d'entretien, un nœud mobile PEUT utiliser l'autoconfiguration d'adresse sans état [RFC4862] ou à états pleins (par exemple, DHCPv6 [RFC3315]). Si un nœud mobile a besoin d'utiliser une adresse de source (autre que l'adresse inspécifiée) dans les paquets envoyés au titre de l'autoconfiguration d'adresse, il DOIT utiliser une adresse IPv6 de liaison locale plutôt que sa propre adresse de rattachement IPv6.

La [RFC4862] spécifie que dans le traitement normal de détection d'adresse dupliquée, le nœud DEVRAIT retarder l'envoi du message initial de sollicitation de voisin d'un délai aléatoire entre 0 et MAX_RTR_SOLICITATION_DELAY. Comme le retard de la détection d'adresse dupliquée (DAD) peut résulter en délais significatifs de la configuration d'une nouvelle adresse d'entretien quand le nœud mobile se déplace sur une nouvelle liaison, le nœud mobile NE DEVRAIT de préférence PAS retarder la DAD quand il configure une nouvelle adresse d'entretien. Le nœud mobile DEVRAIT la retarder conformément aux mécanismes spécifiés dans la RFC 4862 sauf si la mise en œuvre a un comportement qui désynchronise les étapes qui précèdent la DAD dans le cas où plusieurs nœuds effectuent un transfert inter-cellulaire au même moment. De tels comportements de désynchronisation peuvent être dus à des retards aléatoire dans les protocoles de couche 2 ou des pilotes d'appareils, ou dus au mécanisme de détection de mouvement qui est utilisé.

11.5.4 Utilisation de plusieurs adresses d'entretien

Comme décrit au paragraphe 11.5.3, un nœud mobile PEUT utiliser plus d'une adresse d'entretien à la fois. En particulier dans le cas de nombreux réseaux sans fil, un nœud mobile peut effectivement être accessible par de multiples liaisons en même temps (par exemple, avec des cellules qui se chevauchent) sur lesquelles différents préfixes de sous réseaux en liaison peuvent exister. Le nœud mobile DOIT s'assurer que son adresse d'entretien principale a toujours un préfixe qui est annoncé par son routeur par défaut actuel. Après le choix d'une nouvelle adresse d'entretien principale, le nœud mobile DOIT envoyer une mise à jour de lien contenant cette adresse d'entretien à son agent de rattachement. La mise à jour de lien envoyée à son agent de rattachement DOIT avoir le bit H (enregistrement de rattachement) et le bit A (accusé de réception) établis, comme décrit au paragraphe 11.7.1.

Pour faciliter des transferts inter cellulaires en douceur, un nœud mobile DEVRAIT conserver son adresse d'entretien principale antérieure comme adresse d'entretien (non principale) et DEVRAIT encore accepter les paquets à cette adresse, même après avoir enregistré sa nouvelle adresse d'entretien principale auprès de son agent de rattachement. Ceci est raisonnable, car le nœud mobile pourrait seulement recevoir des paquets à son adresse d'entretien principale antérieure si il était bien encore connecté à cette liaison. Si l'adresse d'entretien principale antérieure était allouée en utilisant l'autoconfiguration d'adresse à états pleins [RFC3315], le nœud mobile pourrait ne pas souhaiter libérer l'adresse immédiatement après être passé à une nouvelle adresse d'entretien principale.

Chaque fois qu'un nœud mobile détermine qu'il n'est plus accessible par une certaine liaison, il DEVRAIT invalider toutes les adresses d'entretien associées aux préfixes d'adresse qu'il a découvert en provenance de routeurs sur la liaison injoignable qui ne sont pas dans l'ensemble courant de préfixes d'adresses annoncés par le routeur par défaut actuel (éventuellement nouveau).

11.5.5 Retour au réseau de rattachement

Un nœud mobile détecte qu'il est retourné à sa liaison de rattachement par l'algorithme de détection de mouvement utilisé (paragraphe 11.5.2) quand le nœud mobile détecte que son préfixe de sous réseau de rattachement est de nouveau en liaison. Pour être capable d'envoyer et recevoir des paquets en utilisant son adresse de rattachement à partir de la liaison de rattachement, le nœud mobile DOIT envoyer une mise à jour de lien à son agent de rattachement pour lui donner pour instruction de ne plus intercepter ou tunneler les paquets pour lui. Jusqu'à ce que le nœud mobile envoie une telle mise à jour de désenregistrement de lien, il NE DOIT PAS tenter d'envoyer et recevoir des paquets en utilisant son adresse de rattachement à partir de la liaison de rattachement. L'agent de rattachement va continuer d'intercepter tous les paquets envoyés à l'adresse de rattachement du mobile et les tunneler à l'adresse d'entretien précédemment enregistrée.

Dans cet enregistrement de rattachement, le nœud mobile DOIT établir les bits A (accusé de réception) et H (enregistrement de rattachement) régler le champ Durée de vie à zéro, et régler l'adresse d'entretien pour le lien à la propre

adresse de rattachement du nœud mobile. Le nœud mobile DOIT utiliser son adresse de rattachement comme adresse de source dans la mise à jour de lien.

Quand il envoie cette mise à jour de lien à son agent de rattachement, le nœud mobile doit être prudent en utilisant la sollicitation de voisin [RFC4861] (si nécessaire) pour apprendre l'adresse de couche de liaison de l'agent de rattachement, car l'agent de rattachement va être actuellement configuré à intercepter les paquets pour l'adresse de rattachement du nœud mobile qui utilisent un mandataire de découverte de voisin (Proxy ND). En particulier, le nœud mobile est incapable d'utiliser son adresse de rattachement comme adresse de source dans la sollicitation de voisin jusqu'à ce que l'agent de rattachement cesse de défendre l'adresse de rattachement.

La sollicitation de voisin par le nœud mobile pour l'adresse de l'agent de rattachement va normalement n'être pas nécessaire, car le nœud mobile a déjà appris l'adresse de couche liaison de l'agent de rattachement d'une option Adresse de source de couche de liaison dans une annonce de routeur. Cependant, si il y a plusieurs agents de rattachement, il peut encore être nécessaire d'envoyer une sollicitation. Dans le cas particulier du nœud mobile qui retourne chez lui, le nœud mobile DOIT envoyer le paquet en diffusion groupée, et de plus régler l'adresse de source de cette sollicitation de voisin à l'adresse inspécifiée (0:0:0:0:0:0:0:0). La cible de la sollicitation de voisin DOIT être réglée à l'adresse de rattachement du nœud mobile. L'adresse IP de destination DOIT être réglée à l'adresse de diffusion groupée Nœud sollicité [RFC4291].
L'agent de rattachement va renvoyer en diffusion groupée une annonce de voisin au nœud mobile avec le fanion S (Sollicité) réglé à zéro. Dans tous les cas, le nœud mobile DEVRAIT enregistrer les informations provenant de l'option Adresse de source de couche liaison ou de l'annonce, et régler l'état de l'entrée d'antémémoire de voisin pour l'agent de rattachement à ACCESSIBLE.

Le nœud mobile envoie alors sa mise à jour de lien à l'adresse de couche de liaison de l'agent de rattachement, lui donnant pour instruction de ne plus lui servir d'agent de rattachement. En traitant cette mise à jour de lien, l'agent de rattachement va cesser de défendre l'adresse de rattachement du nœud mobile pour la détection d'adresse dupliquée et ne plus répondre aux sollicitations de voisin pour l'adresse de rattachement du nœud mobile. Le nœud mobile est alors le seul nœud sur la liaison qui reçoit des paquets à l'adresse de rattachement du nœud mobile. De plus, quand il revient chez lui avant l'expiration d'un lien actuel pour son adresse de rattachement, et qu'il configure son adresse de rattachement sur son interface réseau à sa liaison de rattachement, le nœud mobile NE DOIT PAS effectuer de détection d'adresse dupliquée sur sa propre adresse de rattachement, afin d'éviter la confusion ou un conflit avec l'utilisation de la même adresse par son agent de rattachement. Cette règle s'applique aussi à l'adresse de liaison locale déduite du nœud mobile, si le bit L (compatibilité d'adresse de liaison locale) a été établi à la création du lien. Si le nœud mobile retourne chez lui après l'expiration de ses liens pour toutes ses adresses d'entretien, il DEVRAIT alors effectuer une DAD.

Après que le nœud mobile a envoyé la mise à jour de lien, il DOIT être prêt à répondre aux sollicitations de voisin pour son adresse de rattachement. De telles réponses DOIVENT être envoyées en utilisant une annonce de voisin en envoi individuel à l'adresse de couche de liaison de l'envoyeur. Il est nécessaire de répondre, car l'envoi de l'accusé de réception de lien provenant de l'agent de rattachement peut exiger d'effectuer une découverte de voisin, et le nœud mobile peut n'être pas capable de distinguer les sollicitations de voisin venant de l'agent de rattachement des autres sollicitations de voisin. Noter qu'une condition de compétition existe lorsque le nœud mobile et l'agent de rattachement répondent aux mêmes sollicitations envoyées par d'autres nœuds ; ceci va cependant être seulement temporaire, jusqu'à ce que la mise à jour de lien soit acceptée.

Après avoir reçu l'accusé de réception de lien de sa mise à jour de lien de son agent de rattachement, le nœud mobile DOIT envoyer en diffusion groupée sur la liaison de rattachement (à l'adresse de diffusion groupée Tous-les-nœuds) une annonce de voisin [RFC4861], pour annoncer la propre adresse de couche de liaison du nœud mobile pour sa propre adresse de rattachement. L'adresse cible dans cette annonce de voisin DOIT être réglée à l'adresse de rattachement du nœud mobile, et l'annonce DOIT inclure une option Adresse de couche liaison cible spécifiant l'adresse de couche liaison du nœud mobile. Le nœud mobile DOIT envoyer une telle annonce de voisin en diffusion groupée pour chacune de ses adresses de rattachement, comme définies par les préfixes en liaison actuels, incluant son adresse de liaison locale. Le fanion S (sollicité) dans ces annonces NE DOIT PAS être établi, car elles n'ont pas été sollicitées par une sollicitation de voisin. Le fanion O (outrepasser) dans ces annonces DOIT être établi, indiquant que les annonces DEVRAIENT outrepasser toutes les entrées existantes d'antémémoire de voisins chez tout nœud qui les reçoit.

Comme la diffusion groupée sur la liaison locale (comme un Ethernet) n'est normalement pas d'une fiabilité garantie, le nœud mobile PEUT retransmettre ces annonces de voisin [RFC4861] jusqu'à MAX_NEIGHBOR_ADVERTISEMENT fois pour augmenter leur fiabilité. Il est toujours possible que certains nœuds sur la liaison de rattachement ne reçoivent aucune de ces annonces de voisin, mais ces nœuds seront finalement capables de les récupérer par l'utilisation de la détection de voisin injoignable [RFC4861].

Noter que le tunnel via l'agent de rattachement s'arrête normalement de fonctionner au moment même où l'enregistrement de rattachement est supprimé.

11.6 Procédure d'acheminement de retour

Ce paragraphe définit les règles que le nœud mobile doit suivre quand il effectue la procédure d'acheminement de retour. Le paragraphe 11.7.2 décrit les règles quand la procédure d'acheminement de retour doit être initiée.

11.6.1 Envoi des messages Initiation d'essai

Un nœud mobile qui initie une procédure d'acheminement de retour DOIT envoyer (en parallèle) un message Initiation d'essai de rattachement et un message Initiation d'essai d'entretien. Cependant, si le nœud mobile a reçu récemment (voir au paragraphe 5.2.7) un jeton de génération de clé de rattachement ou d'entretien ou les deux, et les indices de nom occasionnel associés pour les adresses désirées, il PEUT les réutiliser. Donc, la procédure d'acheminement de retour peut dans certains cas être achevée avec une seule paire de messages. Elle peut même être achevée sans aucun messages du tout, si le nœud mobile a un jeton de génération de clé de rattachement récent et a précédemment visité la même adresse d'entretien de sorte qu'il a aussi un jeton de génération de clé d'entretien récent. Si le nœud mobile entend envoyer une mise à jour de lien avec la durée de vie réglée à zéro et l'adresse d'entretien égale à son adresse de rattachement -- comme quand il retourne chez lui -- envoyer un message Initiation d'essai de rattachement est suffisant. Dans ce cas, la génération de la clé de gestion de lien dépend exclusivement du jeton de génération de clé de rattachement (paragraphe 5.2.5).

Un message Initiation d'essai de rattachement DOIT être créé comme décrit au paragraphe 6.1.3.

Un message Initiation d'essai d'entretien DOIT être créé comme décrit au paragraphe 6.1.4. Quand il envoie un message Initiation d'essai de rattachement ou un message Initiation d'essai d'entretien, le nœud mobile DOIT enregistrer dans sa liste de mise à jour de lien les champs suivants provenant des messages :

- o L'adresse IP du nœud auquel le message a été envoyé.
- o L'adresse de rattachement du nœud mobile. Cette valeur va apparaître dans le champ Adresse de source du message Initiation d'essai de rattachement. Quand il envoie le message Initiation d'essai d'entretien, cette adresse n'apparaît pas dans le message, mais représente l'adresse de rattachement pour laquelle le lien est désiré.
- o L'heure à laquelle chacun de ces messages a été envoyé.
- o Les mouchards utilisés dans les messages.

Noter qu'un seul message Initiation d'essai d'entretien peut être suffisant même quand il y a plusieurs adresses de rattachement. Dans ce cas, le nœud mobile PEUT enregistrer les mêmes informations dans plusieurs entrées de liste de mise à jour de liens.

11.6.2 Réception des messages d'essai

À réception d'un paquet portant un message Essai de rattachement, un nœud mobile DOIT valider le paquet conformément aux essais suivants :

- o L'adresse de source du paquet appartient à un nœud correspondant pour lequel le nœud mobile a une entrée de liste de mise à jour de lien avec un état indiquant qu'une procédure d'acheminement de retour est en cours. Noter qu'il peut y avoir plusieurs de ces entrées.
- o La liste de mises à jour de lien indique qu'aucun jeton de génération de clé de rattachement n'a encore été reçu.
- o L'adresse de destination du paquet a l'adresse de rattachement du nœud mobile, et le paquet a été reçu dans un tunnel provenant de l'agent de rattachement.
- o Le champ Mouchard d'initiation de rattachement dans le message correspond à la valeur mémorisée dans la liste de mise à jour de lien.

Tout message d'essai de rattachement qui ne satisfait pas à tous ces essais DOIT être ignoré en silence. Autrement, le nœud mobile DOIT enregistrer l'indice de nom occasionnel de rattachement et le jeton de génération de clé de rattachement dans la liste de mises à jour de lien. Si l'entrée de liste de mises à jour de lien n'a pas de jeton de génération de clé d'entretien, le nœud mobile DEVRAIT continuer d'attendre le message Essai d'entretien.

À réception d'un paquet portant un message Essai d'entretien, un nœud mobile DOIT valider le paquet conformément aux essais suivants :

- o L'adresse de source du paquet appartient à un nœud correspondant pour lequel le nœud mobile a une entrée de liste de mises à jour de lien avec un état indiquant que la procédure d'acheminement de retour est en cours. Noter qu'il peut y avoir plusieurs de ces entrées.
- o La liste de mises à jour de lien indique qu'aucun jeton de génération de clé d'entretien n'a encore été reçu.
- o L'adresse de destination du paquet est l'adresse d'entretien courante du nœud mobile.
- o Le champ Mouchard d'initiation d'entretien dans le message correspond à la valeur mémorisée dans la liste de mises à jour de lien.

Tout message d'essai d'entretien qui ne satisfait pas à tous ces essais DOIT être ignoré en silence. Autrement, le nœud mobile DOIT enregistrer l'indice de nom occasionnel d'entretien et le jeton de génération de clé d'entretien dans la liste de mises à jour de lien. Si l'entrée de liste de mises à jour de lien n'a pas de jeton de génération de clé de rattachement, le nœud mobile DEVRAIT continuer d'attendre le message Essai d'entretien.

Si après avoir reçu le message Essai d'entretien ou Essai de rattachement et effectué les actions ci-dessus, l'entrée de liste de mises à jour de lien a les deux jetons de génération de clé de rattachement et d'entretien, la procédure d'acheminement de retour est achevée. Le nœud mobile DEVRAIT alors poursuivre l'envoi de sa mise à jour de lien comme décrit au paragraphe 11.7.2.

Les nœuds correspondants d'avant la publication de la présente spécification peuvent ne pas prendre en charge le protocole d'en-tête de mobilité. Ces nœuds vont répondre aux messages Initiation d'essai de rattachement et d'entretien avec un problème de paramètre ICMP de code 1. Le nœud mobile DEVRAIT prendre ces messages comme l'indication que le nœud correspondant ne peut pas fournir l'optimisation de chemin, et revenir à l'utilisation du tunnelage bidirectionnel.

11.6.3 Protection des paquets d'acheminement de retour

Le nœud mobile DOIT prendre en charge la protection des messages Essai de rattachement et Initiation d'essai de rattachement comme décrit au paragraphe 10.4.6.

Quand IPsec est utilisé pour protéger la signalisation d'acheminement de retour ou les paquets de charge utile, le nœud mobile DOIT régler l'adresse de source qu'il utilise pour les paquets tunnelés sortants à l'adresse d'entretien principale en cours. Le nœud mobile commence à utiliser une nouvelle adresse d'entretien principale immédiatement après l'envoi d'une mise à jour de lien à l'agent de rattachement pour enregistrer cette nouvelle adresse.

11.7 Traitement des liens

11.7.1 Envoi de mise à jour de lien à l'agent de rattachement

Afin de changer son adresse d'entretien principale comme décrit aux paragraphes 11.5.1 et 11.5.3, un nœud mobile DOIT enregistrer cette adresse d'entretien après de son agent de rattachement afin d'en faire son adresse d'entretien principale.

Aussi, si le nœud mobile veut les services de l'agent de rattachement au delà de la période d'enregistrement courante, le nœud mobile devrait lui envoyer une nouvelle mise à jour de lien bien avant l'expiration de cette période, même si il ne change pas son adresse d'entretien principale. Cependant, si l'agent de rattachement a retourné un accusé de réception de lien pour l'enregistrement actuel avec le champ État réglé à 1 (accepté mais découverte de préfixe nécessaire) le nœud mobile ne devrait pas essayer de s'enregistrer à nouveau avant qu'il ait appris la validité de ses préfixes de rattachement par la découverte de préfixe mobile. Ceci est normalement nécessaire chaque fois que cette valeur d'état est reçue, parce que les informations apprises antérieurement peuvent avoir changé.

Pour enregistrer une adresse d'entretien ou pour étendre la durée de vie d'un enregistrement existant, le nœud mobile envoie un paquet à son agent de rattachement contenant une mise à jour de lien, le paquet étant construit comme suit :

- Le bit H (enregistrement de rattachement) DOIT être établi dans la mise à jour de lien.
- Le bit A (accusé de réception) DOIT être établi dans la mise à jour de lien.
- Le paquet DOIT contenir une option de destination Adresse de rattachement, donnant l'adresse de rattachement du nœud mobile pour le lien.
- L'adresse d'entretien pour le lien DOIT être utilisée comme adresse de source dans l'en-tête IPv6 du paquet, sauf si une option de mobilité Adresse d'entretien de remplacement est incluse dans la mise à jour de lien. Cette option DOIT être incluse dans tous les enregistrements de rattachement, car le protocole ESP ne va pas être capable de protéger les adresses d'entretien dans l'en-tête IPv6. (Les mises en œuvre IPv6 mobile qui savent qu'elles utilisent IPsec AH pour protéger un message particulier peuvent éviter cette option. Pour faire bref, l'usage de AH n'est pas discuté dans ce document.)
- Si l'adresse de liaison locale du nœud mobile a le même identifiant d'interface que l'adresse de rattachement pour laquelle il fournit une nouvelle adresse d'entretien, alors le nœud mobile DEVRAIT établir le bit L (compatibilité d'adresse de liaison locale).
- Si l'adresse de rattachement a été générée en utilisant la [RFC4941], alors l'adresse de liaison locale a peu de chances d'avoir un identifiant d'interface compatible. Dans ce cas, le nœud mobile DOIT mettre à zéro le bit L (compatibilité d'adresse de liaison locale).
- Si les associations de sécurité IPsec entre le nœud mobile et l'agent de rattachement ont été établies dynamiquement, et si le nœud mobile a la capacité de mettre à jour son point d'extrémité dans le protocole de gestion de clés utilisé à la nouvelle adresse d'entretien chaque fois qu'il bouge, le nœud mobile DEVRAIT établir le bit K (capacité de mobilité de gestion de clé) dans la mise à jour de lien. Autrement, le nœud mobile DOIT mettre ce bit à zéro.

- La valeur spécifiée dans le champ Durée de vie DOIT être non à zéro et DEVRAIT être inférieure ou égale à la durée de vie valide restante de l'adresse de rattachement et de l'adresse d'entretien spécifiée pour le lien.

Les nœuds mobiles qui utilisent la découverte dynamique d'adresse d'agent de rattachement devraient être prudents avec les longues durées de vie. Si le nœud mobile perd la connaissance de son lien avec un agent de rattachement spécifique, l'enregistrement d'un nouveau lien avec un autre agent de rattachement peut être impossible car l'agent de rattachement précédent défend toujours le lien existant. Donc, pour s'assurer que les nœuds mobiles qui utilisent la découverte d'adresse d'agent de rattachement ne perdent pas les informations sur leur lien, ils DEVRAIENT se désenregistrer avant de perdre ces informations, ou utiliser des durées de vie courtes.

Le bit A (accusé de réception) dans la mise à jour de lien demande à l'agent de rattachement de retourner un accusé de réception de lien en réponse à cette mise à jour de lien. Comme décrit au paragraphe 6.1.8, le nœud mobile DEVRAIT retransmettre cette mise à jour de lien à son agent de rattachement jusqu'à ce qu'il reçoive un accusé de réception de lien correspondant. Une fois qu'il a atteint une période de temporisation de retransmission de MAX_BINDACK_TIMEOUT, le nœud mobile DEVRAIT redémarrer le processus de livraison de mise à jour de lien, mais en essayant plutôt le prochain agent de rattachement retourné durant la découverte dynamique d'adresse d'agent de rattachement (voir au paragraphe 11.4.1). Si il y avait seulement un agent de rattachement, le nœud mobile DEVRAIT plutôt continuer de retransmettre périodiquement la mise à jour de lien à ce rythme jusqu'à ce qu'elle soit acquittée (ou jusqu'à ce qu'il commence à tenter de s'enregistrer sur une adresse d'entretien principale différente). Voir au paragraphe 11.8 les informations sur la retransmission des mises à jour de lien.

Avec la mise à jour de lien, le nœud mobile demande à l'agent de rattachement de servir d'agent de rattachement pour l'adresse de rattachement en question. Jusqu'à l'expiration de la durée de vie de cet enregistrement, l'agent de rattachement se considère comme l'agent de rattachement pour cette adresse de rattachement.

Chaque mise à jour de lien DOIT être authentifiée comme venant du bon nœud mobile, comme défini au paragraphe 5.1. Le nœud mobile DOIT utiliser son adresse de rattachement -- soit dans l'option de destination Adresse de rattachement, soit dans le champ Adresse de source de l'en-tête IPv6 -- dans les mises à jour de lien envoyées à l'agent de rattachement. Ceci est nécessaire afin de permettre aux politiques IPsec d'être confrontées à l'adresse de rattachement correcte.

Quand il envoie une mise à jour de lien à son agent de rattachement, le nœud mobile DOIT aussi créer ou mettre à jour l'entrée de liste de mises à jour de lien correspondante, comme spécifié au paragraphe 11.7.2.

La dernière valeur de numéro de séquence envoyée à l'agent de rattachement dans une mise à jour de lien est mémorisée par le nœud mobile. Si le nœud mobile envoyeur n'a pas connaissance de la valeur correcte de numéro de séquence, il peut commencer à une valeur quelconque. Si l'agent de rattachement rejette cette valeur, il renvoie un accusé de réception de lien avec un code d'état 135, et le dernier numéro de séquence accepté dans le champ Numéro de séquence de l'accusé de réception de lien. Le nœud mobile DOIT mémoriser cette information et utiliser la prochaine valeur de numéro de séquence pour la prochaine mise à jour de lien qu'il envoie.

Si le nœud mobile a des adresses de rattachement supplémentaires, le nœud mobile DEVRAIT alors envoyer un paquet supplémentaire contenant une mise à jour de lien à son agent de rattachement pour enregistrer l'adresse d'entretien pour chacune de ces autres adresses de rattachement.

L'agent de rattachement va seulement effectuer une DAD pour l'adresse de rattachement du nœud mobile quand le nœud mobile a fourni un lien valide entre son adresse de rattachement et une adresse d'entretien. Si un certain temps s'écoule pendant lequel le nœud mobile n'a pas de lien à l'agent de rattachement, il est possible qu'un autre nœud autoconfigure l'adresse de rattachement du nœud mobile. Donc, le nœud mobile DOIT traiter la création d'un nouveau lien avec l'agent de rattachement en utilisant une adresse de rattachement existante, de la même façon que la création d'une nouvelle adresse de rattachement. Dans l'éventualité improbable où cette adresse de rattachement du nœud mobile serait autoconfigurée comme adresse IPv6 d'un autre nœud du réseau de rattachement, l'agent de rattachement va répondre à la mise à jour de lien suivante du nœud mobile par un accusé de réception de lien contenant un code d'état de 134 (échec de détection d'adresse dupliquée). Dans ce cas, le nœud mobile NE DOIT PAS tenter de réutiliser la même adresse de rattachement. Il DEVRAIT continuer d'enregistrer les adresses d'entretien pour ses autres adresses de rattachement, si il en est. Les mécanismes présentés dans la [RFC5026] "Amorçage IPv6 mobile dans un scénario de partage" permettent aux nœuds mobiles d'acquérir de nouvelles adresses de rattachement pour remplacer celles pour lesquelles un code d'état de 134 a été reçu.

11.7.2 Enregistrement de correspondant

Quand le nœud mobile est assuré que son adresse de rattachement est valide, il peut initier un enregistrement correspondant dans le but de permettre au nœud correspondant de mettre en antémémoire l'adresse d'entretien actuelle du nœud mobile. Cette procédure consiste en la procédure d'acheminement de retour suivie par un enregistrement.

Ce paragraphe définit quand l'enregistrement correspondant est à initier et les règles à suivre lorsque il est effectué.

Après l'envoi d'une mise à jour de lien par le nœud mobile à son agent de rattachement, enregistrant une nouvelle adresse d'entretien principale (comme décrit au paragraphe 11.7.1) le nœud mobile DEVRAIT initier un enregistrement correspondant pour chaque nœud qui apparaît déjà sans la liste de mises à jour de lien du nœud mobile. Les procédures initiées peuvent être utilisées pour mettre à jour ou supprimer les informations de lien dans le nœud correspondant.

Pour les nœuds qui n'apparaissent pas dans la liste de mises à jour de lien du nœud mobile, celui-ci PEUT initier un enregistrement correspondant à tout moment après l'envoi de la mise à jour de lien à son agent de rattachement. Les considérations sur quand (et si) initier la procédure dépendent des schémas spécifiques de mouvement et de trafic du nœud mobile et sortent du domaine d'application de ce document.

De plus, le nœud mobile PEUT initier l'enregistrement correspondant en réponse à la réception d'un paquet qui satisfait à tous les essais suivants :
- o Le paquet a été tunnelé en utilisant l'encapsulation IPv6.
- o L'adresse de destination dans l'en-tête IPv6 du tunnel (externe) est égale à une des adresses d'entretien du nœud mobile.
- o L'adresse de destination dans l'en-tête IPv6 (interne) du tunnel est égale à une des adresses de rattachement du nœud mobile.
- o L'adresse de source dans l'en-tête IPv6 du tunnel (externe) diffère de l'adresse de source dans l'en-tête IPv6 original (interne).
- o Le paquet ne contient pas de message Essai de rattachement, Initiation d'essai de rattachement, Essai d'entretien, ou Initiation d'essai d'entretien.

Si un nœud mobile a plusieurs adresses de rattachement, il devient important de choisir la bonne adresse de rattachement à utiliser dans l'enregistrement correspondant. L'adresse de rattachement utilisée DOIT être l'adresse de destination du paquet original (interne).

L'adresse de l'homologue utilisée dans la procédure DOIT être déterminée comme suit :
- o Si une option de destination Adresse de rattachement est présente dans le paquet original (interne) l'adresse provenant de cette option est utilisée.
- o Autrement, l'adresse de source dans l'en-tête IPv6 original (interne) du paquet est utilisée.

Noter que la validité du paquet original est vérifiée avant de tenter d'initier un enregistrement correspondant. Par exemple, si une option de destination Adresse de rattachement apparaissait dans le paquet original, alors les règles du paragraphe 9.3.1 sont suivies.

Un nœud mobile PEUT aussi choisir de garder sa localisation topologique confidentielle à l'égard de certains nœuds correspondants, et n'a donc pas besoin d'initier l'enregistrement correspondant.

À l'achèvement réussi de la procédure d'acheminement de retour, et après avoir reçu un accusé de réception de lien réussi de l'agent de rattachement, une mise à jour de lien PEUT être envoyée au nœud correspondant.

Dans toute mise à jour de lien envoyée par un nœud mobile, l'adresse d'entretien (adresse de source dans l'en-tête IPv6 du paquet ou adresse d'entretien dans l'option de mobilité Adresse d'entretien de remplacement de la mise à jour de lien) DOIT être réglée à une des adresses d'entretien actuellement utilisées par le nœud mobile ou à l'adresse de rattachement du nœud mobile. Un nœud mobile PEUT régler l'adresse d'entretien différemment pour envoyer les mises à jour de lien à différents nœuds correspondants.

Un nœud mobile PEUT aussi envoyer une mise à jour de lien à un tel nœud correspondant, lui donnant pour instruction de supprimer tout lien existant pour le nœud mobile de son antémémoire de liens, comme décrit au paragraphe 6.1.7. Même dans ce cas, un achèvement réussi de la procédure d'acheminement de retour est d'abord exigé.

Si l'adresse d'entretien n'est pas réglée à l'adresse de rattachement du nœud mobile, la mise à jour de lien demande que le nœud correspondant crée ou mette à jour toute entrée pour le nœud mobile dans l'antémémoire de liens du nœud correspondant. Ceci est fait afin d'enregistrer une adresse d'entretien à utiliser pour l'envoi de futurs paquets au nœud mobile. Dans ce cas, la valeur spécifiée dans le champ Durée de vie envoyé dans la mise à jour de lien DEVRAIT être inférieure ou égale à la durée de vie restante de l'enregistrement de rattachement et de l'adresse d'entretien spécifiée pour le lien. L'adresse d'entretien donnée dans la mise à jour de lien PEUT différer de l'adresse d'entretien principale du nœud mobile.

Si la mise à jour de lien est envoyée au nœud correspondant, demandant la suppression de toutes les entrées d'antémémoire de liens existantes pour le nœud mobile, l'adresse d'entretien est réglée à l'adresse de rattachement du nœud mobile et le

champ Durée de vie est réglé à zéro. Dans ce cas, la génération de la clé de gestion de lien dépend exclusivement du jeton de génération de clé de rattachement (paragraphe 5.2.5). L'indice de nom occasionnel d'entretien DEVRAIT être réglé à zéro dans ce cas. En respectant les règles de création de mise à jour de lien ci-dessous, l'adresse d'entretien DOIT être réglée à l'adresse de rattachement si le nœud mobile est chez lui, ou à l'adresse d'entretien actuelle si il est hors de chez lui.

Si le nœud mobile veut s'assurer que sa nouvelle adresse d'entretien a été entrée dans l'antémémoire de liens du nœud correspondant, il doit demander un accusé de réception en établissant le bit A (accusé de réception) dans la mise à jour de lien.

Une mise à jour de lien est créée comme suit :
- o L'adresse d'entretien courante du nœud mobile DOIT être envoyée dans l'adresse de source de l'en-tête IPv6 ou dans l'option de mobilité Adresse d'entretien de remplacement.
- o L'adresse de destination de l'en-tête IPv6 DOIT contenir l'adresse du nœud correspondant.
- o L'en-tête de mobilité est construit conformément aux règles des paragraphes 6.1.7 et 5.2.6, incluant les données d'autorisation de lien (calculées comme défini au paragraphe 6.2.7) et éventuellement les options de mobilité Indices de nom occasionnel.
- o L'adresse de rattachement du nœud mobile DOIT être ajoutée au paquet dans une option de destination Adresse de rattachement, sauf si l'adresse de source est l'adresse de rattachement.

Chaque mise à jour de lien DOIT avoir un numéro de séquence supérieur au numéro de séquence envoyé dans la précédente mise à jour de lien à la même adresse de destination (si il en est). Les numéros de séquence sont comparés modulo 2**16, comme décrit au paragraphe 9.5.1. Il n'est cependant pas exigé que la valeur du numéro de séquence s'augmente strictement de 1 à chaque nouvelle mise à jour de lien envoyée ou reçue, pour autant que la valeur reste dans la fenêtre. La dernière valeur de numéro de séquence envoyée à une destination dans une mise à jour de lien est mémorisée par le nœud mobile dans son entrée de liste de mises à jour de lien pour cette destination. Si le nœud mobile envoyeur n'a pas d'entrée de liste de mises à jour de lien, le numéro de séquence DEVRAIT commencer à une valeur aléatoire. Le nœud mobile NE DOIT PAS utiliser le même numéro de séquence dans deux mises à jour de lien différentes au même nœud correspondant, même si les mises à jour de lien proviennent de différentes adresses d'entretien.

Le nœud mobile est responsable de l'achèvement de l'enregistrement de correspondant, ainsi que de toute retransmission qui peut être nécessaire (sous réserve de la limitation de taux d'envoi définie au paragraphe 11.8).

11.7.3 Réception des accusés de réception de liens

À réception d'un paquet portant un accusé de réception de lien, un nœud mobile DOIT valider le paquet conformément aux essais suivants :
- o Le paquet satisfait aux exigences d'authentification pour l'accusé de réception de liens définies aux paragraphes 6.1.8 et à la Section 5. C'est-à-dire, si la mise à jour de lien a été envoyée à l'agent de rattachement, la protection IPsec sous-jacente est utilisée. Si la mise à jour de lien a été envoyée au nœud correspondant, l'option de mobilité Données d'autorisation de lien DOIT être présente et avoir une valeur valide.
- o L'option de mobilité Données d'autorisation de lien, si elle est présente, DOIT être la dernière option et NE DOIT PAS avoir de bourrage en queue.
- o Le champ Numéro de séquence correspond au numéro de séquence envoyé par le nœud mobile à cette adresse de destination dans une mise à jour de lien en instance, et le champ État n'est pas 135.

Tout accusé de réception de lien qui ne satisfait pas à tous ces essais DOIT être ignoré en silence.

Quand un nœud mobile reçoit un paquet portant un accusé de réception de lien valide, le nœud mobile DOIT examiner le champ État comme suit :
- o Si le champ État indique que la mise à jour de lien est acceptée (le champ État est inférieur à 128) alors le nœud mobile DOIT mettre à jour l'entrée correspondante dans sa liste de mises à jour de lien pour indiquer que la mise à jour de lien a été acquittée ; le nœud mobile DOIT alors arrêter de retransmettre la mise à jour de lien. De plus, si la valeur spécifiée dans le champ Durée de vie dans l'accusé de réception de lien est inférieure à la valeur de durée de vie envoyée dans la mise à jour de lien dont il est accusé réception, le nœud mobile DOIT soustraire la différence entre ces deux valeurs de durée de vie de la durée de vie restante pour le lien comme maintenue dans l'entrée correspondante de la liste de mises à jour de lien (avec une valeur minimum pour la durée de vie d'entrée de liste de mise à jour de lien de 0). C'est-à-dire que si la valeur de durée de vie envoyée dans la mise à jour de lien était L_màj, la valeur de durée de vie reçue dans l'accusé de réception de lien était L_acc, et la durée de vie restante actuelle de l'entrée de liste de mise à jour de lien est L_reste, alors la nouvelle valeur pour la durée de vie restante de l'entrée de liste de mise à jour de lien devrait être max((L_reste - (L_màj - L_acc)), 0) où max(X, Y) est le maximum de X et Y. L'effet de cette démarche est de gérer correctement la vue du nœud mobile de la durée de vie restante du lien (comme maintenue dans l'entrée correspondante de la liste de

mise à jour de lien) afin qu'elle décompte correctement la valeur de durée de vie donnée dans l'accusé de réception de lien, mais avec un décompte de temporisateur commençant au moment où la mise à jour de lien a été envoyée.

Les nœuds mobiles DEVRAIENT envoyer une nouvelle mise à jour de lien bien avant l'expiration de cette période afin d'étendre la durée de vie. Cela aide à éviter l'interruption de la communication qui pourrait autrement être causée par les délais du réseau ou la dérive d'horloge.

- Si l'accusé de réception de lien réussit correctement à l'authentification et si la valeur du champ État est 135 (numéro de séquence hors de la fenêtre) le nœud mobile DOIT alors mettre à jour son numéro de séquence de lien pour qu'il corresponde de façon appropriée au numéro de séquence donné dans l'accusé de réception de lien. Autrement, si la valeur du champ État est 135 mais si l'accusé de réception de lien n'est pas authentifié, le message DOIT être ignoré en silence.
- Si la valeur du champ État est 1 (accepté mais découverte de préfixe nécessaire) le nœud mobile DEVRAIT envoyer un message Sollicitation de préfixe mobile pour mettre à jour ses informations sur les préfixes disponibles.
- Si le champ État indique que la mise à jour de lien a été rejetée (le champ État est supérieur ou égal à 128) le nœud mobile peut alors prendre des mesures pour corriger la cause de l'erreur et retransmettre la mise à jour de lien (avec une nouvelle valeur de numéro de séquence) sous réserve de la restriction de limitation de taux spécifiée au paragraphe 11.8. Si ceci n'est pas fait ou échoue, le nœud mobile DEVRAIT alors enregistrer dans sa liste des mises à jour de lien que les futures mises à jour de lien NE DEVRAIENT PAS être envoyées à cette destination.

Le traitement d'une option de mobilité Avis de rafraîchissement de lien au sein de l'accusé de réception de lien dépend de la provenance de l'accusé de réception. Cette option DOIT être ignorée si l'accusé de réception venait d'un nœud correspondant. Si il venait de l'agent de rattachement, le nœud mobile utilise le champ Intervalle de rafraîchissement dans l'option comme suggestion qu'il DEVRAIT tenter de rafraîchir son enregistrement de rattachement à l'intervalle plus court indiqué.

Si l'accusé de réception venait de l'agent de rattachement, le nœud mobile examine la valeur du bit K (capacité de mobilité de gestion de clé). Si ce bit est à zéro, le nœud mobile DEVRAIT éliminer les connexions de protocole de gestion de clés, si il en est, à l'agent de rattachement. Le nœud mobile PEUT aussi initier une nouvelle connexion de gestion de clés. Si ce bit est établi, le nœud mobile DEVRAIT placer son propre point d'extrémité dans les connexions de protocole de gestion de clés à l'agent de rattachement, si il en est un. Le nouveau point d'extrémité du nœud mobile devrait être la nouvelle adresse d'entretien.

11.7.4 Réception des demandes de rafraîchissement de lien

Quand un nœud mobile reçoit un paquet contenant un message Demande de rafraîchissement de lien, si le nœud mobile a une entrée de liste de mises à jour de lien pour la source de la demande de rafraîchissement de lien, et si le nœud mobile veut conserver son entrée d'antémémoire de liens au nœud correspondant, le nœud mobile devrait alors commencer une procédure d'acheminement de retour. Si le nœud mobile veut faire supprimer son entrée d'antémémoire de liens, il peut soit ignorer la demande de rafraîchissement de lien et attendre que le lien arrive à expiration, soit à tout moment, il peut supprimer son lien avec un nœud correspondant avec une mise à jour de lien explicite avec une durée de vie de zéro et l'adresse d'entretien réglée à l'adresse de rattachement. Si le nœud mobile ne sait pas si il a besoin de l'entrée d'antémémoire de liens, il peut prendre la décision en fonction de la mise en œuvre, par exemple sur la base des ressources disponibles.

Noter que le nœud mobile devrait être attentif à ne pas répondre aux demandes de rafraîchissement de lien pour des adresses qui ne sont pas dans la liste des mises à jour de lien pour éviter d'être soumis à une attaque de déni de service.

Si la procédure d'acheminement de retour s'achève avec succès, un message de mise à jour de lien DEVRAIT être envoyé, comme décrit au paragraphe 11.7.2. Le champ Durée de vie dans cette mise à jour de lien DEVRAIT être réglé à une nouvelle durée de vie, étendant toute durée de vie courante restant d'une précédente mise à jour de lien envoyée à ce nœud (comme indiqué dans toute entrée existante de liste de mises à jour de lien pour ce nœud) et la durée de vie DEVRAIT là encore être inférieure ou égale à la durée de vie restante de l'enregistrement de rattachement et de l'adresse d'entretien spécifiée pour le lien. Quand il envoie cette mise à jour de lien, le nœud mobile DOIT mettre à jour sa liste des mises à jour de lien de la même façon que pour toute autre mise à jour de lien envoyée par le nœud mobile.

11.8 Limitation des retransmissions et du débit

Le nœud mobile est responsable de la limitation du taux de retransmissions dans la procédure d'acheminement de retour, dans les enregistrements, et dans la découverte de préfixe sollicitée.

Quand le nœud mobile envoie une sollicitation de préfixe mobile, une initiation d'essai de rattachement, une initiation d'essai d'entretien, ou une mise à jour de lien pour laquelle il attend une réponse, le nœud mobile doit déterminer une valeur pour le temporisateur de retransmission initiale :

- o Si le nœud mobile envoie une sollicitation de préfixe mobile, il DEVRAIT utiliser un intervalle initial de retransmission de INITIAL_SOLICIT_TIMER (voir la Section 12).
- o Si le nœud mobile envoie une mise à jour de lien et n'a pas de lien existant avec l'agent de rattachement, il DEVRAIT utiliser InitialBindackTimeoutFirstReg (voir la Section 13) comme valeur pour le temporisateur de retransmission initiale. Ce long intervalle de retransmission va permettre à l'agent de rattachement d'achever la procédure de détection d'adresse dupliquée rendue obligatoire dans ce cas, comme détaillé au paragraphe 11.7.1.
- o Autrement, le nœud mobile devrait utiliser la valeur spécifiée de INITIAL_BINDACK_TIMEOUT pour le temporisateur de retransmission initiale.

Si le nœud mobile échoue à recevoir une réponse valide correspondante dans l'intervalle de retransmission initiale choisi, il DEVRAIT retransmettre le message jusqu'à la réception d'une réponse.

Les retransmissions par le nœud mobile DOIVENT utiliser un processus de retard exponentiel dans lequel la période de temporisation est doublée à chaque retransmission, jusqu'à ce que le nœud reçoive une réponse ou que la période de temporisation atteigne la valeur de MAX_BINDACK_TIMEOUT. Le nœud mobile PEUT continuer indéfiniment d'envoyer ces messages à ce taux réduit.

Le nœud mobile DEVRAIT commencer un processus de retard séparé pour les différents types de messages, les différentes adresses de rattachement, et les différentes adresses d'entretien. Cependant, en plus, une limitation globale de taux s'applique pour les messages envoyés à un nœud correspondant particulier. Ceci assure que le nœud correspondant a un délai suffisant pour répondre, par exemple quand les liens pour plusieurs adresses de rattachement sont enregistrées. Le nœud mobile NE DOIT PAS envoyer de messages En-tête de mobilité d'un type particulier à un nœud correspondant particulier plus de MAX_UPDATE_RATE fois par seconde.

Les retransmissions de mises à jour de lien DOIVENT utiliser une valeur de numéro de séquence supérieure à celle utilisée pour la précédente transmission de cette mise à jour de lien. Les messages retransmis d'initiation d'essai de rattachement et d'essai d'entretien DOIVENT utiliser les nouvelles valeurs de mouchards.

12. Constantes du protocole

DHAAD_RETRIES	4 retransmissions
INITIAL_BINDACK_TIMEOUT	1 seconde
INITIAL_DHAAD_TIMEOUT	3 secondes
INITIAL_SOLICIT_TIMER	3 secondes
MAX_BINDACK_TIMEOUT	32 secondes
MAX_DELETE_BCE_TIMEOUT	10 secondes
MAX_NONCE_LIFETIME	240 secondes
MAX_TOKEN_LIFETIME	210 secondes
MAX_RO_FAILURE	3 essais
MAX_RR_BINDING_LIFETIME	420 secondes
MAX_UPDATE_RATE	3 fois
PREFIX_ADV_RETRIES	3 retransmissions
PREFIX_ADV_TIMEOUT	3 secondes

13. Variables de configuration du protocole

MaxMobPfxAdvInterval	par défaut : 86 400 secondes
MinDelayBetweenRAs	par défaut : 3 secondes, minimum : 0,03 seconde
MinMobPfxAdvInterval	par défaut : 600 secondes
InitialBindackTimeoutFirstReg	par défaut : 1,5 seconde

Les agents de rattachement DOIVENT permettre que les trois premières variables soient configurées par la gestion du système, et les nœuds mobiles DOIVENT permettre que la dernière variable soit configurée par la gestion du système.

La valeur par défaut pour InitialBindackTimeoutFirstReg a été calculée comme 1,5 fois la valeur par défaut de RetransTimer, comme spécifié dans la découverte de voisin [RFC4861] fois la valeur par défaut de DupAddrDetectTransmits, comme spécifié dans l'autoconfiguration d'adresse sans état [RFC4862].

La valeur MinDelayBetweenRAs outrepasse la valeur de la constante de protocole MIN_DELAY_BETWEEN_RAS, comme spécifié dans la découverte de voisin [RFC4861]. Cette variable DEVRAIT être réglée à MinRtrAdvInterval, si MinRtrAdvInterval est moins de 3 secondes.

14. Considérations relatives à l'IANA

Le présent document définit un nouveau protocole IPv6, En-tête de mobilité, décrit au paragraphe 6.1. Ce protocole a reçu le numéro de protocole 135.

Le présent document crée aussi un nouvel espace de noms "Type d'en-tête de mobilité", pour le champ Type de MH dans l'en-tête de mobilité. Les types de message actuels sont décrits à partir du paragraphe 6.1.2, et sont les suivants :

0 Demande de rafraîchissement de lien
1 Initiation d'essai de rattachement
2 Initiation d'essai d'entretien
3 Essai de rattachement
4 Essai d'entretien
5 Mise à jour de lien
6 Accusé de réception de lien
7 Erreur de lien

De futures valeurs de type de MH peuvent être allouées par action de normalisation ou approbation de l'IESG [RFC5226].

De plus, chaque message de mobilité peut contenir des options de mobilité comme décrit au paragraphe 6.2. Le présent document définit un nouvel espace de noms "Option de mobilité" pour identifier ces options. Les options de mobilité actuelles sont définies à partir du paragraphe 6.2.2 et sont les suivantes :

0 Pad1
1 PadN
2 Avis de rafraîchissement de lien
3 Adresse d'entretien de remplacement
4 Indices de nom occasionnel
5 Données d'autorisation

De futures valeurs du type d'option peuvent être alloués par action de normalisation ou approbation de l'IESG [RFC5226].

Finalement, ce document crée un troisième espace de noms "Code d'état" pour le champ État dans le message Accusé de réception de lien. La liste des valeurs courantes est au paragraphe 6.1.8 et ce sont :

0 Mise à jour de lien acceptée
1 Accepté mais découverte de préfixe nécessaire
128 Raison non spécifiée
129 Administrativement interdit
130 Ressources insuffisantes
131 Enregistrement de rattachement non accepté
132 Pas de sous réseau de rattachement
133 Pas d'agent de rattachement pour ce nœud mobile
134 Échec de détection d'adresse dupliquée
135 Numéro de séquence hors de la fenêtre
136 Indice de nom occasionnel de rattachement expiré
137 Indice de nom occasionnel d'entretien expiré
138 Noms occasionnels expirés
139 Changement de type d'enregistrement interdit
174 Adresse d'entretien invalide

Les futures valeurs du champ État peuvent être allouées par action de normalisation ou approbation de l'IESG [RFC5226]

Tous les champs marqués "Réservé" ne peuvent être alloués que par action de normalisation ou approbation de l'IESG.

Le présent document définit aussi une nouvelle option de destination IPv6, l'option Adresse de rattachement, décrite au paragraphe 6.3. Cette option a reçu la valeur de type d'option de 0xC9.

Le présent document définit aussi un nouvel en-tête IPv6 d'acheminement de type 2, décrit au paragraphe 6.4. La valeur 2 a été allouée par l'IANA.

De plus, le présent document définit quatre types de messages ICMP, deux utilisés au titre du mécanisme de découverte dynamique d'adresse d'agent de rattachement, et deux utilisés à la place des Sollicitations et des Annonces de routeur quand le nœud mobile est hors de la liaison de rarrachement. Ces messages ont reçu les numéros de type ICMPv6 dans la gamme des messages d'information :

- o Le message Demande de découverte d'adresse d'agent de rattachement, décrit au paragraphe 6.5;
- o Le message de réponse de découverte d'adresse d'agent de rattachement, décrit au paragraphe 6.6;
- o La sollicitation de préfixe mobile, décrite au paragraphe 6.7; et
- o L'annonce de préfixe mobile, décrite au paragraphe 6.8.

Le présent document définit aussi deux nouvelles options de découverte de voisin [RFC4861] qui ont reçu les valeurs de type d'option dans l'espace de numérotation d'option pour les messages de découverte de voisin :

- o L'option Intervalle d'annonces, décrite au paragraphe 7.3
- o L'option Informations d'agent de rattachement, décrite au paragraphe 7.4.

15. Considérations pour la sécurité

15.1 Menaces

Toute solution de mobilité doit se protéger contre les mauvaises utilisations des caractéristiques et mécanismes de mobilité. Dans IPv6 mobile, la plupart des menaces potentielles sont concernées par les faux liens, qui résultent généralement en des attaques de déni de service. Certaines des menaces posent aussi des menaces potentielles d'interposition, de capture, d'atteintes à la confidentialité, et d'usurpation d'identité. Les principales menaces contre lesquelles protègent ce protocole sont :

- o Les menaces qui impliquent des mises à jour de lien envoyées aux agents de rattachement et nœuds correspondants. Par exemple, un attaquant peut prétendre qu'un certain nœud mobile est actuellement à une localisation différente de celle qu'il a réellement. Si un agent de rattachement accepte de telles informations falsifiées qui lui sont envoyés, le nœud mobile peut ne pas obtenir le trafic qui lui est destiné. De façon similaire, un nœud (mobile) malveillant peut utiliser l'adresse de rattachement d'un nœud victime dans une mise à jour de lien falsifiée envoyée à un nœud correspondant.

  Ceci fait peser des menaces sur la confidentialité, l'intégrité, et la disponibilité. C'est-à-dire qu'un attaquant peut apprendre le contenu des paquets destinés à un autre nœud en redirigeant le trafic sur lui-même. De plus, un attaquant peut utiliser les paquets redirigés pour tenter de s'établir comme interposé entre un nœud mobile et un nœud correspondant. Ceci permettrait à l'attaquant de se faire passer pour le nœud mobile, conduisant à des problèmes d'intégrité et de disponibilité.

  Un nœud mobile malveillant peut aussi envoyer des mises à jour de lien dans lesquelles l'adresse d'entretien est réglée à l'adresse d'un nœud victime. Si de telles mises à jour de lien étaient acceptées, le nœud malveillant pourrait tromper le nœud correspondant pour lui faire envoyer de potentiellement grosses quantités de données à la victime ; les réponses du nœud correspondant aux messages envoyés par le nœud mobile malveillant vont être envoyés à l'hôte ou réseau victime. Ceci pourrait être utilisé pour causer une attaque de déni de service répartie. Par exemple, le nœud correspondant pourrait être un site qui va envoyer un flux vidéo à forte bande passante à quiconque le demande. Noter que l'utilisation de protocoles de contrôle des flux comme TCP ne défend pas nécessairement contre ce type d'attaque, parce que l'attaquant peut falsifier les accusés de réception. Même garder secrets les numéros de séquence initiaux de TCP n'aide pas parce que l'attaquant peut recevoir les quelques premiers segments (incluant le ISN) à sa propre adresse, et rediriger seulement ensuite le flux à l'adresse de la victime. Ces types d'attaques peuvent aussi être dirigés sur des réseaux au lieu de nœuds. D'autres variantes de cette menace sont décrites dans [28] et [35].

  Un attaquant pourrait aussi tenter de perturber les communications d'un nœud mobile en répétant une mise à jour de lien que le nœud a envoyé antérieurement. Si la vieille mise à jour de lien est acceptée, les paquets destinés au nœud mobile vont être envoyés à son ancienne localisation et non à sa localisation actuelle.

  Un nœud mobile malveillant associé à plusieurs agents de rattachement pourrait créer une boucle d'acheminement parmi eux. Ceci peut être réalisé quand un nœud mobile lie une adresse de rattachement située sur un premier agent de rattachement à une autre adresse de rattachement sur un second agent de rattachement. Ce type de lien va forcer les agents de rattachement à acheminer le même paquet à chacun des autres sans savoir qu'une boucle d'acheminement a été créée. Un tel problème de boucle se limite aux cas où un nœud mobile a plusieurs agents de rattachement et qu'il lui est permis d'être associé à plusieurs agents de rattachement. Pour le cas de l'agent de rattachement unique, une politique chez l'agent de rattachement va empêcher le lien d'une adresse de rattachement à une autre adresse de rattachement hébergée par le même agent de rattachement.

Les problèmes potentiels causés par de telles boucles d'acheminement dans ce scénario peuvent être substantiellement réduits par l'utilisation de l'option Limite de tunnel spécifiée dans la [RFC2473].

En conclusion, il y a des menaces de déni de service, d'interposition, de confidentialité, et d'usurpation d'identité contre les parties impliquées dans l'envoi de mises à jour de lien légitimes, la menace de boucles d'acheminement quand il y a plusieurs agents de rattachement, et des menaces de déni de service contre toute autre partie.

- Menaces associées aux paquets de charge utile : les paquets de charge utile échangés avec les nœuds mobiles sont exposés à des menaces similaires à celles du trafic IPv6 régulier. Cependant, IPv6 mobile introduit l'option de destination Adresse de rattachement et un nouveau type d'en-tête d'acheminement (type 2) et utilise des en-têtes de tunnelage dans les paquets de charge utile. Le protocole doit protéger contre de nouvelles menaces potentielles impliquant l'utilisation de ces mécanismes.

  Les tiers sont exposés à une menace de réflexion via l'option de destination Adresse de rattachement, sauf si des précautions appropriées de sécurité sont respectées. L'option de destination Adresse de rattachement pourrait être utilisée pour diriger le trafic de réponse vers un nœud dont l'adresse IP apparaît dans l'option. Dans ce cas, le filtrage d'entrée ne va pas capturer la fausse "adresse de retour" [38], [RFC4225].

  Une menace similaire existe avec les tunnels entre le nœud mobile et l'agent de rattachement. Un attaquant peut falsifier les paquets dans le tunnel entre le nœud mobile et l'agent de rattachement, les faisant apparaître comme du trafic venant du nœud mobile alors qu'il ne le sont pas. Noter qu'un attaquant qui est capable de falsifier les paquets dans le tunnel va normalement être aussi capable de falsifier les paquets qui paraissent venir directement du nœud mobile. Ce n'est pas une nouvelle menace par elle-même. Cependant, il peut être plus facile aux attaquants d'échapper à la détection en évitant le filtrage d'entrée et les mécanismes de traçage des paquets. De plus, des paquets falsifiés dans le tunnel peuvent être utilisés pour obtenir l'accès au réseau de rattachement.

  Finalement, un en-tête d'acheminement pourrait aussi être utilisé dans des attaques en réflexion, et dans des attaques conçues pour outrepasser les pare-feu. La généralité de l'en-tête d'acheminement régulier permettrait de circonvenir les règles fondées sur l'adresse IP dans les pare-feu. Elle permettrait aussi la réflexion du trafic aux autres nœuds. Ces menaces existent avec les en-têtes d'acheminement en général, même si l'usage qu'exige IPv6 est sûr.

- Menaces associées à la découverte dynamique d'agent de rattachement et de préfixe mobile.

- Menaces contre les mécanismes de sécurité IPv6 mobile eux-mêmes : un attaquant pourrait, par exemple, tromper les participants en leur faisant exécuter des opérations cryptographiques coûteuses ou en allouant de la mémoire pour les besoins de la conservation de l'état. Le nœud victime n'aurait plus de ressources pour traiter les autres tâches.

Comme service fondamental dans la pile IPv6, IPv6 mobile est supposé être déployé dans la plupart des nœuds de l'Internet IPv6. Les menaces ci-dessus devraient donc être considérées comme applicables à tout l'Internet.

On devrait aussi noter que des menaces supplémentaires résultent des mouvements en tant que tels, même sans l'implication de protocoles de mobilité. Les nœuds mobiles doivent être capables de se défendre dans les réseaux qu'ils visitent, car les défenses périmétriques normales appliquées dans le réseau de rattachement ne les protègent plus.

15.2 Caractéristiques

La présente spécification fournit une série de caractéristiques conçues pour atténuer les risques introduits par les menaces citées ci-dessus. Les principales caractéristiques de sécurité sont les suivantes :

- tunnelage inverse comme dispositif obligatoire,
- protection des mises à jour de lien envoyées aux agents de rattachement,
- protection des mises à jour de lien envoyées aux nœuds correspondants,
- protection contre les attaques en réflexion qui utilisent l'option de destination Adresse de rattachement,
- protection des tunnels entre le nœud mobile et l'agent de rattachement,
- fermeture des vulnérabilités de l'en-tête d'acheminement,
- atténuation des menaces de déni de service aux mécanismes de sécurité de IPv6 mobile eux-mêmes.

La prise en charge du tunnelage inverse chiffré (voir au paragraphe 11.3.1) permet aux nœuds mobiles de contrer certaines sortes d'analyse de trafic.

La protection des mises à jour de lien qui sont envoyées aux agents de rattachement et de celles qui sont envoyées à des nœuds correspondants arbitraires exige des solutions de sécurité très différentes à cause de situations différentes. Les

nœuds mobiles et les agents de rattachement sont naturellement supposés être soumis à l'administration du réseau du domaine de rattachement.

Donc, ils peuvent et sont supposés avoir une association de sécurité qui peut être utilisée pour authentifier fiablement les messages échangés. Voir au paragraphe 5.1 la description des mécanismes du protocole, et au paragraphe 15.3 une discussion sur le niveau de sécurité résultant.

Il est prévu que l'optimisation de chemin IPv6 mobile sera utilisée sur une base globale entre nœuds appartenant à des domaines administratifs différents. Ce serait une tâche très exigeante que de construire une infrastructure d'authentification à cette échelle. De plus, une infrastructure d'authentification traditionnelle ne peut pas être facilement utilisée pour authentifier les adresses IP parce que les adresses IP peuvent changer souvent. Il n'est pas suffisant de juste authentifier les nœuds mobiles ; l'autorisation de revendiquer le droit d'utiliser une adresse est aussi nécessaire. Donc, une approche "sans infrastructure" est nécessaire. La méthode sans infrastructure choisie est décrite au paragraphe 5.2, et le paragraphe 15.4 discute du niveau de sécurité résultant et des raisons de la conception de cette approche.

Des règles spécifiques guident l'utilisation de l'option de destination Adresse de rattachement, de l'en-tête d'acheminement, et des en-têtes de tunnelage dans les paquets de charge utile. Ces règles sont nécessaires pour supprimer les faiblesses associées à leur utilisation sans restriction. L'effet de ces règles est discuté aux paragraphes 15.7, 15.8, et 15.9.

Les menaces de déni de service contre les mécanismes de sécurité IPv6 mobile eux-mêmes concernent principalement les procédures de mise à jour de lien avec les nœuds correspondants. Le protocole a été conçu pour limiter les effets de telles attaques, comme il est décrit au paragraphe 15.4.5.

15.3 Mises à jour de liens à l'agent de rattachement

La signalisation entre le nœud mobile et l'agent de rattachement exige la protection de l'intégrité des messages. C'est nécessaire pour assurer à l'agent de rattachement qu'une mise à jour de lien provient d'un nœud mobile légitime. De plus, un ordre correct et une protection contre la répétition sont en option.

IPsec ESP protège l'intégrité des mises à jour de lien et des accusés de réception de lien en sécurisant les messages de mobilité entre le nœud mobile et l'agent de rattachement.

IPsec ne peut fournir la protection contre la répétition que si un chiffrement dynamique est utilisé (ce qui peut ne pas être toujours le cas). IPsec ne garantit pas l'ordre correct des paquets, mais seulement qu'ils n'ont pas été répétés. À cause de cela, les numéros de séquence au sein des messages IPv6 sont utilisés pour assurer l'ordre correct (voir au paragraphe 5.1). Cependant, si l'espace de numéro de séquence de 16 bits de IPv6 mobile est entièrement parcouru, ou si l'agent de rattachement réamorce et perd l'état concernant les numéros de séquence, des attaques en répétition et en réarrangement deviennent possible. L'utilisation du chiffrement dynamique, les protections IPsec anti répétition, et les numéros de séquence IPv6 mobile peuvent ensemble empêcher de telles attaques. Il est aussi recommandé que l'utilisation d'une mémorisation non volatile soit envisagée pour les agents de rattachement, pour éviter de perdre leur état.

Un schéma de fenêtre glissante est utilisé pour les numéros de séquence. La protection contre les répétitions et le réarrangement sans mécanisme de gestion de clés fonctionne quand l'attaquant se souvient de jusqu'à un maximum de 2**15 mises à jour de lien.

Les mécanismes ci-dessus ne montrent pas que l'adresse d'entretien donnée dans la mise à jour de lien est correcte. Cela ouvre la possibilité d'attaques de déni de service contre des tiers. Cependant, comme le nœud mobile et l'agent de rattachement ont une association de sécurité, l'agent de rattachement peut toujours identifier un nœud mobile qui se comporte mal. Cela permet à l'opérateur de l'agent de rattachement de suspendre le service de ce nœud mobile, et éventuellement de prendre des mesures fondées sur les relations d'affaires avec le propriétaire du nœud mobile.

Noter que l'utilisation d'une seule paire d'associations de sécurité chiffrées manuellement entre en conflit avec la génération d'une nouvelle adresse de rattachement [RFC4941] pour le nœud mobile, ou avec l'adoption d'un nouveau préfixe de sous réseau de rattachement. C'est parce que les associations de sécurité IPsec sont liées aux adresses utilisées. Bien que le chiffrement automatique fondé sur le certificat atténue dans une certaine mesure ce problème, il est quand même nécessaire de s'assurer qu'un certain nœud mobile ne peut pas envoyer de mises à jour de lien pour l'adresse d'un autre nœud mobile. En général, ceci conduit à l'inclusion d'adresses de rattachement dans les certificats dans le champ SubjectAltName. Cela limite aussi l'introduction de nouvelles adresses sans des procédures manuelles ou automatiques pour établir les nouveaux certificats. Donc, la présente spécification restreint la génération de nouvelles adresses de rattachement (quelle qu'en soit la raison) aux situations où existe déjà une association de sécurité ou un certificat pour la nouvelle adresse.

La prise en charge de IKEv2 a été spécifiée comme facultative. Ce qui suit sur l'utilisation du chiffrement manuel devrait être observé :

- Comme expliqué précédemment, avec IPsec en chiffrement manuel, une forme limitée de protection existe seulement contre les attaques en répétition et en réarrangement. Une vulnérabilité existe si l'espace de numéro de séquence est entièrement parcouru ou si l'agent de rattachement réamorce et oublie ses numéros de séquence (et utilise une mémoire volatile pour mémoriser les numéros de séquence). En supposant que le nœud mobile bouge de façon continue toutes les 10 minutes, il faut en gros 455 jours avant que l'espace entier de numéros de séquence soit parcouru. Les schémas normaux de mouvement atteignent rarement cette fréquence aujourd'hui.
- Un nœud mobile et son agent de rattachement appartiennent au même domaine. Si ce n'était pas le cas, le chiffrement manuel ne serait pas possible [RFC4107], mais dans IPv6 mobile seules ces deux parties ont besoin de connaître les clés configurées manuellement. De même, on note que IPv6 mobile emploie les chiffrements de bloc standard dans IPsec, et n'est pas vulnérable aux problèmes associés au chiffrement de flux et au chiffrement manuel.
- On s'attend à ce que le propriétaire du nœud mobile et l'administrateur de l'agent de rattachement s’accordent sur les clés utilisées et les autres paramètres par un mécanisme hors ligne. L'utilisation de IKEv2 avec IPv6 mobile est documentée plus en détails dans la [RFC4877]. Ce qui suit devrait être observé concernant l'utilisation de IKEv2 :
- Il est nécessaire d'empêcher un nœud mobile de revendiquer une autre adresse de rattachement du nœud mobile. L'agent de rattachement doit vérifier que le nœud mobile qui essaye de négocier la SA pour une certaine adresse de rattachement est autorisé pour cette adresse de rattachement. Cela implique que même avec l'utilisation de IKEv2, une entrée de politique doit être configurée pour chaque adresse de rattachement desservie par l'agent de rattachement. Il est possible d'inclure les adresses de rattachement dans le champ Subject AltName du certificat pour éviter cela. Cependant, il n'est pas garanti que les mises en œuvre prennent en charge l'utilisation d'une adresse IP (adresse d'entretien) particulière alors qu'une autre adresse (adresse de rattachement) apparaît dans le certificat. Dans tous les cas, même cette approche exigerait des tâches spécifiques de l'utilisateur dans l'autorité de certificat.
- Du fait des problèmes mentionnés au paragraphe 11.3.2, la SA IKEv2 entre le nœud mobile et son agent de rattachement est établie en utilisant l'adresse d'entretien actuelle du nœud mobile. Cela implique que quand le nœud mobile passe à une nouvelle localisation, il peut devoir rétablir une association de sécurité IKEv2. Un fanion K (capacité de mobilité de gestion de clé) est fourni pour les mises en œuvre qui peuvent mettre à jour les points d'extrémité IKEv2 sans rétablir une association de sécurité IKEv2, mais la prise en charge de ce comportement est facultative.
- Néanmoins, même si la configuration par nœud mobile est exigée avec IKEv2, un important avantage de IKEv2 est qu'il automatise la négociation des paramètres cryptographiques, incluant les indices de paramètres de sécurité (SPI, *Security Parameter Indices*) les algorithmes de chiffrement, et ainsi de suite. Donc, moins d'informations de configuration sont nécessaires.
- La fréquence des mouvements dans certaines couches de liaison ou scénarios de déploiement peut être assez élevée pour rendre possibles des attaques en répétition et réarrangement, si seul le chiffrement manuel est utilisé. IKEv2 DEVRAIT être utilisé dans ce cas. Des scénarios potentiellement vulnérables impliquent un mouvement continu à travers de petites cellules, ou une alternance non contrôlée entre les points de rattachement réseau disponibles.
- De façon similaire, dans certains scénarios de déploiement, le nombre de nœuds mobiles peut être très grand. Dans ces cas, il peut être nécessaire d’utiliser des mécanismes automatiques pour réduire l'effort de gestion de l'administration des paramètres cryptographiques, même si une certaine configuration par nœud mobile est toujours nécessaire. IKEv2 DEVRAIT aussi être utilisé dans ces cas.

15.4 Mises à jour de liens aux nœuds correspondants

Les motifs de la conception de la procédure d'acheminement de retour sont d'avoir une prise en charge suffisante pour IPv6 mobile, sans créer de nouveaux problèmes de sécurité significatifs. Le but de cette procédure n'était pas de protéger contre des attaques qui étaient toujours possible avant l'introduction de IPv6 mobile.

Les paragraphes qui suivent décrivent les propriétés de sécurité de la méthode utilisée, à la fois du point de vue de possibles attaquants sur le chemin qui peuvent voir ces valeurs cryptographiques qui ont été envoyées en clair (paragraphes 15.4.2 et 15.4.3) et du point de vue des autres attaquants (paragraphe 15.4.6).

15.4.1 Généralités

La méthode sans infrastructure choisie vérifie que le nœud mobile est "vivant" (c'est-à-dire, il répond aux sondes) à ses adresses de rattachement et d'entretien. Le paragraphe 5.2 décrit la procédure d'acheminement de retour en détail. La procédure utilise les principes suivants :

- Un échange de messages vérifie que le nœud mobile est accessible à ses adresses, c’est-à-dire, il est au moins capable d'émettre et recevoir le trafic aux deux adresses de rattachement et d'entretien.
- La mise à jour de lien éventuelle est liée cryptographiquement aux jetons fournis dans les messages échangés.
- Des échanges symétriques sont employés pour éviter d'utiliser ce protocole dans les attaques en réflexion. Dans un échange symétrique, les réponses sont toujours envoyées à la même adresse que celle d'où la demande a été envoyée.

- Le nœud correspondant opère sans état jusqu'à ce qu'il reçoive une mise à jour de lien pleinement autorisée.
- Une protection supplémentaire est fournie par le chiffrement des tunnels entre le nœud mobile et l'agent de rattachement avec IPsec ESP. Comme le tunnel transporte aussi les échanges de nom occasionnel, la capacité des attaquants de voir ces noms occasionnels est limitée. Par exemple, cela empêche le lancement des attaques à partir de la liaison étrangère courante du nœud mobile, même quand aucune confidentialité de couche de liaison n'est disponible.

Le niveau de sécurité résultant est en théorie le même que sans cette protection supplémentaire : les jetons d'acheminement de retour sont toujours exposés sur seulement un chemin dans tout l'Internet. Cependant, les nœuds mobiles se trouvent souvent sur des liaisons non sûres, comme un LAN sans fil à accès public. Donc, dans de nombreux cas, cet ajout fait une différence en pratique.

Pour plus d'informations sur les raisons de la conception de la procédure d'acheminement de retour, voir [28] [35] [34] [RFC4225]. Les mécanismes utilisés ont été adoptés à partir de ces documents.

15.4.2 Propriétés de sécurité élaborées

Le procédure d'acheminement de retour protège les mises à jour de lien contre tous les attaquants qui ne sont pas capables de surveiller le chemin entre l'agent de rattachement et le nœud correspondant. La procédure ne défend pas contre les attaquants qui peuvent surveiller ce chemin. Noter que de tels attaquants sont en tous cas capables de monter une attaque active contre le nœud mobile quand il est à sa localisation de rattachement. La possibilité de telles attaques n'est pas une entrave au déploiement de IPv6 mobile parce que ces attaques sont possibles sans considération de l'utilisation ou non de IPv6 mobile.

Cette procédure protège aussi contre les attaques de déni de service dans lesquelles l'attaquant prétend être mobile, mais utilise l'adresse de la victime comme adresse d'entretien. Ceci causerait l'envoi par le nœud correspondant à la victime d'un trafic inattendu. Cette procédure défend contre ces attaques en exigeant au moins la présence passive de l'attaquant à l'adresse d'entretien ou sur le chemin du correspondent à l'adresse d'entretien. Normalement, ce devrait être le nœud mobile.

15.4.3 Comparaison avec les communications IPv6 régulières

Ce paragraphe discute de la protection offerte par la méthode d'acheminement de retour en la comparant à la sécurité des communications IPv6 régulières. On divise les vulnérabilités en trois classes : (1) celles relatives aux attaquants sur le réseau local du nœud mobile, de l'agent de rattachement, ou du nœud correspondant, (2) celles relatives aux attaquants sur le chemin entre le réseau de rattachement et le nœud correspondant, et (3) les attaquants hors chemin, c’est-à-dire, le reste de l'Internet.

On discute maintenant des vulnérabilités des communications IPv6 régulières. Les vulnérabilités en liaison des communications IPv6 incluent les attaques de déni de service, d'usurpation d'identité, d'interposition, d'espionnage, et autres. Ces attaques peuvent être lancées à travers l'espionnage de la découverte de routeur, de la découverte de voisin, et autres mécanismes IPv6. Certaines de ces attaques peuvent être empêchées par l’utilisation de la protection cryptographique des paquets.

Une situation similaire existe avec les attaquants sur le chemin. C'est-à-dire que sans protection cryptographique, le trafic est complètement vulnérable.

En supposant que les attaquants n'ont pas pénétré la sécurité des protocoles d'acheminement de l'Internet, les attaques sont plus difficiles à lancer à partir de localisations hors chemin. Les attaques qui peuvent être lancées de ces localisations sont principalement des attaques de déni de service, comme des attaques d'inondation et/ou réflexion. Il n'est pas possible à un attaquant hors chemin de s'interposer.

Ensuite, on considère les vulnérabilités qui existent quand IPv6 est utilisé avec IPv6 mobile et la procédure d'acheminement de retour. Sur la liaison locale, les vulnérabilités sont les mêmes que dans IPv6, mais des attaques par usurpation d'identité et par interposition peuvent aussi être lancées contre les futures communications, et non juste les communications en cours. Si une mise à jour de lien est envoyée alors que l'attaquant est présent sur la liaison, ses effets restent pour la durée de vie du lien. Ceci se produit même si l'attaquant quitte la liaison. À l'opposé, un attaquant qui utilise seulement le IPv6 de base n'a généralement pas de séjour sur la liaison afin de continuer l'attaque. Noter que afin de lancer ces nouvelles attaques, l'adresse IP de la victime doit être connue. Cela rend cette attaque faisable, principalement dans le contexte d'identifiants d'interface bien connus, comme ceux qui apparaissent déjà dans le trafic sur la liaison ou enregistrés dans le DNS.

Les attaquants en chemin peuvent exploiter des vulnérabilités similaires dans le IPv6 régulier. Il y a aussi cependant des différences mineures. Les attaques en usurpation d'identité, par interposition, et de déni de service peuvent être lancées

avec juste l'interception de quelques paquets, tandis que dans le IPv6 régulier, il est nécessaire d'intercepter chaque paquet. L'effet des attaques est cependant le même sans considération de la méthode. Dans tous les cas, la tâche la plus difficile d'un attaquant dans ces attaques est d'obtenir le bon chemin.

Les vulnérabilités pour des attaquants hors chemin sont les mêmes que dans l'IPv6 régulier. Les nœuds qui ne sont pas sur le chemin entre l'agent de rattachement et le nœud correspondant ne seront pas capables de recevoir les messages de sonde d'adresse de rattachement.

En conclusion, on peut déclarer les principaux résultats suivants de cette comparaison :

- L'acheminement de retour empêche toutes les attaques hors chemin au delà de celles qui sont déjà possibles dans l'IPv6 régulier. C'est le résultat le plus important, empêchant les attaquants sur l'Internet d'exploiter les vulnérabilités.
- Les vulnérabilités pour les attaquants sue la liaison de l'agent de rattachement, la liaison du nœud correspondant, et le chemin entre eux sont en gros les mêmes que dans l'IPv6 régulier.
- Cependant, une différence est que dans l'IPv6 de base un attaquant sur le chemin doit être constamment présent sur la liaison ou le chemin, tandis qu'avec IPv6 mobile, un attaquant peut laisser un lien derrière lui après être parti. Pour cette raison, la présente spécification limite la création des liens à au plus MAX_TOKEN_LIFETIME secondes après la dernière vérification de possibilité d'acheminement, et limite la durée d'un lien à au plus MAX_RR_BINDING_LIFETIME secondes. Avec ces limites, les attaquants ne peuvent tirer aucun avantage pratique de ces vulnérabilités.
- Il y a quelques autres différences mineures, telles qu'un effet de la vulnérabilité au déni de service. Elles peuvent être considérées comme insignifiantes.
- Le chemin entre l'agent de rattachement et un nœud correspondant est normalement le plus facile pour les attaques sur les liaisons à l'une ou l'autre extrémité, en particulier si ces liaisons sont des LAN sans fil à accès public. Les attaques contre les routeurs ou commutateurs sur le chemin sont normalement plus difficiles à accomplir. La sécurité sur la couche 2 des liaisons joue alors un rôle majeur dans la sécurité résultante du réseau global. De façon similaire, la sécurité de la découverte de voisin et de routeur IPv6 sur ces liaisons a un large impact. Si elles sont sécurisées à l'avenir à l'aide de quelque nouvelle technologie, cela pourrait changer la situation concernant le point d'attaque le plus facile.

Pour une discussion en profondeur de ces questions, voir la [RFC4225].

15.4.4 Attaques en répétition

La procédure d'acheminement de retour protège aussi les participants contre les mises à jour de lien répétées. L'attaquant est incapable de répéter le même message à cause du numéro de séquence qui fait partie de la mise à jour de lien. Il est aussi incapable de modifier la mise à jour de lien car la vérification de MAC va échouer après une telle modification.

Il faut cependant aussi faire attention quand on supprime des liens au nœud correspondant. Si un lien est supprimé alors que le nom occasionnel utilisé à sa création est encore valide, un attaquant pourrait répéter la vieille mise à jour de lien. Les règles mentionnées au paragraphe 5.2.8 assurent que ceci ne peut pas se produire.

15.4.5 Attaques de déni de service

La procédure d'acheminement de retour a une protection contre les attaques de déni de service par épuisement des ressources. Les nœuds correspondants ne conservent aucun état sur les nœuds mobiles individuels jusqu'à ce qu'une mise à jour de lien authentifiée arrive. Ceci est réalisé par la construction des jetons de génération de clés à partir des noms occasionnels et clés de nœud qui ne sont pas spécifiques des nœuds mobiles individuels. Les jetons de génération de clé (keygen) peuvent être reconstruits par le nœud correspondant, sur la base des informations d'adresse de rattachement et d'entretien qui arrivent avec la mise à jour de lien. Cela signifie que les nœuds correspondants sont en sécurité à l'égard des attaques d'épuisement de mémoire sauf lorsque des attaquants sur le chemin sont en cause. Du fait de l'utilisation du chiffrement symétrique, les nœuds correspondants sont aussi relativement en sûreté contre les attaques en épuisement de ressources de CPU.

Néanmoins, comme [28] le décrit, il y a des situations dans lesquelles il est impossible aux nœuds mobiles et correspondants de déterminer si ils ont réellement besoin d'un lien ou si ils ont juste été amenés à le croire par un attaquant. Donc, il est nécessaire de considérer les situations où de telles attaques sont faites.

Même si l'optimisation de chemin est une optimisation très importante, ce n'est quand même qu'une optimisation. Un nœud mobile peut communiquer avec un nœud correspondant même si le correspondant refuse d'accepter les mises à jour de lien. Cependant, les performances vont en souffrir parce que les paquets provenant du nœud correspondant pour le nœud mobile vont être acheminés via l'agent de rattachement du mobile plutôt que par un chemin plus direct. Un nœud correspondant peut se protéger contre certaines des attaques en épuisement de ressources comme suit : si le nœud correspondant est

inondé par un grand nombre de mises à jour de lien qui échouent aux vérifications d'intégrité cryptographique, il peut arrêter de traiter les mises à jour de lien ; si un nœud correspondant trouve qu'il dépense trop de ressources à vérifier des mises à jour de lien boguées qu'il n'en économiserait probablement en acceptant des mises à jour de lien authentiques, il peut alors éliminer en silence certaines ou toutes les mises à jour de lien sans effectuer aucune opération cryptographique.

Les couches au dessus de IP peuvent généralement fournir des informations supplémentaires pour aider à déterminer si il est besoin d'établir un lien avec un homologue spécifique. Par exemple, TCP sait si le nœud a une file d'attente de données qu'il essaye d'envoyer à un homologue. Une mise en œuvre de la présente spécification n'est pas obligée d'utiliser ces informations provenant des couches supérieures de protocole, mais certaines mises en œuvre vont probablement être capables de gérer leurs ressources plus efficacement en utilisant de telles informations.

On exige aussi que toutes les mises en œuvre soient capables de désactiver administrativement l'optimisation de chemin.

15.4.6 Longueurs de clé

Des attaquants peuvent essayer de casser la procédure d'acheminement de retour de nombreuses façons. Le paragraphe 15.4.2 discute de la situation où l'attaquant peut voir les valeurs cryptographiques envoyées en clair, et le paragraphe 15.4.3 discute de l'impact que cela a sur les communications IPv6. Ce paragraphe discute si les attaquants peuvent deviner les valeurs correctes sans les voir.

Lorsque la procédure d'acheminement de retour est en cours, des mouchards de 64 bits sont utilisés pour protéger contre les réponses falsifiées. On estime que c'est suffisant, étant donné qu'il faudrait deviner à l'aveugle une réponse à un très grand nombre de messages avant que le succès soit probable.

Les jetons utilisés dans la procédure d'acheminement de retour fournissent ensemble 128 bits d'information. Ces informations sont utilisées en interne comme entrée d'une fonction de hachage pour produire une quantité de 160 bits convenable pour produire le hachage chiffré dans la mise à jour de lien en utilisant l'algorithme HMAC_SHA1. La longueur finale du hachage chiffré est de 96 bits. Les facteurs limitant dans ce cas sont la longueur du jeton d'entrée et la longueur du hachage chiffré final. L'application de la fonction de hachage interne ne réduit pas l'entropie.

Le hachage chiffré final de 96 bits est de taille normale est il est estimé être sûr. L'entrée de 128 bits provenant des jetons est coupée en deux parties, le jeton de génération de clé de rattachement et le jeton de génération de clé d'entretien. Un attaquant peut essayer de deviner la valeur correcte du mouchard, mais cela va encore exiger un grand nombre de messages (en moyenne 2**63 messages pour une ou 2**127 pour deux). De plus, étant donné que les mouchards ne sont valides que pour un court instant, l'attaque doit conserver un fort taux constant de messages pour obtenir un effet durable. Cela ne paraît pas réalisable en pratique.

Quand le nœud mobile retourne chez lui, il lui est juste permis d'utiliser le jeton de génération de clé de rattachement de 64 bits. C'est moins que 128 bits, mais l'attaquer à l'aveugle exigerait quand même l'envoi d'un grand nombre de messages. Si l'attaquant est sur le chemin et est capable de voir la mise à jour de lien, on peut concevoir qu'il puisse casser le hachage chiffré en force brute. Cependant, dans ce cas, l'attaquant doit être sur le chemin, ce qui paraît offrir des moyens plus faciles pour un déni de service que d'empêcher l'optimisation de chemin.

15.5 Découverte dynamique de l'adresse de l'agent de rattachement

La fonction de découverte dynamique d'adresse d'agent de rattachement pourrait être utilisée pour apprendre les adresses des agents de rattachement dans le réseau de rattachement.

La capacité d'apprendre les adresses des nœuds peut être utile aux attaquants parce qu'un examen en force brute de l'espace d'adresses n'est pas praticable avec IPv6. Donc, ils pourraient tirer parti de tout moyen qui rend plus facile la cartographie du réseau. Par exemple, si une menace de sécurité ciblée sur les routeurs ou même les agents de rattachement est découverte, avoir un simple mécanisme ICMP pour trouver facilement des cibles potentielles peut se révéler être un risque supplémentaire (bien que mineur) pour la sécurité.

Le présent document ne définit aucun mécanisme d'authentification pour les messages de découverte dynamique d'adresse d'agent de rattachement. Donc, l'agent de rattachement ne peut pas vérifier l'adresse de rattachement du nœud mobile qui a demandé la liste des agents de rattachement.

À part la découverte de la ou des adresses des agents de rattachement, les attaquants ne vont pas être capables d'apprendre beaucoup à partir de ces informations, et les nœuds mobiles ne peuvent pas être amenés par ruse à utiliser de mauvais agents de rattachement, car toutes les autres communication avec les agents de rattachement sont sûres.

Dans les cas où une sécurité supplémentaire est nécessaire, on peut considérer à la place l'utilisation de l'amorçage MIPv6 [RFC5026] (fondée sur les enregistrements de ressource SRV du DNS [RFC2782]) en conjonction avec les mécanismes de sécurité suggérés dans ces spécifications. Dans cette solution, la sécurité est fournie par le cadre de sécurité du DNS (DNSSEC) [RFC4033]. Les données préconfigurées nécessaires sur le nœud mobile pour ce mécanisme sont le nom de domaine du fournisseur du service mobile, qui est marginalement meilleur que le préfixe de sous réseau de rattachement. Pour la sécurité, une ancre de confiance qui domine le domaine est nécessaire.

15.6 Découverte du préfixe mobile

La fonction de découverte de préfixe mobile peut laisser fuir aux espions des informations intéressantes sur la topologie du réseau et les durée de vies des préfixes ; pour cette raison, les demandes sur ces informations doivent être authentifiées. Les réponses et informations de préfixe non sollicitées doivent être authentifiées pour empêcher que les nœuds mobiles soient amenés à croire de fausses informations sur les préfixes et éventuellement empêcher les communications avec les adresses existantes. Facultativement, le chiffrement peut être appliqué pour empêcher les fuites d'informations de préfixes.

15.7 Tunnelage via l'agent de rattachement

Les tunnels entre le nœud mobile et l'agent de rattachement peuvent être protégés en assurant une utilisation appropriée des adresses de source, et une protection cryptographique facultative. Ces procédures sont discutées au paragraphe 5.5.

Les mises à jour de lien aux agents de rattachement sont sûres. Quand il reçoit le trafic tunnelé, l'agent de rattachement vérifie que l'adresse IP externe correspond à la localisation actuelle du nœud mobile. Ceci agit comme une forme faible de protection contre les paquets falsifiés qui paraissent venir du nœud mobile. Ceci est particulièrement utile, si aucune sécurité de bout en bout n'est appliquée entre le mobile et les nœuds correspondants. La vérification de l'adresse IP externe empêche les attaques où l'attaquant est contrôlé par un filtrage d'entrée. Cela empêche aussi les attaques où l'attaquant ne connaît pas l'adresse d'entretien actuelle du nœud mobile. Les attaquants qui connaissent l'adresse d'entretien et ne sont pas contrôlés par le filtrage d'entrée pourront encore envoyer du trafic à travers l'agent de rattachement. Ceci inclut les attaquants sur la même liaison locale que le nœud mobile. Mais de tels attaquants pourraient envoyer des paquets qui paraissent venir du nœud mobile sans attaquer le tunnel ; l'attaquant pourrait simplement envoyer des paquets avec l'adresse de source réglée à l'adresse de rattachement du nœud mobile. Cependant, cette attaque ne fonctionne pas si la destination finale du paquet est dans le réseau de rattachement, et certaines formes de défense de périmètre sont appliquées pour les paquets envoyés à ces destinations. Dans ce cas, il est recommandé que soit appliquée une sécurité de bout en bout ou une protection supplémentaire du tunnel, comme il est usuel dans les situations d'accès à distance.

Les agents de rattachement et nœuds mobiles peuvent utiliser IPsec ESP pour protéger les paquets de charge utile tunnelés entre eux. Ceci est utile pour protéger les communications contre des attaquants sur le chemin du tunnel.

Quand une adresse locale unique (ULA, *Unique-Local Address*) [RFC4086] est utilisée comme adresse de rattachement, le tunnelage inverse peut être utilisé pour envoyer le trafic local provenant d'une autre localisation. Les administrateurs devraient être conscients de cela quand ils permettent de telles adresses de rattachement. En particulier, la vérification de l'adresse IP externe décrite ci-dessus ne suffit pas contre tous les attaquants. L'utilisation de tunnels chiffrés est particulièrement utile pour ces sortes d'adresses de rattachement.

15.8 Option Adresse de rattachement

Quand le nœud mobile envoie les paquets directement au nœud correspondant, le champ Adresse de source de l'en-tête IPv6 du paquet est l'adresse d'entretien. Donc, le filtrage d'entrée [RFC2827] fonctionne de la manière usuelle même pour les nœuds mobiles, car l'adresse de source est topologiquement correcte. L'option Adresse de rattachement est utilisée pour informer le nœud correspondant de l'adresse de rattachement du nœud mobile.

Cependant, l'adresse d'entretien dans le champ Adresse de source ne survit pas dans les réponses envoyées par le nœud correspondant sauf si il a un lien pour ce nœud mobile. Aussi, tous les mécanismes de traçage d'un attaquant ne fonctionnent pas quand les paquets sont reflétés à travers les nœuds correspondants en utilisant l'option Adresse de rattachement. Pour ces raisons, la présente spécification restreint l'utilisation de l'option Adresse de rattachement. Elle peut seulement être utilisée quand un lien a déjà été établi avec la participation du nœud à l'adresse de rattachement, comme décrit aux paragraphes 5.5 et 6.3. Cela empêche les attaques en réflexion par l'utilisation de l'option Adresse de rattachement. Cela assure aussi que les nœuds correspondants répondent à la même adresse d'où le nœud mobile envoie le trafic.

Aucune authentification particulière de l'option Adresse de rattachement n'est exigée au delà de ce qui est mentionné ci-dessus, mais noter que si l'en-tête IPv6 d'un paquet est couvert par l'en-tête d'authentification IPsec, cette authentification couvre alors aussi l'option Adresse de rattachement. Donc, même quand l'authentification est utilisée dans l'en-tête IPv6, la

sécurité du champ Adresse de source dans l'en-tête IPv6 n'est pas compromise par la présence d'une option Adresse de rattachement. Sans authentification du paquet, tout champ de l'en-tête IPv6 incluant le champ Adresse de source ou toute autre partie du paquet et l'option Adresse de rattachement peut être falsifié ou modifié dans le transit. Dans ce cas, le contenu de l'option Adresse de rattachement n'est pas plus suspect qu'une autre partie du paquet.

15.9 En-tête d'acheminement de type 2

La définition de l'en-tête d'acheminement de type 2 est décrite au paragraphe 6.4. Cette définition et les règles de traitement associées ont été choisies de façon que l'en-tête ne puisse pas être utilisé pour ce qui est traditionnellement vu comme acheminement de source. En particulier, l'adresse de rattachement dans l'en-tête d'acheminement va toujours devoir être allouée à l'adresse de rattachement du nœud receveur ; sinon, le paquet sera éliminé.

Généralement, l'acheminement de source pose un certain nombre de problèmes de sécurité. Parmi eux figure l'inversion automatique de routes de source non authentifiés (ce qui est un problème pour IPv4, mais pas pour IPv6). Un autre problème est la capacité d'utiliser l'acheminement de source pour "sauter" entre nœuds à l'intérieur, aussi bien qu'à l'extérieur, d'un pare-feu. Ces problèmes de sécurité ne sont pas en cause dans IPv6 mobile, à cause des règles mentionnées ci-dessus.

Par nature, la sémantique de l'en-tête d'acheminement de type 2 est la même que la forme particulière de tunnelage de IP dans IP où les adresses de source interne et externe sont les mêmes.

Cela implique qu'un appareil qui met en œuvre le filtrage de paquets devrait être capable de distinguer entre un en-tête d'acheminement de type 2 et les autres en-têtes d'acheminement, comme exigé au paragraphe 8.3. Ceci est nécessaire afin de permettre le trafic IPv6 mobile tout en ayant encore l'option du filtrage des autres utilisations d'en-têtes d'acheminement.

15.10 SHA-1 est assez sûr pour les messages de contrôle IPv6 mobile

Le présent document s'appuie sur des codes d'authentification de message fondés sur le hachage (HMAC, *hash-based message authentication code*) calculés en utilisant l'algorithme de hachage SHA-1 [FIPS180-1] pour le jeton de génération de clé de rattachement et le jeton de génération de clé d'entretien, ainsi que les champs d'authentification dans les données de mise à jour de lien et d'autorisation de lien (voir au paragraphe 5.2.4). Bien que SHA-1 ait été déconseillé pour certains mécanismes cryptographiques, SHA-1 est considéré comme sûr pour le futur prévisible lorsque utilisé comme spécifié ici. Pour les détails, voir la [RFC6194].

16. Contributeurs

Le travail effectué par Tuomas Aura, Mike Roe, Greg O'Shea, Pekka Nikander, Erik Nordmark, et Michael Thomas a donné forme aux protocoles d'acheminement de retour décrits dans [35].

Des contributions significatives ont été faites par les membres de l'équipe de conception de la sécurité de IPv6 mobile, includant (par ordre alphabétique) Gabriel Montenegro, Pekka Nikander, et Erik Nordmark.

17. Remerciements

Nous tenons à remercier les membres des groupes de travail IP mobile, Extensions de mobilité pour IPv6, et IPng pour leurs commentaires et suggestions sur ce travail. Nous tenons particulièrement à remercier (par ordre alphabétique) Fred Baker, Josh Broch, Samita Chakrabarti, Robert Chalmers, Noel Chiappa, Jean-Michel Combes, Greg Daley, Vijay Devarapalli, Rich Draves, Francis Dupont, Ashutosh Dutta, Arnaud Ebalard, Wesley Eddy, Thomas Eklund, Jun-Ichiro Itojun Hagino, Brian Haley, Marc Hasson, John Ioannidis, James Kempf, Rajeev Koodli, Suresh Krishnan, Krishna Kumar, T.J. Kniveton, Joe Lau, Aime Le Rouzic, Julien Laganier, Jiwoong Lee, Benjamin Lim, Vesa-Matti Mantyla, Kevin Miles, Glenn Morrow, Ahmad Muhanna, Thomas Narten, Karen Nielsen, Simon Nybroe, David Oran, Mohan Parthasarathy, Basavaraj Patil, Brett Pentland, Lars Henrik Petander, Alexandru Petrescu, Mattias Petterson, Ken Powell, Ed Remmell, Phil Roberts, Patrice Romand, Luis A. Sanchez, Pekka Savola, Jeff Schiller, Arvind Sevalkar, Keiichi Shima, Tom Soderlund, Hesham Soliman, Jim Solomon, Tapio Suihko, Dave Thaler, Pascal Thubert, Benny Van Houdt, Jon-Olov Vatn, Ryuji Wakikawa, Kilian Weniger, Carl E. Williams, Vladislav Yasevich, Alper Yegin, et Xinhua Zhao, pour leur relecture détaillée des versions antérieures de ce document. Leurs suggestions ont aidé a améliorer la conception et la présentation du protocole.

Nous tenons aussi à remercier les participants à l'événement d'essai de IPv6 mobile (1999), les développeurs qui ont participé à l'essai d'interopérabilité IPv6 mobile à Connectathons (2000, 2001, 2002, et 2003) et les participants à l'essai d'interopérabilité de ETSI (2000, 2002). Finalement nous remercions le projet TAHI qui a fourni les suites d'essai pour IPv6 mobile.

18. Références

18.1 Références normatives

[FIPS180-1] National Institute of Standards and Technology, "Secure Hash Standard", FIPS PUB 180-1, avril 1995, <http://www.itl.nist.gov/fipspubs/fip180-1.ht >.

[RFC2104] H. Krawczyk, M. Bellare et R. Canetti, "HMAC : Hachage de clés pour l'authentification de message", février 1997.

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

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

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

[RFC2526] D. Johnson, S. Deering, "Adresses réservées d'envoi à la cantonade de sous-réseau IPv6", mars 1999. *(P.S.)*

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

[RFC2782] A. Gulbrandsen, P. Vixie et L. Esibov, "Enregistrement de ressource DNS pour la spécification de la localisation des services (DNS SRV)", février 2000.

[RFC3776] J. Arkko, V. Devarapalli, F. Dupont, "Utilisation de IPsec pour la protection de la signalisation IPv6 mobile entre nœuds mobiles et agents nominaux", juin 2004. (*MàJ par* RFC4877) *(P.S.)*

[RFC4033] R. Arends, et autres, "Introduction et exigences pour la sécurité du DNS", mars 2005.

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

[RFC4193] R. Hinden, B. Haberman, "Adresses IPv6 en envoi individuel uniques localement", octobre 2005. *(P.S.)*

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

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

[RFC4302] S. Kent, "En-tête d'authentification IP", décembre 2005. *(P.S.)*

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

[RFC4443] A. Conta et autres, "Spécification du protocole de message de contrôle Internet (ICMPv6) pour la version 6 du protocole Internet (IPv6)", mars 2006. (*Remplace* RFC2463) (*MàJ* RFC2780) (*MàJ par* RFC4884) *(D.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)

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

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

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

[RFC5026] G. Giaretta et autres, "Amorçage IPv6 mobile dans un scénario de partage", octobre 2007. *(P.S.)*

[RFC5226] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, mai 2008. (*Remplace* RFC2434 *; remplacée par* RFC8126)

[RFC5996] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, "Protocole d'échange de clés sur Internet, version 2 (IKEv2)", septembre 2010 (*Remplace* RFC4306, RFC4718) (*MàJ par* RFC5998) ; *remplacée par* RFC7296 *(STD79)*

18.2 Références pour information

[RFC2003] C. Perkins, "Encapsulation de IP dans IP", octobre 1996. (*MàJ par* RFC 3168, RFC 6864) *(P.S.)*

[RFC2004] C. Perkins, "Encapsulation minimale au sein de IP", octobre 1996. *(P.S.)*

[RFC2827] P. Ferguson, D. Senie, "Filtrage d'entrée de réseau : Combattre les attaques de déni de service qui utilisent l'usurpation d'adresse de source IP", mai 2000. (*MàJ par* RFC3704) (BCP0038)

[RFC3232] J. Reynolds, "Numéros alloués : la RFC 1700 est remplacée par une base de données en ligne", janvier 2002.

[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, RFC6644, RFC7227 *; rendue obsolète par* RFC8415)

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

[RFC3627] P. Savola, "L'utilisation de la longueur de préfixe /127 est considérée comme dommageable entre routeurs", septembre 2003. *(Historique)*

[RFC3753] J. Manner et M. Kojo, éd., "Terminologie de la mobilité", juin 2004. *(Information)*

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

[RFC4107] S. Bellovin, R. Housley, "Lignes directrices pour la gestion des clés de chiffrement", juin 2005. (BCP0107)

[RFC4225] P. Nikander et autres, "Fondements des concepts de sécurité de l'optimisation de l'acheminement d'IPv6 mobile", décembre 2005. *(Information)*

[RFC5014] E. Nordmark et autres, "API de prises IPv6 pour la sélection d'adresse de source", septembre 2007. *(Information)*

[RFC5095] J. Abley, P. Savola, G. Neville-Neil "En-têtes d'acheminement de type 0 déconseillés dans IPv6**",** décembre 2007. *(P.S.)*

[RFC5944] C. Perkins, "Prise en charge de la mobilité sur IP pour IPv4, révisée", novembre 2010. (*Remplace RFC*3344) *(P.S.)*

[RFC6194] T. Polk et autres, "Considérations sur la sécurité pour les algorithmes de résumé de message SHA-0 et SHA-1", mars 2011. *(Information)*

[RFC6611] K. Chowdhury, A. Yegin, "Amorçage de IPv6 mobile (MIPv6) pour le scénario intégré", mai 2012. *(P.S.)*

[28] Aura, T. et J. Arkko, "MIPv6 BU Attacks et Defenses", Travail en cours, mars 2002.

[29] Krishnan, S. et G. Tsirtsis, "MIPv6 Home Link Detection", Travail en cours, mars 2008.

[34] Nordmark, E., "Securing MIPv6 BUs using return routability (BU3WAY)", Travail en cours, novembre 2001.

[35] Roe, M., "Authentication of IPv6 mobile mises à jour de lien et Acknowledgments", Travail en cours, mars 2002.

[38] Savola, P., "Security of IPv6 Routing Header and Adresse de rattachement Options", Travail en cours, mars 2002.

Appendice A Extensions futures

A.1 Portage

Le présent document ne spécifie pas comment porter les paquets de charge utile sur les messages relatifs au lien. Cependant, il est envisagé que ce puisse être spécifié dans un document séparé quand des questions comme l'interaction entre portage et IPsec seront pleinement résolues (voir aussi en A.3). Les messages d'acheminement de retour pourront indiquer la prise en charge du portage avec une nouvelle option de mobilité.

A.2 Acheminement triangulaire

Du fait de la crainte d'ouvrir la voie à des attaques en réflexion avec l'option de destination Adresse de rattachement, la présente spécification exige que cette option soit vérifiée dans l'antémémoire de liens, c'est-à-dire., il doit y avoir une entrée d'antémémoire de liens pour l'adresse de rattachement et l'adresse d'entretien.

De futures extensions pourront être spécifiées pour permettre l'utilisation d'options de destination Adresse de rattachement non vérifiées d'une façon qui n'introduise pas de problème de sécurité.

A.3 Nouvelles méthodes d'autorisation

Alors que la procédure d'acheminement de retour fournit un bon niveau de sécurité, il existe des méthodes qui ont des niveaux de sécurité plus élevés. Ensuite, comme exposé au paragraphe 15.4, de futures améliorations de la sécurité de IPv6 pourront causer un besoin d'améliorer aussi la sécurité de la procédure d'acheminement de retour. Utiliser IPsec comme seule méthode pour autoriser les mises à jour de lien aux nœuds correspondants est aussi possible. La protection de l'en-tête de mobilité à cette fin est aisée, bien qu'on doive s'assurer que la SA IPsec a été créée avec l'autorisation appropriée d'utiliser l'adresse de rattachement référencée dans la mise à jour de lien. Par exemple, un certificat utilisé par IKEv2 pour créer l'association de sécurité pourrait contenir l'adresse de rattachement. Une future spécification pourra préciser cela.

A.4 Extensions de découverte de voisin

De futures spécifications pourront améliorer l'efficacité des tâches de découverte de voisin, ce qui pourrait aider dans les mouvements rapides. Un facteur est actuellement examiné : les délais causés par le mécanisme de détection d'adresse dupliquée. Actuellement, la détection d'adresse dupliquée doit être effectuée pour chaque nouvelle adresse d'entretien lorsque le nœud mobile se déplace, et pour l'adresse de liaison locale du nœud mobile sur chaque nouvelle liaison. En particulier, le besoin et les compromis de refaire la détection d'adresse dupliquée pour l'adresse de liaison locale chaque fois que le nœud mobile passe sur de nouvelles liaisons devront être examinés. Des améliorations dans ce domaine sont cependant généralement applicables et progressent indépendamment de la spécification IPv6 mobile.

De futures améliorations fonctionnelles pourront aussi être pertinentes pour IPv6 mobile et d'autres applications. Par exemple, des mécanismes qui permettraient la récupération d'une collision de détection d'adresse dupliquée seraient utiles pour les adresses de liaison locale, d'entretien, et de rattachement.

Appendice B Changements depuis la RFC3775

Le questions suivantes ont été identifiées durant l'évolution du document actuel. Des discussions sur la plupart des questions se trouvent sur la page de la Toile du groupe de travail [mext] à http://trac.tools.ietf.org/wg/mext/trac/report/6

Question n° 1 : dernier SQN accepté [Ahmad Muhanna]. Solution : spécifier que le nœud mobile met à jour son numéro de séquence de lien pour correspondre au numéro de séquence donné dans l'accusé de réception de lien (si l'accusé de réception de lien passe correctement l'authentification et si l'état est 135 (numéro de séquence hors de fenêtre). Voir au paragraphe 11.7.3.

Question n° 4 : supprime les références aux adresses de site local [George Tsirtsis]. Corrigé.

Question n° 5 : mauvais numéro de protocole (2 au lieu de 135) utilisé dans la discussion sur le pseudo en-tête de contrôle. Corrigé. Voir au paragraphe 6.1.1.

Question n° 8 : application utilisant l'adresse d'entretien [Julien Laganier]. Cite l'API de prise IPv6 pour la spécification de choix d'adresse de source [RFC5014]. Voir au paragraphe 11.3.4.

Question n° 10 : usage de la "durée de vie de HA" [Ryuji Wakikawa]. Le nœud mobile DEVRAIT mémoriser la liste des agents de rattachement pour utilisation ultérieure dans le cas où l'agent de rattachement qui gère actuellement la transmission de l'adresse d'entretien du nœud mobile deviendrait indisponible. Voir au paragraphe 11.4.1.

Question n° 11 : désenregistrement au retour chez lui [Vijay Devarapalli]. Pour être capable d'envoyer et recevoir des paquets en utilisant son adresse de rattachement à partir de la liaison de rattachement, le nœud mobile DOIT envoyer une mise à jour de lien à son agent de rattachement pour lui dire de ne plus intercepter ou tunneler les paquets pour lui. Jusqu'à ce que le nœud mobile envoie une telle mise à jour de lien de désenregistrement, il NE DOIT PAS tenter d'envoyer et recevoir des paquets en utilisant son adresse de rattachement à partir de la liaison de rattachement. Voir au paragraphe 11.5.5.

Question #12 : BErr envoyée par le HA aussi, pas seulement par le CN [Alexandru Petrescu]. Corrigé. Voir au 4.2.

Question n° 13 : détection de liaison de rattachement [Suresh Krishnan]. Proposition : Ajouter le paragraphe 11.5.2 pour la détection de liaison de rattachement, d'après "Détection de liaison de rattachement MIPv6" [29].

Question n° 14 : références à l'amorçage [Vijay Devarapalli]. Cite "Amorçage IPv6 mobile dans le scénario partagé" [RFC5026] et "Amorçage MIP6 pour le scénario intégré" [RFC6611]. Voir au paragraphe 4.1.

Question n° 17 : le nœud mobile multi rattachements peut causer une boucle d'acheminement entre les agents de rattachement [Benjamin Lim]. Ajout d'un conseil de sécurité au paragraphe 15.1, pour souligner le risque de boucle d'acheminement parmi les HA (par exemple, in 3GPP) : un nœud mobile malveillant associé à plusieurs agents de rattachement pourrait créer une boucle d'acheminement entre eux. Cela se produirait quand un nœud mobile lie une adresse de rattachement située sur un premier agent de rattachement à une autre adresse de rattachement sur un second agent de rattachement.

Question n° 18 : questions concernant l'option Adresse de rattachement et ICMP / Erreurs de lien [Fabian Mauchle].
Proposition : Utiliser la valeur dans le champ Prochain en-tête {50 (ESP), 51 (AH), 135 (En-tête de mobilité)} pour déterminer si une entrée d'antémémoire de liens est requise. Voir au paragraphe 9.3.1.
Proposition : Si le message Erreur de lien a été envoyé par l'agent de rattachement, le nœud mobile DEVRAIT envoyer une mise à jour de lien à l'agent de rattachement conformément au paragraphe 11.7.1. Voir au paragraphe 11.3.6.

Question n° 19 : condition de compétition de désenregistrement de BU [Kilian Weniger]. Un problème survient si le désenregistrement arrive chez l'agent de rattachement avant une mise à jour de lien immédiatement précédente.
Solution : l'agent de rattachement retarde la suppression de BCE après l'envoi de l'accusé de réception de lien. Voir au paragraphe 10.3.2.

Question n° 6 : corrections et mises à jour rédactionnelles mineures.
Mise à jour des références à IPsec et IKE sur l'architecture IPsec et IKEv2 révisée.
Mise à jour de HMAC_SHA1 [RFC2104] en normative au lieu de pour information.
Inclusion de la discussion (voir au paragraphe 15.10) pour informer les mises en œuvre que HMAC_SHA1 est considéré offrir une protection suffisante pour les messages de contrôle tels qu'exigés par IPv6 mobile.

Adresse des auteurs

David B. Johnson
Rice University
Dept. of Computer Science, MS 132
6100 Main Street
Houston TX 77005-1892
USA
mél : dbj@cs.rice.edu

Charles E. Perkins (éditeur)
Tellabs, Inc.
4555 Great America Parkway, Suite 150
Santa Clara CA 95054
USA
mél : charliep@computer.org

Jari Arkko
Ericsson
Jorvas 02420
Finland
mél : jari.arkko@ericsson.com