Groupe de travail Réseau
Request for Comments : 5555
Catégorie : Sur la voie de la normalisation

H. Soliman, éd., Elevate Technologies
mai 2009
Traduction Claude Brière de L'Isle

Prise en charge par IPv6 mobile des hôtes et routeurs double pile

Statut du présent mémoire

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

Résumé

Les spécifications actuelles de IPv6 mobile et de mobilité du réseau (NEMO, *IPv6 mobile and Network Mobility*) prennent en charge seulement IPv6. La présente spécification étend ces normes pour permettre l'enregistrement d'adresses et préfixes IPv4, respectivement, et le transport de paquets IPv4 et IPv6 sur le tunnel à l'agent de rattachement. La présente spécification permet aussi au nœud mobile l'itinérance sur IPv6 et IPv4, y compris les cas où une traduction d'adresse réseau est présente sur le chemin entre le nœud mobile et son agent de rattachement.

Table des matières

1. Introduction

IPv6 mobile [RFC3775] et NEMO [RFC3963] permettent aux nœuds mobiles de se déplacer au sein de l'Internet tout en conservant l'accessibilité et les sessions en cours, en utilisant une adresse ou préfixe de rattachement IPv6. Cependant, comme IPv6 n'est pas largement déployé, il est peu probable que les nœuds mobiles utilisent initialement seulement des adresses IPv6 pour leurs connexions. Il est raisonnable de supposer que les nœuds mobiles vont, pendant longtemps, avoir besoin d'une adresse de rattachement IPv4 qui puisse être utilisée par les couches supérieures. Il est aussi raisonnable de supposer que les nœuds mobiles vont se déplacer sur des réseaux qui pourraient ne pas prendre en charge IPv6 et auraient donc besoin de la capacité de prendre en charge une adresse d'entretien IPv4. Donc, la présente spécification étend les capacités de IPv6 mobile pour permettre à des nœuds mobiles double piles de demander que leur agent de rattachement (aussi double piles) tunnelle les paquets IPv4/IPv6 adressés à leurs adresses de rattachement, ainsi que leurs adresses d'entretien IPv4/IPv6.

En utilisant la présente spécification, les nœuds mobiles vont seulement avoir besoin de IPv6 mobile et de la [RFC3963] pour gérer la mobilité lorsque ils se déplacent au sein de l'Internet, éliminant donc le besoin de faire fonctionner simultanément deux protocoles de gestion de la mobilité. La présente spécification fournit les extensions nécessaires afin de permettre que des nœuds mobiles double piles utilisent seulement la mobilité IPv6.

La présente spécification va aussi considérer les cas où un nœud mobile se déplace dans un réseau privé IPv4 et est configuré avec une adresse d'entretien IPv4 privée. Dans ces scénarios, le nœud mobile doit être capable de traverser le NAT IPv4 afin de communiquer avec l'agent de rattachement. La traversée de NAT IPv4 pour IPv6 mobile est présentée dans la présente spécification.

Dans la présente spécification, le terme de "nœud mobile" se réfère à l'hôte mobile et à un routeur mobile sauf si la discussion est spécifique des hôtes ou des routeurs. De même, on utilise le terme "adresse de rattachement" pour refléter un format d'adresse/préfixe. Noter que les fonctions d'hôte mobile et de routeur ont déjà été définies dans la [RFC3775] et la [RFC3963], respectivement. La présente spécification ne change pas ces comportements déjà définis, ni n'étend les types spécifiques d'hôtes et de routeurs déjà définis, avec les deux exceptions suivantes : (i) permettre au nœud mobile de communiquer avec son agent de rattachement même sur des réseaux IPv4, et (ii) permettre l'utilisation d'adresses et préfixes IPv4 de rattachement.

Dans la présente spécification, les extensions sont définies pour la mise à jour de lien et l'accusé de réception de lien. On devrait noter que toutes ces extensions s'appliquent aux cas où le nœud mobile communique avec un point d'ancrage de mobilité (MAP, *Mobility Anchor Point*) comme défini dans la [RFC5380]. Les exigences sur le MAP sont identiques à celles déclarées pour l'agent de rattachement ; cependant, il est peu probable que la traversée de NAT soit nécessaire avec un MAP, car il est supposé être dans le même domaine d'adresse.

1.1 Notation des exigences

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

1.2 Motifs de l'utilisation de IPv6 mobile seul

IPv6 offre un certain nombre d'améliorations sur l'IPv4 d'aujourd'hui, principalement parce que son grand espace d'adresses IPv6 mobile offre un certain nombre d'améliorations sur IPv4 mobile [RFC3344], principalement à cause des capacités héritées de IPv6. Par exemple, l'optimisation de chemin et la découverte dynamique d'agent de rattachement peuvent seulement être réalisées avec IPv6 mobile.

Un des avantages du grand espace d'adresses fourni par IPv6 est qu'il permet aux nœuds mobiles d'obtenir une adresse d'entretien unique au monde où qu'ils soient. Donc, il n'y a pas besoin des techniques de traversée de traducteur d'adresse réseau (NAT, *Network Address Translator*) conçues pour IPv4 mobile. Cela permer à IPv6 mobile d'être un protocole de gestion de la mobilité significativement plus simple et plus efficace en bande passante. En même temps, durant la transition vers IPv6, la traversée de NAT pour les réseaux privés IPv4 existants doit être considérée. La présente spécification

introduit la traversée de NAT à cette fin.

Les avantages ci-dessus concernent le cas d'utilisation seulement de IPv6 mobile pour les nœuds mobiles à double piles, car cela permet une solution de mobilité à long terme. L'utilisation de IPv6 mobile pour la mobilité à double piles élimine le besoin de changer la solution de mobilité à cause de l'introduction de IPv6 au sein d'un réseau déployé.

1.3 Scénarios considérés par la présente spécification

Il y a plusieurs scénarios qui illustrent les potentielles incompatibilités pour les nœuds mobiles qui utilisent IPv6 mobile. Certains des problèmes associés à la mobilité et les problèmes de transition ont été présentés dans la [RFC4977]. La présente spécification considère les scénarios qui visent tous les problèmes discutés dans la [RFC4977]. Les scénarios considérés dans la présente spécification sont énumérés ci-dessous.

Tous les scénarios qui suivent supposent que le nœud mobile et l'agent de rattachement sont à capacité IPv4 et IPv6 et que seul IPv6 mobile est utilisé entre le nœud mobile et l'agent de rattachement. On suppose aussi que l'agent de rattachement est toujours accessible par une adresse IPv4 unique au monde. Finalement, il est important de noter que les scénarios suivants ne sont pas mutuellement exclusifs.

Scénario 1 : réseau étranger IPv4 seulement
Dans ce scénario, un nœud mobile est connecté à un réseau étranger IPv4 seulement. Le nœud mobile peut seulement configurer une adresse d'entretien IPv4.

Scénario 2 : nœud mobile derrière un NAT
Dans ce scénario, le nœud mobile est dans un réseau étranger privé IPv4 qui a un appareil de NAT qui le connecte à l'Internet. Si l'agent de rattachement est situé en dehors de l'appareil de NAT, le nœud mobile va avoir besoin d'un mécanisme de traversée de NAT pour communiquer avec l'agent de rattachement.

On devrait noter que la [RFC5389] souligne les problèmes de certains types de NAT qui agissent comme une passerelle générique de niveau application (ALG, *Application Level Gateway*) et réécrivent tout champ de 32 bits qui contient les adresses IP publiques du NAT. La présente spécification ne prend pas en charge de tels NAT.

Scénario 3 : agent de rattachement derrière un NAT.
Dans ce scénario, la communication entre le nœud mobile et l'agent de rattachement est de plus compliquée par le fait que l'agent de rattachement est situé dans un réseau IPv4 privé. Cependant, dans ce scénario, on suppose qu'une adresse IPv4 unique au monde est allouée à l'agent de rattachement. L'adresse ne pourrait pas être configurée physiquement sur l'interface de l'agent de rattachement. Elle est plutôt associée à l'agent de rattachement sur l'appareil de traduction d'accès à l'adresse réseau (NAPT, *Network Address Port Translation*) qui permet à l'agent de rattachement d'être accessible à travers une transposition d'adresse ou d'accès.

Scénario 4 : utilisation d'applications IPv4 seulement.
Dans ce scénario, le nœud mobile peut être situé dans un réseau IPv4, IPv6, ou duel. Cependant, le nœud mobile pourrait être en communication avec un nœud seulement IPv4. Dans ce cas, le nœud mobile va avoir besoin d'une adresse IPv4 stable pour son application. La solution de remplacement à l'utilisation d'une adresse IPv4 est d'utiliser des traducteurs de protocole ; cependant, la communication de bout en bout avec IPv4 est préférée à l'utilisation de traducteurs de protocole.

Le nœud mobile peut aussi être en communication avec une application seulement IPv4 qui exige une adresse IPv4.

Les cas ci-dessus illustrent le besoin d'allocation d'une adresse de rattachement IPv4 stable au nœud mobile. Ceci est fait en utilisant une adresse de rattachement IPv4. Comme faire fonctionner simultanément IPv4 mobile et IPv6 mobile est problématique (comme illustré dans la [RFC4977]) ce scénario ajoute l'exigence que IPv6 mobile prenne en charge les adresse de rattachement IPv4.

Scénario 5 : réseaux à capacité IPv6 et IPv4.
Dans ce scénario, le nœud mobile devrait préférer l'utilisation d'une adresse d'entretien IPv6 pour son adresse de rattachement IPv6 ou IPv4. Le tunnelage normal IP dans IP devrait être utilisé dans ce scénario comme décrit dans la [RFC3775]. Dans de rares exceptions, lorsque le tunnelage IP dans IP pour IPv6 ne permet pas au nœud mobile de joindre l'agent de rattachement, le nœud mobile suit l'algorithme d'envoi décrit au paragraphe 4.4.1. Le tunnelage UDP dans les réseaux IPv6 est proposé dans le présent document comme mécanisme en dernier ressort quand l'accessibilité ne peut pas être réalisée par le tunnelage normal IP dans IP. Ce ne devrait pas être vu comme un mode de fonctionnement normal et ne devrait pas être utilisé en premier lieu.

2. Vue d'ensemble de la solution

Afin de permettre à IPv6 mobile d'être utilisé par les nœuds mobiles double piles, on doit faire ce qui suit :

- Les nœuds mobiles devraient être capables d'utiliser simultanément les adresses IPv4 et IPv6 de rattachement ou d'entretien et de mettre à jour leurs agents de rattachement en conséquence.

- Les nœuds mobiles doivent être capables de connaître l'adresse IPv4 de l'agent de rattachement ainsi que son adresse IPv6. Il n'y a cependant pas besoin de découverte de préfixe IPv4.

- Les nœuds mobiles doivent être capables de détecter la présence d'un appareil de NAT et de le traverser afin de communiquer avec l'agent de rattachement.

Cette Section présente une vue d'ensemble des extensions requises afin de permettre aux nœuds mobiles d'utiliser seulement IPv6 mobile pour la gestion de la mobilité IP.

2.1 Découverte de l'adresse de l'agent de rattachement

La découverte dynamique d'adresse d'agent de rattachement (DHAAD, *Dynamic Home Agent Address Discovery*) est définie dans la [RFC3775] pour permettre aux nœuds mobiles de découvrir leurs agents de rattachement en ajoutant un identifiant d'interface d'envoi à la cantonade bien connue à leur préfixe de liaison de rattachement. Cependant, ce mécanisme est fondé sur un acheminement d'envoi à la cantonade IPv6. Si un nœud mobile (MN) est situé dans un réseau étranger seulement IPv4, il ne peut pas s'appuyer sur l'acheminement IPv6 natif. Dans ce scénario, la solution pour découvrir l'adresse IPv4 de l'agent de rattachement est par le système des noms de domaine (DNS, *Domain Nom System*). Si le MN est rattaché à un réseau seulement IPv6 ou double piles, il peut aussi utiliser les procédures définies dans la [RFC6611] pour découvrir les informations d'agent de rattachement. Noter que l'utilisation de la [RFC6611] ne peut pas donner au nœud mobile les informations qui lui permettent de communiquer avec l'agent de rattachement si le nœud mobile est situé dans un réseau IPv4 seulement. Dans ce scénario, le nœud mobile doit découvrir l'adresse IPv4 de son agent de rattachement par le DNS.

Pour une recherche dans le DNS par nom, le nœud mobile devrait être configuré avec le nom de l'agent de rattachement. Quand le nœud mobile a besoin de découvrir un agent de rattachement, il envoie une demande au DNS avec le QNAME réglé au nom configuré. Un exemple est "ha1.exemple.com". Si un agent de rattachement a une adresse IPv4 et IPv6, l'enregistrement correspondant du DNS devrait être configuré avec des enregistrements "AAAA" et "A". En conséquence, la réponse du DNS va contenir les enregistrements "AAAA" et "A".

Pour une recherche dans le DNS par service, l'enregistrement SRV défini dans la [RFC5026] est réutilisé. Par exemple, si le nom de service est "mip6" et si le nom de protocole est "ipv6" dans l'enregistrement SRV, le nœud mobile DEVRAIT envoyer une demande au DNS avec le QNAME réglé à "_mip6._ipv6.exemple.com". La réponse devrait contenir le ou les FQDN de l'agent de rattachement et peut inclure aussi les enregistrements "AAAA" et "A" correspondants.

Si plusieurs agents de rattachement résident sur la liaison de rattachement, chacun configuré avec une adresse IPv4 publique, alors l'opération ci-dessus s'applique. Les entrées de DNS correctes peuvent être configurées en conséquence.

2.2 Sollicitation et annonce de préfixe mobile

Conformément à la [RFC3775], le nœud mobile peut envoyer une sollicitation de préfixe mobile et recevoir une annonce de préfixe mobile contenant tous les préfixes annoncés sur la liaison de rattachement.

Un nœud mobile double piles PEUT envoyer un message Sollicitation de préfixe mobile encapsulé dans IPv4 (c'est-à-dire, IPv6 dans IPv4) dans le cas où le nœud mobile n'a pas accès à IPv6 dans le réseau local. Sécuriser ces messages exige que le nœud mobile ait une association de sécurité avec l'agent de rattachement, en utilisant IPsec et sur la base de l'adresse d'entretien IPv4 du nœud mobile, comme décrit dans les [RFC3775] et [RFC4877].

La [RFC3775] exige que le nœud mobile inclue l'option Adresse de rattachement dans le message de sollicitation envoyé à l'agent de rattachement. Si le nœud mobile est situé dans un réseau IPv4, il ne va pas lui être alloué une adresse IPv6 à inclure dans l'adresse de source. Dans ce cas, le nœud mobile DOIT utiliser son adresse de rattachement dans le champ

Adresse de source du paquet IPv6, en plus d'utiliser l'option Adresse de rattachement comme attendu par la [RFC3775].

2.3 Gestion de lien

Un nœud mobile double pile va avoir besoin de mettre à jour son agent de rattachement avec son adresse d'entretien. Si un nœud mobile a une adresse de rattachement IPv4 et IPv6, il va devoir créer une entrée d'antémémoire de lien pour chaque adresse. Le format du paquet IP portant les messages de mise à jour de lien et d'accusé de réception va varier selon que le nœud mobile a ou non accès à IPv6 dans le réseau visité. Il y a trois scénarios différents à considérer à l'égard du réseau visité :

- o le réseau visité a la connexité IPv6 et fournit au nœud mobile une adresse d'entretien (à états pleins ou sans état) ;
- o le nœud mobile peut seulement configurer une adresse IPv4 unique au monde dans le réseau visité ;
- o le nœud mobile peut seulement configurer une adresse IPv4 privée dans le réseau visité.

2.3.1 Réseau étranger prenant en charge IPv6

Dans ce cas, le nœud mobile est capable de configurer une adresse IPv6 unique au monde. Le nœud mobile va envoyer une mise à jour de lien à l'adresse IPv6 de son agent de rattachement, comme défini dans la [RFC3775]. La mise à jour de lien PEUT inclure l'option Adresse de rattachement IPv4 introduite dans le présent document. Après réception de la mise à jour de lien, l'agent de rattachement crée deux entrées d'antémémoire de lien : une pour l'adresse IPv4 de rattachement du nœud mobile et une autre pour l'adresse de rattachement IPv6 du nœud mobile. Les deux entrées vont pointer sur l'adresse d'entretien IPv6 du nœud mobile. Donc, chaque fois qu'un paquet est adressé à l'adresse de rattachement IPv4 ou IPv6 du nœud mobile, l'agent de rattachement va le tunneler dans IPv6 à l'adresse d'entretien IPv6 du nœud mobile qui est incluse dans la mise à jour de lien. Effectivement, le nœud mobile établit deux tunnels différents, un pour son trafic IPv4 (IPv4 dans IPv6) et un pour son trafic IPv6 (IPv6 dans IPv6) avec une seule mise à jour de lien.

Dans ce scénario, le présent document étend la [RFC3775] en incluant l'option Adresse de rattachement IPv4 dans le message de mise à jour de lien. De plus, si le réseau prend en charge IPv4 et IPv6, ou si le nœud mobile rencontre des problèmes avec le tunnelage IP dans IP, le présent document propose des actions d'atténuation comme décrit au paragraphe 4.4.1.

Après avoir accepté la mise à jour de lien et créé les entrées d'antémémoire de lien correspondantes, l'agent de rattachement DOIT envoyer un accusé de réception de lien au nœud mobile comme défini dans la [RFC3775]. De plus, si la mise à jour de lien incluse dans l'option Adresse de rattachement IPv4, l'accusé de réception de lien DOIT inclure l'option Accusé de réception d'adresse IPv4 comme décrit au paragraphe 3.2.1. Cette option informe le nœud mobile de si le lien a été accepté pour l'adresse de rattachement IPv4. Si cette option n'est pas incluse dans l'accusé de réception de lien et si l'option Adresse de rattachement IPv4 était incluse dans la mise à jour de lien, le nœud mobile DOIT supposer que l'agent de rattachement ne prend pas en charge l'option Adresse de rattachement IPv4 et donc NE DEVRAIT PAS inclure l'option dans les futures mises à jour de lien à cette adresse d'agent de rattachement.

Quand un nœud mobile acquiert des adresses d'entretien IPv4 et IPv6 sur le réseau étranger, il DEVRAIT donner la priorité à l'adresse d'entretien IPv6 pour son lien MIPv6 comme décrit au paragraphe 4.4.1.

2.3.2 Réseau étranger prenant en charge seulement IPv4

Si le nœud mobile est dans un réseau étranger qui prend seulement en charge IPv4, il doit détecter si un NAT est dans son chemin de communication à l'agent de rattachement. Ceci est fait lors de l'échange des messages de mise à jour de lien et d'accusé de réception comme montré plus loin dans le présent document. La détection de NAT est nécessaire pour les besoins de signalisation présentés dans la présente spécification.

2.3.2.1 Réseau étranger prenant en charge seulement IPv4 (adresses publiques)

Dans ce scénario, le nœud mobile va devoir tunneler les paquets IPv6 contenant la mise à jour de lien à l'adresse IPv4 de l'agent de rattachement. Le nœud mobile utilise l'adresse IPv4 qu'il a obtenue du réseau étranger comme adresse de source dans l'en-tête externe. La mise à jour de lien va contenir l'adresse de rattachement IPv6 du nœud mobile. Cependant, comme l'adresse d'entretien dans ce scénario est l'adresse IPv4 du nœud mobile, le nœud mobile DOIT inclure son adresse d'entretien IPv4 dans le paquet IPv6. L'adresse IPv4 est représentée dans l'option Adresse d'entretien IPv4 définie dans la présente spécification. Si le nœud mobile avait une adresse de rattachement IPv4, il DOIT aussi inclure l'option Adresse de rattachement IPv4 décrite dans la présente spécification.

Après avoir accepté la mise à jour de lien, l'agent de rattachement DOIT créer une nouvelle entrée d'antémémoire de lien pour l'adresse de rattachement IPv6 du nœud mobile. Si une option Adresse de rattachement IPv4 est incluse, l'agent de rattachement DOIT créer une autre entrée pour cette adresse. Toutes les entrées DOIVENT pointer sur l'adresse d'entretien IPv4 du nœud mobile. Donc, tous les paquets adressés à la ou aux adresses de rattachement (IPv4 ou IPv6) du nœud mobile vont être encapsulés dans un en-tête IPv4 qui inclut l'adresse IPv4 de l'agent de rattachement dans le champ Adresse de source et l'adresse d'entretien IPv4 du nœud mobile dans le champ Adresse de destination.

Après avoir accepté les mises à jour de lien et créé les entrées correspondantes, l'agent de rattachement DOIT envoyer un accusé de réception de lien comme spécifié dans la [RFC3775]. De plus, si la mise à jour de lien incluait une option Adresse de rattachement IPv4, l'accusé de réception de lien DOIT inclure l'option Accusé de réception d'adresse IPv4 comme décrit au paragraphe 3.2.1. L'accusé de réception de lien est encapsulé dans l'adresse d'entretien IPv4, qui était incluse dans le champ Adresse de source de l' en-tête IPv4 encapsulant la mise à jour de lien.

2.3.2.2 Réseau étranger prenant en charge seulement IPv4 (adresses privées)

Dans ce scénario, le nœud mobile va devoir tunneler les paquets IPv6 contenant la mise à jour de lien à l'adresse IPv4 de l'agent de rattachement. Afin de traverser l'appareil de NAT, les paquets IPv6 sont tunnelés en utilisant UDP et IPv4. L'accès UDP alloué à l'agent de rattachement est 4191 (dsmipv6).

Le nœud mobile utilise l'adresse IPv4 qu'il obtient du réseau visité comme une adresse de source dans l'en-tête IPv4. La mise à jour de lien va contenir l'adresse de rattachement IPv6 du nœud mobile.

Après avoir accepté la mise à jour de lien, l'agent de rattachement DOIT créer une nouvelle entrée d'antémémoire de lien pour l'adresse de rattachement IPv6 du nœud mobile. Si une option Adresse de rattachement IPv4 est incluse, l'agent de rattachement DOIT créer une autre entrée pour cette adresse. Toutes les entrées DOIVENT pointer sur l'adresse d'entretien IPv4 du nœud mobile incluse dans l'adresse de source de l'en-tête IPv4 qui a encapsulé le message de mise à jour de lien. De plus, le tunnel utilisé DOIT indiquer l'encapsulation UDP pour la traversée de NAT. Donc, tous les paquets adressés à la ou aux adresses de rattachement (IPv4 ou IPv6) du nœud mobile vont être encapsulés dans UDP et ensuite encapsulés dans un en-tête IPv4 qui inclut l'adresse IPv4 de l'agent de rattachement dans le champ Adresse de source et l'adresse d'entretien IPv4 du nœud mobile dans le champ Adresse de destination. Noter que l'agent de rattachement DOIT mémoriser les numéros d'accès de source UDP contenus dans le paquet portant la mise à jour de lien afin d'être capable de transmettre les paquets au nœud mobile.

Après avoir accepté les mises à jour de lien et créé les entrées correspondantes, l'agent de rattachement DOIT envoyer un accusé de réception de lien comme spécifié dans la [RFC3775]. De plus, si la mise à jour de lien incluait une option Adresse de rattachement IPv4, l'accusé de réception de lien DOIT inclure l'option Accusé de réception d'adresse IPv4 comme décrit plus loin dans la présente spécification. L'accusé de réception de lien est encapsulé dans UDP et ensuite dans IPv4 avec l'adresse IPv4 de l'agent de rattachement dans le champ Adresse de source et l'adresse d'entretien IPv4 du nœud mobile dans le champ Destination. L'adresse IPv4 dans le champ Destination du paquet IPv4 est l'adresse de source qui a été reçue dans l'en-tête IPv4 contenant le message de mise à jour de lien. Le paquet IPv6 interne va contenir l'adresse IPv6 de l'agent de rattachement comme adresse de source et l'adresse de rattachement IPv6 du nœud mobile dans le champ Adresse de destination.

Le nœud mobile doit conserver les liens de NAT pour son adresse d'entretien IPv4 courante. Cela est fait par l'envoi régulier de mises à jour de lien à l'agent de rattachement.

2.4 Optimisation de chemin

L'optimisation de chemin, comme spécifié dans la [RFC3775], va opérer de manière identique pour les nœuds mobiles double piles quand ils sont situés dans un réseau visité qui fournit des adresses IPv6 au nœud mobile et lorsque il communique avec un nœud correspondant à capacité IPv6. Cependant, quand il est situé dans un réseau IPv4 seulement, ou quand il utilise l'adresse de rattachement IPv4 pour communiquer avec un nœud correspondant IPv4, l'optimisation de chemin ne va pas être possible du fait de la difficulté d'effectuer l'essai d'acheminement de retour. Dans la présente spécification, l'encapsulation UDP est seulement utilisée entre le nœud mobile et son agent de rattachement. Donc, les nœuds mobiles vont devoir communiquer à travers l'agent de rattachement.

L'optimisation de chemin ne va pas être possible pour le trafic IPv4 -- c'est-à-dire, le trafic adressé à l'adresse de rattachement IPv4 du nœud mobile. C'est similaire à utiliser IPv4 mobile ; donc, il n'y a pas de réduction des caractéristiques résultant de l'utilisation de la présente spécification.

2.5 Allocation dynamique d'adresse de rattachement IPv4

Il est possible de permettre que l'adresse de rattachement IPv4 du nœud mobile soit allouée de façon dynamique. C'est fait en incluant 0.0.0.0 dans l'option Adresse de rattachement IPv4 qui est incluse dans la mise à jour de lien. L'agent de rattachement DEVRAIT allouer une adresse IPv4 au nœud mobile et l'inclure dans l'option Accusé de réception d'adresse IPv4 envoyée au nœud mobile. Dans ce cas, la durée de vie du lien est liée au minimum de la durée de vie du lien IPv6 et de la durée du prêt de l'adresse de rattachement IPv4.

3. Extensions et modifications à IPv6 mobile

Cette Section souligne les ajouts au protocole et aux mises en œuvre requis pour prendre en charge la présente spécification.

3.1 Extensions de mise à jour de lien

3.1.1 Option Adresse de rattachement IPv4

Cette option est incluse dans l'en-tête de mobilité, incluant le message de mise à jour de lien envoyé du nœud mobile à l'agent de rattachement ou au point d'ancrage de mobilité. L'exigence d'alignement pour cette option est 4n.

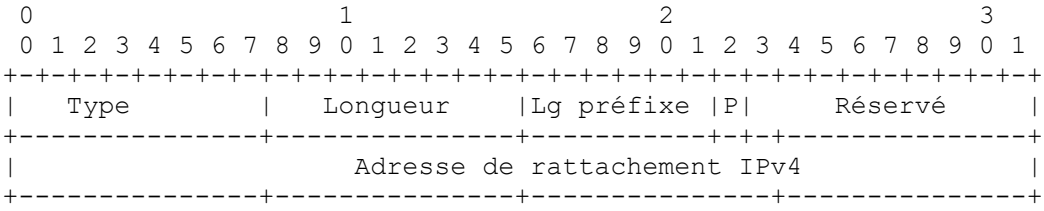

Figure 1 : Option Adresse de rattachement IPv4

Type : 29

Longueur : 6

Lg préfixe : longueur du préfixe alloué au nœud mobile. Si une seule adresse est allouée, ce champ DOIT être réglé à 32. Dans la première mise à jour de lien demandant un préfixe, le champ contient la longueur du préfixe demandé. Cependant, dans les mises à jour de lien suivantes, ce champ doit contenir la longueur du préfixe alloué. Une valeur de zéro est invalide et DOIT être considérée comme une erreur.

P : fanion qui indique, quand il est établi, que le nœud mobile demande un préfixe de réseau mobile. Ce fanion est seulement pertinent pour les nouvelles demandes, et doit être ignoré pour les rafraîchissements de lien.

Réservé : ce champ est réservé pour une utilisation future. il DOIT être réglé à zéro par l'envoyeur et ignoré par le receveur.

Adresse de rattachement IPv4 : adresse de rattachement IPv4 du nœud mobile qui devrait être défendue par l'agent de rattachement. Ce champ pourrait contenir toute adresse IPv4 d'envoi individuel (publique ou privée) qui a été allouée au nœud mobile. La valeur 0.0.0.0 est utilisée pour demander une adresse de rattachement IPv4 à l'agent de rattachement. Un nœud mobile peut choisir d'utiliser cette option pour demander un préfixe en réglant cette adresse toute à zéro et en établissant le fanion P. Le nœud mobile pourrait alors former une adresse de rattachement IPv4 sur la base du préfixe alloué. Autrement, le nœud mobile peut utiliser deux options différentes, une pour demander une adresse (statique ou dynamique) et une autre pour demander un préfixe.

3.1.2 Option Adresse d'entretien IPv4

Cette option est incluse dans l'en-tête de mobilité, incluant le message de mise à jour de lien envoyé du nœud mobile à un agent de rattachement ou point d'ancrage de mobilité. L'exigence d'alignement pour cette option est 4n.

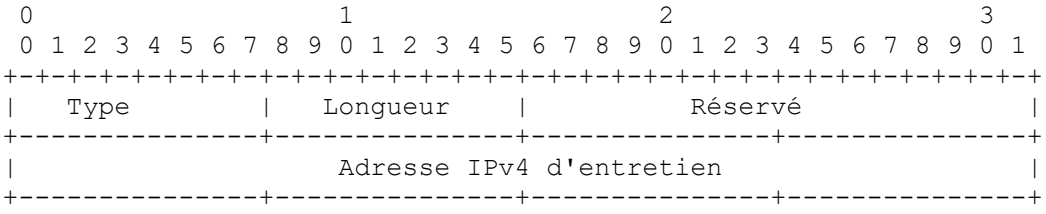

Figure 2 : Option Adresse d'entretien IPv4

Type : 32

Longueur : 6

Réservé : Ce champ est réglé à zéro par l'envoyeur et ignoré par le receveur.

Adresse d'entretien IPv4 : ce champ contient l'adresse d'entretien IPv4 du nœud mobile. L'adresse d'entretien IPv4 est utilisée quand le nœud mobile est situé dans un réseau seulement IPv4.

3.1.3 Extensions de message de mise à jour de lien

La présente spécification étend le message de mise à jour de lien avec un nouveau fanion. Le fanion est montré et décrit ci-dessous.

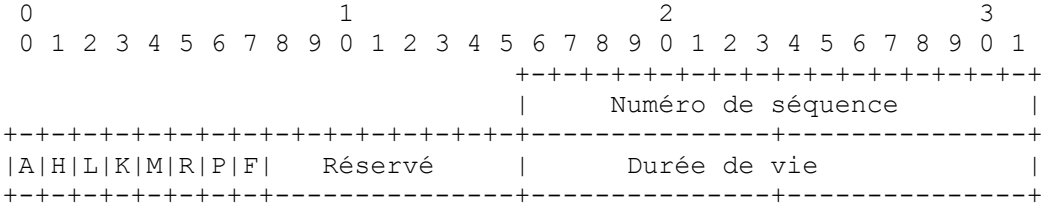

Figure 3 : Message de mise à jour de lien

F : Quand il est établi, ce fanion indique une demande pour forcer l'encapsulation UDP sans considération de si un NAT est présent sur le chemin entre le nœud mobile et l'agent de rattachement. Ce fanion peut être établi par le nœud mobile si il est obligé d'utiliser l'encapsulation UDP sans considération de la présence d'un NAT. Ce fanion NE DEVRAIT PAS être établi quand le nœud mobile est configuré avec une adresse d'entretien IPv6 -- à l'exception du scénario mentionné au paragraphe 4.4.1.

3.2 Extensions d'accusé de réception de lien

3.2.1 Option Accusé de réception d'adresse IPv4

Cette option est incluse dans l'en-tête de mobilité, incluant le message d'accusé de réception de lien envoyé de l'agent de rattachement ou du point d'ancrage de mobilité au nœud mobile. Cette option indique si une entrée d'antémémoire de lien a été créée pour l'adresse IPv4 du nœud mobile. De plus, cette option inclut une adresse de rattachement IPv4 dans le cas d'une configuration dynamique d'adresse de rattachement IPv4 (c'est-à-dire, si l'adresse IPv4 non spécifiée était incluse dans la mise à jour de lien). L'exigence d'alignement pour cette option est 4n.

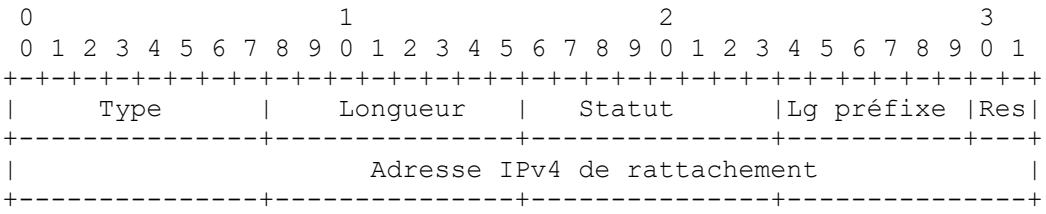

Figure 4 : Option Accusé de réception d'adresse IPv4

Type : 30

Longueur : 6

Statut : Indique le succès ou l'échec du lien d'adresse de rattachement IPv4. Les valeurs de 0 à 127 indiquent le succès. Les valeurs supérieures indiquent l'échec.

Lg préfixe : longueur du préfixe de l'adresse allouée. Ce champ est seulement valide en cas de succès et DOIT être réglé à zéro et ignoré en cas d'échec. Ce champ outrepasse ce que le nœud mobile demandait (si il n'est pas égal à la longueur demandée).

Res : Ce champ est réservé pour une utilisation future. Il DOIT être réglé à zéro par l'envoyeur et ignoré par le receveur

Adresse de rattachement IPv4 : adresse de rattachement IPv4 que l'agent de rattachement va utiliser dans l'entrée d'antémémoire de lien. Ce pourrait être une adresse publique ou privée. Ce champ DOIT contenir l'adresse de rattachement IPv4 du nœud mobile. Si l'adresse a été allouée dynamiquement, l'agent de rattachement va ajouter l'adresse pour en informer le nœud mobile. Autrement, si l'adresse est allouée statiquement au nœud mobile, l'agent de rattachement va la copier du message de mise à jour de lien.

Les valeurs suivantes sont allouées pour le champ Statut :

0	Succès
128	Échec, raison non spécifiée
129	Administrativement interdit
130	Adresse de rattachement IPv4 incorrecte
131	Adresse IPv4 invalide
132	Allocation dynamique d'adresse de rattachement IPv4 indisponible
133	Allocation de préfixe non autorisée

3.2.2 Option Détection de NAT

Cette option est envoyée de l'agent de rattachement au nœud mobile pour indiquer si un NAT est dans le chemin. Cette option PEUT aussi inclure une heure de rafraîchissement de lien de NAT suggérée pour le nœud mobile. Cela pourrait être utile pour des scénarios où le nœud mobile est connu pour être en mouvement au sein du domaine administratif de l'agent de rattachement et donc, la temporisation de NAT est connue (par configuration) de l'agent de rattachement. Le paragraphe 3.5 de la [RFC5405] discute en détails les problèmes de temporisation de NAT.

L'exigence d'alignement pour cette option est 4n. Si un NAT est détecté, cette option DOIT être envoyée par l'agent de rattachement.

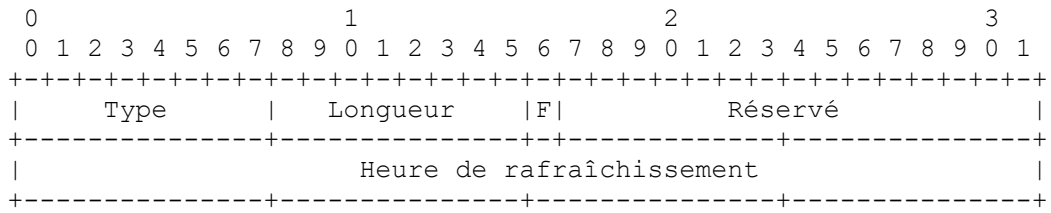

Figure 5 : Option Détection de NAT

Type : 31

Longueur : 6

F : Ce fanion indique au nœud mobile que l'encapsulation UDP est exigée. Quand il est établi, ce fanion indique que le nœud mobile DOIT utiliser l'encapsulation UDP même si un NAT n'est pas situé entre le nœud mobile et l'agent de rattachement. Ce fanion NE DEVRAIT PAS être établi quand une adresse d'entretien IPv6 est allouée au nœud mobile -- à l'exception du traitement des scénarios discutés au paragraphe 4.4.1.

Réservé : Ce champ est réservé pour une utilisation future. il DOIT être réglé à zéro par l'envoyeur et ignoré par le receveur.

Heure de rafraîchissement : une heure suggérée (en secondes) pour que le nœud mobile rafraîchisse le lien de NAT. Si elle est réglée à zéro, elle est ignorée. Si ce champ est réglé tout à 1, cela signifie que les maintiens en vie ne sont pas nécessaires, c'est-à-dire, aucun NAT n'a été détecté. L'agent de rattachement DOIT être configuré avec une valeur par défaut pour l'heure de rafraîchissement. La valeur recommandée est donnée à la Section 6.

4. Fonctionnement du protocole

Cette Section présente le fonctionnement du protocole et le traitement des messages présentés ci-dessus. De plus, elle introduit le mécanisme de détection et de traversée de NAT utilisé par la présente spécification.

4.1 Formats de tunnelage

La présente spécification permet au nœud mobile d'utiliser divers formats de tunnelage selon sa localisation et les capacités du réseau visité. Le nœud mobile peut tunneler IPv6 dans IPv4, IPv4 dans IPv6, ou utiliser l'encapsulation UDP pour tunneler IPv6 dans IPv4. Naturellement, la présente spécification prend aussi en charge le tunnelage de IPv6 dans IPv6 [RFC2473].

La présente spécification permet d'utiliser le tunnelage fondé sur UDP entre le nœud mobile et son agent de rattachement ou le MAP. Un format d'encapsulation UDP signifie l'ordre des en-têtes suivant : IPv4/v6, UDP, IP (v4 ou v6), autres en-têtes.

Noter que l'utilisation de l'encapsulation UDP pour les adresses d'entretien IPv6 NE DEVRAIT PAS être faite sauf dans les circonstances soulignées au paragraphe 4.4.1.

Quand il utilise ce format, le receveur analyse le champ Version qui suit l'en-tête UDP afin de déterminer si l'en-tête suivant est IPv4 ou IPv6. Le reste des en-têtes est traité normalement. L'ordre des en-têtes ci-dessus ne prend pas en compte les en-têtes IPsec car ils peuvent être placés dans différentes parties du paquet. Le format ci-dessus DOIT être pris en charge par toutes les mises en œuvre de la présente spécification et DOIT toujours être utilisé pour envoyer le message de mise à jour de lien.

Le tunnelage UDP peut aussi encapsuler un en-tête d'encapsulation de charge utile de sécurité (ESP, *Encapsulating Security Payload*) comme montré ci-dessous : IPv4/v6, UDP, ESP, IP (v4 ou v6), autres en-têtes.

La négociation de format de tunnel sûr décrite ci-dessus est discutée au paragraphe 5.2. Le receveur d'un tunnel UDP détecte si un en-tête ESP est ou non présent sur la base de l'accès UDP utilisé.

4.1.1 Impacts du tunnelage sur le transport et la MTU

Changer le format de tunnel peut survenir à cause du mouvement du nœud mobile d'un réseau à un autre. Cela peut impacter la MTU de la liaison et du chemin, ce qui peut affecter la quantité de bande passante disponible aux applications. Le nœud mobile peut utiliser la découverte de la MTU de chemin (PMTUD, *Path MTU Discovery*) comme spécifié dans la [RFC4459].

Pour s'accommoder du trafic qui utilise la notification explicite d'encombrement (ECN, *Explicit Congestion Notification*) il est RECOMMANDÉ que les information d'ECN et de codet de services différenciés (DSCP, *Differentiated Services Code Point*) soient copiées entre les en-têtes interne et externe comme défini dans les [RFC3168] et [RFC2983]. Il est RECOMMANDÉ que l'option de pleine fonctionnalité définie au paragraphe 9.1.1 de la [RFC3168] soit utilisée pour traiter ECN.

Noter que certaines mises en œuvre peuvent ne pas être capables d'utiliser ECN sur le tunnel UDP. Cela est dû à l'absence d'accès aux bits ECN dans l'API UDP sur la plupart des plates-formes. Cependant, ce problème peut être évité si l'encapsulation UDP est faite dans le noyau.

Noter que, quand on utilise l'encapsulation UDP, le champ Durée de vie (TTL, *Time to Live*) doit être décrémenté de la même manière que quand l'encapsulation IP dans IP est utilisée.

4.2 Détection de NAT

Ce paragraphe traite de la détection de NAT pour les besoins de l'encapsulation de paquets entre le nœud mobile et l'agent de rattachement quand le nœud mobile est présent dans un réseau privé IPv4. IPv6 mobile utilise IKEv2 pour établir l'association de sécurité (SA) IPsec entre le nœud mobile et l'agent de rattachement. IKEv2 a son propre mécanisme de détection de NAT. Cependant, la détection de NAT de IKEv2 est seulement utilisée pour les besoins d'établissement de la SA IPsec pour sécuriser le trafic. Les interactions entre les mécanismes de traversée de NAT sont décrites à la Section 5.

La détection de NAT est faite quand le message initial de mise à jour de lien est envoyé du nœud mobile à l'agent de rattachement. Quand il est situé dans une liaison étrangère seulement IPv4, le nœud mobile envoie le message de mise à jour de lien encapsulé dans UDP et IPv4. L'adresse de source du paquet IPv6 est l'adresse de rattachement IPv6 du nœud mobile. L'adresse de destination est l'adresse IPv6 de l'agent de rattachement. L'en-tête IPv4 contient l'adresse d'entretien IPv4 dans le champ Adresse de source et l'adresse IPv4 de l'agent de rattachement dans le champ Adresse de destination.

Quand l'agent de rattachement reçoit la mise à jour de lien encapsulée, il compare l'adresse IPv4 du champ Adresse de source dans l'en-tête IPv4 avec l'adresse IPv4 incluse dans l'option Adresse d'entretien IPv4. Si les deux adresses correspondent, aucun appareil de NAT n'est dans le chemin. Autrement, un NAT est dans le chemin et l'option de détection de NAT est incluse dans l'accusé de réception de lien. L'accusé de réception de lien et tous les futurs paquets sont alors encapsulés dans UDP et IPv4. L'adresse de source dans l'en-tête IPv4 est l'adresse IPv4 de l'agent de rattachement. L'adresse de destination est l'adresse IPv4 reçue de l'en-tête IPv4 encapsulant la mise à jour de lien (cette adresse va être différente de l'adresse d'entretien IPv4 quand un NAT est dans le chemin). L'accès de source dans le paquet est l'accès de source de l'agent de rattachement. L'accès de destination est l'accès de source reçu dans le message de mise à jour de lien. Noter que l'agent de rattachement mémorise les numéros d'accès et les associe au tunnel du nœud mobile afin de transmettre les paquets futurs.

À réception de l'accusé de réception de lien avec l'option de détection de NAT, le nœud mobile établit le tunnel à l'agent de rattachement pour l'encapsulation UDP. Donc, tous les futurs paquets à l'agent de rattachement sont tunnelés dans UDP et IPv4. Pour tous les paquets IPv6 tunnelés, l'adresse de source dans l'en-tête IPv6 est l'adresse de rattachement IPv6 du nœud mobile et l'adresse de destination est l'adresse IPv6 du nœud correspondant. Tous les paquets IPv4 tunnelés vont contenir l'adresse de rattachement IPv4 du nœud mobile dans le champ Adresse de source du paquet IPv4 interne et l'adresse IPv4 du nœud correspondant dans le champ Adresse de destination. L'en-tête IPv4 externe est le même que le paquet interne soit IPv4 ou IPv6.

Si aucun appareil de NAT n'a été détecté dans le chemin entre le nœud mobile et l'agent de rattachement, alors les paquets IPv6 sont tunnelés dans un en-tête IPv4 sauf si l'agent de rattachement force l'encapsulation UDP en utilisant le fanion F. Le contenu des en-têtes interne et externe est identique à celui de l'encapsulation UDP.

Un nœud mobile DOIT toujours tunneler les mises à jour de lien dans UDP quand il est situé dans un réseau IPv4 seulement. Ce processus permet essentiellement la détection perpétuelle de NAT. De même, l'agent de rattachement DOIT encapsuler les accusés de réception de lien dans un en-tête UDP chaque fois que la mise à jour de lien est encapsulée dans UDP.

En conclusion, les formats de paquet pour les messages de mise à jour de lien et d'accusé de réception sont montrés ci-dessous :

Mise à jour de lien *(BU)* reçue par l'agent de rattachement :
En-tête IPv4 (src=V4ADDR, dst=HA_V4ADDR)
En-tête UDP
En-tête IPv6 (src=V6HOA, dst=HAADDR)
En-tête ESP
En-tête Mobilité
BU [IPv4 HAO]
Option CoA IPv4

Où V4ADDR est soit l'adresse d'entretien IPv4 soit l'adresse fournie par l'appareil de NAT. V6HOA est l'adresse de rattachement IPv6 du nœud mobile. La mise à jour de lien PEUT aussi contenir l'option Adresse de rattachement IPv4, IPv4 HAO.

Accusé de réception de lien *(BA)* envoyé par l'agent de rattachement :
En-tête IPv4 (src= HA_V4ADDR, dst=V4ADDR)
En-tête UDP

En-tête IPv6 (src=HAADDR, dst=V6HOA)
En-tête ESP
En-tête Mobilité
BA ([IPv4 ACK], NAT DET)

Où V6HOA est l'adresse de rattachement IPv6 du nœud mobile. Le IPv4 ACK est l'option Accusé de réception d'adresse IPv4, qui est seulement incluse si l'option Adresse de rattachement IPv4 est présente dans la BU. NAT DET est l'option de détection de NAT, qui DOIT être présente dans le message d'accusé de réception de lien si la mise à jour de lien était encapsulée dans UDP.

4.3 Maintiens en vie de NAT

Si un NAT est détecté, le nœud mobile va devoir rafraîchir les liens de NAT afin d'être accessible à partir de l'agent de rattachement. Les liens de NAT peuvent être rafraîchis par l'envoi et la réception de trafic encapsulé dans UDP. Cependant, si le nœud mobile n'est pas actif, il va devoir envoyer périodiquement un message à l'agent de rattachement afin de rafraîchir le lien de NAT. Cela peut être fait en utilisant le message de mise à jour de lien. La paire mise à jour de lien/accusé de réception va assurer que les liens de NAT sont rafraîchis de manière fiable. Il n'y a pas de moyen pour le nœud mobile de savoir le temps exact du lien de NAT. Le temps par défaut suggéré dans la présente spécification est NATKATIMEOUT (voir à la Section 6). Si l'agent de rattachement suggère une période de rafraîchissement différente dans l'accusé de réception de lien, le nœud mobile DEVRAIT utiliser la valeur suggérée par l'agent de rattachement.

Si le moment de rafraîchissement dans l'option Détection de NAT dans l'accusé de réception de lien est réglé tout à 1, le nœud mobile n'a pas besoin d'envoyer de message pour rafraîchir le lien de NAT. Cependant, le nœud mobile peut quand même devoir encapsuler le trafic dans UDP. Ce scénario peut avoir lieu quand un NAT n'est pas détecté mais que l'agent de rattachement exige quand même que le nœud mobile utilise l'encapsulation UDP.

On devrait noter que un nœud mobile qui n'a pas besoin d'être accessible (c'est-à-dire, un qui se soucie seulement de l'aspect continuité de session de IP mobile) n'a pas besoin de rafraîchir le lien de NAT. Dans ce cas, le nœud mobile serait seulement capable d'initier une communication avec d'autres nœuds. Cependant, cela va probablement impliquer que le nœud mobile va devoir envoyer une mise à jour de lien avant d'initier une communication après une longue période d'inactivité car il est probable qu'il lui sera alloué un accès et une adresse IPv4 différents par le NAT quand il initiera la communication. Donc, une mise en œuvre peut choisir, au nom de la simplicité, de toujours maintenir les liens de NAT même quand elle n'a pas besoin de l'accessibilité.

Noter que les maintiens en vie sont aussi nécessaires pour IKEv2 sur l'accès UDP 4500. C'est nécessaire pour la détection d'homologue mort de IKE *(Internet Key Exchange Protocol)* qui n'est pas traitée par les maintiens en vie DSMIPv6.

4.4 Fonctionnement de nœud mobile

En plus des opérations spécifiées dans les [RFC3775] et [RFC3963], la présente spécification exige que les nœuds mobiles soient capables de prendre en charge une adresse de rattachement IPv4. La présente spécification exige aussi que le nœud mobile choisisse une adresse d'entretien IPv4 ou IPv6. On discute d'abord du choix d'adresse d'entretien, puis on continue avec la gestion de lien et la transmission du trafic normal.

4.4.1 Choix d'une adresse d'entretien

Quand un nœud mobile est dans un réseau visité double piles, il aura à choisir entre une adresse d'entretien IPv4 et IPv6. Le nœud mobile DEVRAIT préférer l'adresse d'entretien IPv6 et la lier à sa ou ses adresses de rattachement. Si un nœud mobile tentait de lier l'adresse d'entretien IPv6 à sa ou ses adresses de rattachement et si la mise à jour de lien est arrivée en fin de temporisation, le nœud mobile DEVRAIT :

- o Renvoyer la mise à jour de lien en utilisant l'algorithme de retard exponentiel décrit dans la [RFC3775].
- o Si après trois tentatives, un accusé de réception de lien n'a pas été reçu, le nœud mobile DEVRAIT envoyer une nouvelle mise à jour de lien en utilisant l'adresse d'entretien IPv4. L'algorithme de retard exponentiel décrit dans la [RFC3775] devrait être utilisé pour les retransmissions des mises à jour de lien si nécessaire.

Cette procédure devrait être utilisée pour éviter des scénarios où la connexité IPv6 ne peut pas être aussi fiable que IPv4. Cette non fiabilité peut avoir lieu durant les déploiements précoces de IPv6 ou peut simplement être due à des pannes temporaires affectant l'acheminement IPv6.

Il est RECOMMANDÉ qu'en mouvement, le nœud mobile ne change pas la famille d'adresses IP choisie pour la précédente mise à jour de lien sauf si le nœud mobile sait qu'il est passé dans un domaine administratif différent où des problèmes précédents avec l'acheminement IPv6 peuvent ne pas être présents. Répéter la procédure ci-dessus à chaque mouvement peut causer une dégradation significative des performances des applications du nœud mobile due à des périodes étendues de perte de paquets après un transfert inter cellulaire, si la panne d'acheminement existe toujours.

Quand on utilise une adresse d'entretien IPv4 et l'encapsulation IP dans IP, si la mise en œuvre de nœud mobile est informée par les couches supérieures de pertes persistantes de paquets, elle peut tenter de renvoyer la mise à jour de lien avec le fanion F établi, demandant l'encapsulation UDP pour tous les paquets. Cela peut éviter des pertes de paquets dues aux situations où les politiques locales de pare-feu empêchent l'utilisation de l'encapsulation IP dans IP.

L'effet de ce mécanisme de choix d'adresses est de permettre les préférences suivantes en l'absence de NAT :
1. IPv6
2. IPv4 (en utilisant l'encapsulation IP dans IP ou UDP si un NAT est détecté)
3. encapsulation UDP quand IP dans IP n'est pas permis par le domaine local.

4.4.2 Envoi des mises à jour de lien

Quand ils envoient un paquet IPv6 contenant une mise à jour de lien alors qu'ils sont connectés à un réseau d'accès IPv4 seulement, les nœuds mobiles DOIVENT s'assurer de ce qui suit :
- Le paquet IPv6 est encapsulé dans UDP.
- L'adresse de source dans l'en-tête IPv4 est l'adresse d'entretien IPv4 du nœud mobile.
- L'adresse de destination dans l'en-tête IPv4 est l'adresse IPv4 de l'agent de rattachement.
- L'adresse de source dans l'en-tête IPv6 est l'adresse de rattachement IPv6 du nœud mobile.
- L'option Adresse de rattachement IPv4 PEUT être incluse dans l'en-tête de mobilité. Cette option contient l'adresse de rattachement IPv4. Si le nœud mobile n'avait pas une adresse de rattachement statique, il PEUT inclure l'adresse IPv4 non spécifiée, qui agit comme une demande d'une adresse de rattachement IPv4 dynamique. Autrement, une ou plusieurs options Adresse de rattachement IPv4 peuvent être incluses avec des demandes de préfixes IPv4 (c'est-à-dire, avec le fanion P établi).
- Si le nœud mobile souhaite utiliser l'encapsulation UDP seulement, il doit établir le fanion F dans le message de mise à jour de lien.
- Le paquet IPv6 DOIT être authentifié conformément à la [RFC3775], sur la base de l'adresse de rattachement IPv6 du nœud mobile.

Quand il envoie une mise à jour de lien provenant d'un réseau visité qui prend en charge IPv6, le nœud mobile DOIT suivre les règles spécifiées dans la [RFC3775]. De plus, si le nœud mobile a une adresse de rattachement IPv4 ou en a besoin d'une, il DOIT inclure l'option Adresse de rattachement IPv4 dans l'en-tête de mobilité. Si le nœud mobile a déjà une adresse de rattachement IPv4 statique, cette adresse DOIT être incluse dans l'option Adresse de rattachement IPv4. Autrement, si le nœud mobile a besoin d'une adresse IPv4 dynamique, il DOIT inclure l'adresse IPv4 0.0.0.0 dans l'option adresse de rattachement IPv4.

En plus des règles de la [RFC3775], le nœud mobile devrait suivre les lignes directrices de choix d'adresse d'entretien du paragraphe 4.4.1.

Quand le nœud mobile reçoit un accusé de réception de lien provenant de l'agent de rattachement, il suit les règles des [RFC3775] et [RFC3963]. De plus, les actions suivantes DOIVENT être effectuées :
- Si le champ Statut indiquait un échec avec le code d'erreur 144, le nœud mobile PEUT renvoyer la mise à jour de lien sans établir le fanion F.
- Si l'en-tête de mobilité inclut une option Accusé de réception d'adresse IPv4 qui indique le succès, le nœud mobile devrait créer deux entrées dans sa liste de mises à jour de lien : une pour l'adresse de rattachement IPv6 et une autre pour l'adresse de rattachement IPv4.
- Si l'option Détection de NAT est présente, le nœud mobile DOIT tunneler les futurs paquets dans UDP et IPv4. Cela DOIT être indiqué dans la liste de mises à jour de lien.
- Si aucune option Accusé de réception d'adresse IPv4 n'est présente, et si une option Adresse de rattachement IPv4 était présente dans la mise à jour de lien, le nœud mobile DOIT seulement créer une entrée de liste de mises à jour de lien pour son adresse de rattachement IPv6. Le nœud mobile PEUT inclure l'option Adresse de rattachement IPv4 dans les futures mises à jour de lien.
- Si une option Accusé de réception d'adresse IPv4 est présente et indique l'échec pour le lien d'adresse de rattachement IPv4, le nœud mobile NE DOIT PAS créer une entrée pour cette adresse dans sa liste de mises à jour de lien. Le nœud mobile PEUT inclure l'option Adresse de rattachement IPv4 dans les futures mises à jour de lien.

4.4.2.1 Suppression des liens

Les nœuds mobiles vont supprimer les liens provenant de l'antémémoire de liens de l'agent de rattachement chaque fois que ils reviennent à la liaison de rattachement, ou simplement quand le support de mobilité n'est pas nécessaire.

Le désenregistrement de l'adresse de rattachement IPv6 est décrit dans la [RFC3775]. Le même mécanisme s'applique dans la présente spécification. Les nœuds mobiles peuvent supprimer le lien pour seulement l'adresse de rattachement IPv4 en envoyant une mise à jour de lien qui n'inclut pas d'option Adresse de rattachement IPv4.

À réception de cette mise à jour de lien, l'agent de rattachement va remplacer les entrées existantes d'antémémoire par lc contenu du nouveau message. Cela assure que le lien d'adresse de rattachement IPv4 est supprimé tout en maintenant un lien IPv6.

Noter que le nœud mobile ne peut pas supprimer le lien d'adresse de rattachement IPv6 tout en maintenant un lien d'adresse de rattachement IPv4.

Un message de mise à jour de lien avec une durée de vie de zéro va supprimer tous les liens pour le nœud mobile.

4.4.3. Envoi de paquets à partir d'un réseau visité

Quand le nœud mobile est situé dans un réseau à capacité IPv6, il envoie et reçoit les paquets IPv6 comme décrit dans la [RFC3775]. Dans les cas où l'encapsulation IP dans IP ne fournit pas la connexité à l'agent de rattachement, le nœud mobile peut choisir d'encapsuler dans UDP comme suggéré au paragraphe 4.4.1. Cependant, cette encapsulation du trafic IPv6 devrait être utilisée en dernier ressort, comme décrit. Le trafic IPv4 est encapsulé dans les paquets IPv6 à l'agent de rattachement.

Quand le nœud mobile est situé dans un réseau IPv4 seulement, il va envoyer les paquets IPv6 à son agent de rattachement conformément au format suivant :
En-tête IPv4 (src=V4CoA, dst=HA_V4ADDR)
[en-tête UDP]
En-tête IPv6 (src=V6HoA, dst=CN)
Protocoles de couche supérieure.

Ici, l'en-tête UDP est seulement utilisé si un NAT a été détecté entre le nœud mobile et l'agent de rattachement, ou si l'agent de rattachement a forcé l'encapsulation UDP. V4CoA est l'adresse d'entretien IPv4 configurée par le nœud mobile dans le réseau visité.

De même, les paquets IPv4 sont envoyés conformément au format suivant :
En-tête IPv4 (src=V4CoA, dst=HA_V4ADDR)
[en-tête UDP]
En-tête IPv4 en-tête (src=V4HoA, dst=V4CN)
Protocoles de couche supérieure.

Ici, l'en-tête UDP est seulement utilisé si un NAT a été détecté entre le nœud mobile et l'agent de rattachement, ou si l'agent de rattachement a forcé l'encapsulation UDP.

4.4.4 Détection de mouvement dans les réseaux IPv4 seul

La [RFC3775] décrit la détection de mouvement principalement sur la base de déclencheurs spécifiques de IPv6 et sur les informations de la découverte de voisin [RFC4861]. Ces déclencheurs ne sont pas disponibles dans un réseau IPv4 seulement. Donc, un nœud mobile situé dans un réseau IPv4 seulement DEVRAIT utiliser les lignes directrices de la [RFC4436] sur les mécanismes de détection de mouvement dans les réseaux IPv4 seulement.

Le nœud mobile détecte qu'il est dans un réseau IPv4 seulement quand l'algorithme de détection de mouvement IPv6 échoue à configurer une adresse IPv6.

La présente spécification ne prend pas en charge les nœuds mobiles qui retournent au réseau de rattachement en utilisant IPv4. C'est-dire, la prise en charge de IPv4 est seulement définie pour les nœuds mobiles qui sont dans un réseau visité.

4.5 Fonctionnement de l'agent de rattachement

En plus de la spécification d'agent de rattachement des [RFC3775] et [RFC3963], l'agent de rattachement doit être capable de traiter l'option Adresse de rattachement IPv4 et de générer l'option Accusé de réception d'adresse IPv4. Les deux options sont incluses dans l'en-tête de mobilité. De plus, l'agent de rattachement DOIT être capable de détecter la présence d'un appareil de NAT et d'indiquer cette présence dans l'option Détection de NAT incluse dans l'accusé de réception de lien.

Un agent de rattachement doit aussi agir comme mandataire pour la résolution d'adresse dans IPv4 pour les adresses de rattachement IPv4 enregistrées des nœuds mobiles qu'il dessert. De plus, le domaine administratif de l'agent de rattachement est responsable d'annoncer les informations d'acheminement des préfixes enregistrés de réseau mobile IPv4 des nœuds mobiles.

Afin de se conformer à la présente spécification, l'agent de rattachement DOIT être capable de trouver l'adresse de rattachement IPv4 d'un nœud mobile quand on lui donne l'adresse de rattachement IPv6. C'est-à-dire, étant donnée une adresse de rattachement IPv6, l'agent de rattachement DOIT mémoriser l'adresse de rattachement IPv4 correspondante si une adresse statique est présente. Si une adresse dynamique est demandée par le nœud mobile, l'agent de rattachement DOIT mémoriser cette adresse (associée à l'adresse de rattachement IPv6) après qu'elle est allouée au nœud mobile.

Quand l'agent de rattachement reçoit une mise à jour de lien encapsulée dans UDP et contenant l'option Adresse de rattachement IPv4, il doit suivre toutes les étapes des [RFC3775] et [RFC3963]. De plus, les vérifications suivantes DOIVENT être effectuées :

- Si l'adresse d'entretien IPv4 dans l'option CoA IPv4 n'est pas la même que l'adresse IPv4 dans l'adresse de source dans l'en-tête IPv4, alors un NAT est dans le chemin. Cette information devrait être marquée par un fanion pour l'accusé de réception de lien.

- Si le fanion F dans la mise à jour de lien est établi, l'agent de rattachement doit déterminer si il accepte de forcer l'encapsulation UDP. Si il ne l'accepte pas, l'accusé de réception de lien est envoyé avec le code d'erreur 144. L'encapsulation UDP NE DEVRAIT PAS être utilisée quand le nœud mobile est situé dans une liaison à capacité IPv6, à l'exception des scénarios mentionnés au paragraphe 4.4.1.

- Si l'option Adresse de rattachement IPv4 contient un adresse IPv4 en envoi individuel valide, l'agent de rattachement DOIT vérifier que cette adresse est allouée au nœud mobile qui a l'adresse de rattachement IPv6 incluse dans l'option Adresse de rattachement. La même chose DOIT être faite pour un préfixe IPv4.

- Si l'option Adresse de rattachement IPv4 contenait l'adresse IPv4 non spécifiée, l'agent de rattachement DEVRAIT allouer dynamiquement une adresse de rattachement IPv4 au nœud mobile. Si aucune n'est disponible, l'agent de rattachement DOIT retourner le code d'erreur 132 dans le champ Statut de l'option Accusé de réception d'adresse IPv4. Si un préfixe est demandé, l'agent de rattachement DEVRAIT allouer un préfixe avec la longueur demandée ; si l'allocation de préfixe (de n'importe quelle longueur) n'est pas possible, l'agent de rattachement DOIT indiquer l'échec de l'opération avec le code d'erreur approprié.

- Si la mise à jour de lien est acceptée pour l'adresse de rattachement IPv4, l'agent de rattachement crée une entrée d'antémémoire de lien pour l'adresse de rattachement/préfixe IPv4. L'agent de rattachement DOIT inclure une option Accusé de réception IPv4 dans l'en-tête de mobilité contenant l'accusé de réception de lien.

- Si la mise à jour de lien est acceptée pour les deux adresses de rattachement IPv4 et IPv6, l'agent de rattachement crée des entrées séparées d'antémémoire de lien, une pour chaque adresse de rattachement. L'adresse d'entretien est celle incluse dans la mise à jour de lien. Si l'adresse d'entretien est une adresse IPv4, l'agent de rattachement DOIT établir un tunnel à l'adresse d'entretien IPv4 du nœud mobile.

Quand il envoie un accusé de réception de lien au nœud mobile, l'agent de rattachement construit le message conformément aux [RFC3775] et [RFC3963]. Noter que l'en-tête d'acheminement DOIT toujours contenir l'adresse de rattachement IPv6 comme spécifié dans la [RFC3775].

Si l'adresse d'entretien du nœud mobile est une adresse IPv4, l'agent de rattachement inclut l'adresse de rattachement IPv6 du nœud mobile dans le champ Adresse de destination de l'en-tête IPv6. Si un NAT est détecté, l'agent de rattachement DOIT alors encapsuler le paquet dans UDP et dans un en-tête IPv4. L'adresse de source est réglée à l'adresse IPv4 de l'agent de rattachement et l'adresse de destination est réglée à l'adresse reçue dans l'adresse de source de l'en-tête IPv4

encapsulant la mise à jour de lien.

Après avoir créé une entrée d'antémémoire de lien pour l'adresse de rattachement du nœud mobile, tous les paquets envoyés aux adresses de rattachement du nœud mobile sont tunnelés par l'agent de rattachement à l'adresse d'entretien du nœud mobile. Si un NAT est détecté, les paquets sont encapsulés dans UDP et IPv4. Autrement, si l'adresse d'entretien est une adresse IPv4 et si aucun NAT n'est détecté, les paquets sont encapsulés dans un en-tête IPv4 sauf si l'encapsulation UDP est forcée par l'agent de rattachement.

4.5.1 Envoi de paquets au nœud mobile

L'agent de rattachement suit les règles spécifiées dans la [RFC3775] pour l'envoi des paquets IPv6 aux nœuds mobiles situés dans les réseaux IPv6. Quand il envoie des paquets IPv4 aux nœuds mobiles dans un réseau IPv6, l'agent de rattachement doit encapsuler les paquets IPv4 dans IPv6.

Quand il envoie des paquets IPv6 à un nœud mobile situé dans un réseau IPv4, l'agent de rattachement utilise le format suivant :
En-tête IPv4 (src= HA_V4ADDR, dst= V4ADDR)
[en-tête UDP]
En-tête IPv6 (src=CN, dst= V6HoA)
Protocoles de couche supérieure

Où l'en-tête UDP est seulement inclus si un NAT est détecté entre le nœud mobile et l'agent de rattachement ou si l'agent de rattachement a forcé l'encapsulation UDP. V4ADDR est l'adresse IPv4 reçue dans le champ Adresse de source du paquet IPv4 contenant la mise à jour de lien.

Quand il envoie des paquets IPv4 à un nœud mobile situé dans un réseau IPv4, l'agent de rattachement doit suivre le format négocié dans l'échange de mise à jour de lien/accusé de réception. En l'absence de format négocié, le format par défaut qui DOIT être pris en charge par toutes les mises en œuvre est :
En-tête IPv4 (src= HA_V4ADDR, dst= V4ADDR)
[en-tête UDP]
En-tête IPv4 (src=V4CN, dst= V4HoA)
Protocoles de couche supérieure

Où l'en-tête UDP est inclus seulement si un NAT est détecté entre le nœud mobile et l'agent de rattachement ou si l'agent de rattachement a forcé l'encapsulation UDP.

4.6 Fonctionnement du nœud correspondant

La présente spécification n'a pas d'impact sur les nœuds IPv4 ou IPv6 correspondants.

5. Considérations sur la sécurité

La présente spécification permet à un nœud mobile d'envoyer une mise à jour de lien pour ses adresses de rattachement IPv6 et IPv4. C'est une légère variante de la [RFC3775], qui exige une mise à jour de lien par adresse de rattachement. Cependant, comme dans la [RFC3775], l'association de sécurité IPsec nécessaire pour authentifier la mise à jour de lien est toujours fondée sur l'adresse de rattachement IPv6 du nœud mobile. Donc, pour autoriser le lien de l'adresse de rattachement IPv4 du nœud mobile, l'agent de rattachement DOIT mémoriser l'adresse IPv4 correspondant à l'adresse IPv6 qui est allouée au nœud mobile. Donc, il est suffisant que l'agent de rattachement sache que la vérification IPsec pour le paquet contenant la mise à jour de lien était valide, pourvu qu'il sache quelle adresse de rattachement IPv4 est associée à quelle adresse de rattachement IPv6. Donc, la sécurité du lien d'adresse de rattachement IPv4 est la même que celle du lien IPv6.

En effet, associer l'adresse de rattachement IPv4 du nœud mobile à son adresse de rattachement IPv6 déplace l'autorisation de la mise à jour de lien pour l'adresse IPv4 à la mise en œuvre de IPv6 mobile, qui la déduit du fait que le nœud mobile a une adresse de rattachement IPv6 et les accréditifs corrects pour envoyer une mise à jour de lien authentique pour l'adresse IPv6.

La présente spécification exige l'utilisation de IKEv2 comme mécanisme par défaut pour le chiffrement dynamique.

Dans les cas où la présente spécification est utilisé pour la traversée de NAT, il est important de noter qu'elle a les mêmes vulnérabilités associées à la [RFC3519]. Un attaquant est capable de capturer la session du nœud mobile avec l'agent de rattachement si il peut modifier le contenu de l'en-tête IPv4 externe. Le contenu de l'en-tête n'est pas authentifié et il n'y a aucun moyen pour que l'agent de rattachement vérifie sa validité. Donc, une attaque par interposition, où un changement du contenu de l'en-tête IPv4 peut causer la dérivation du trafic légitime d'un nœud mobile sur un receveur illégitime indépendamment de l'authenticité du message de mise à jour de lien, est possible.

Dans la présente spécification, le message de mise à jour de lien DOIT être protégé en utilisant le mode de transport ESP. Quand le nœud mobile est situé dans un réseau IPv4 seulement, le message de mise à jour de lien est encapsulé dans UDP comme décrit au paragraphe 4.2. Cependant, UDP NE DEVRAIT PAS être utilisé pour encapsuler le message de mise à jour de lien quand le nœud mobile est situé dans un réseau à capacité IPv6. Si la protection du trafic de charge utile est nécessaire quand le nœud mobile est situé dans un réseau IPv4 seulement, l'encapsulation est faite en utilisant ESP en mode tunnel sur l'accès 4500 comme décrit dans la [RFC3948]. Durant la négociation IKE avec l'agent de rattachement, si le nœud mobile et l'agent de rattachement prennent en charge l'utilisation de l'accès 4500, le nœud mobile DOIT établir l'association de sécurité sur l'accès 4500, sans considération de la présence d'un NAT. Ceci est fait pour éviter de commuter entre les accès 500 et 4500 et la perturbation potentielle du trafic résultant ce cette commutation.

Les transferts inter-cellulaires au sein de réseaux IPv4 privés ou de réseaux IPv6 à IPv4 vont impacter l'association de sécurité entre le nœud mobile et l'agent de rattachement. Le paragraphe suivant présente le comportement attendu du nœud mobile et de l'agent de rattachement dans ces situations. Les détails des négociations IKE et des messages sont illustrés au paragraphe 5.2.

5.1 Interactions de transfert inter cellulaire pour IPsec et IKE

Après que le nœud mobile a détecté le mouvement, il configure une nouvelle adresse d'entretien. Si le nœud mobile est dans un réseau IPv4 seulement, il supprime les entrées d'antémémoire de mise à jour de lien pour les nœuds correspondants, car l'optimisation de chemin ne peut pas être prise en charge. Cela peut causer des pertes de paquets entrants, car les nœuds correspondants distants ne sont pas informés de tels mouvements. Pour éviter la confusion chez le nœud correspondant, le nœud mobile DEVRAIT désenregistrer son lien avec chaque nœud correspondant en envoyant un désenregistrement de mise à jour de lien. Le message de désenregistrement de mise à jour de lien est tunnelé à l'agent de rattachement et au nœud correspondant. Ceci est fait après que le nœud mobile a mis à jour l'agent de rattachement avec sa nouvelle localisation comme expliqué ci-dessous.

Le nœud mobile envoie le message de mise à jour de lien à l'agent de rattachement. Si le nœud mobile est dans un réseau à capacité IPv6, la mise à jour de lien DEVRAIT être envoyée sans encapsulation IPv4/UDP, sauf si l'encapsulation UDP est nécessaire comme décrit au paragraphe 4.4.1. Si le nœud mobile est dans un réseau IPv4 seulement, alors -- après le traitement par IPsec du message de mise à jour de lien (BU) -- il encapsule le BU dans UDP/IPv4 comme expliqué aux paragraphes 4.2 et 4.4. Afin d'être capable d'envoyer la mise à jour de lien quand il est dans un réseau IPv4 seulement, le nœud mobile doit utiliser la nouvelle adresse d'entretien IPv4 dans l'en-tête externe, qui est différente de l'adresse d'entretien utilisé dans le tunnel existant. Cela devrait être fait sans mettre à jour de façon permanente le tunnel au sein de la mise en œuvre de nœud mobile afin de permettre au nœud mobile de recevoir des paquets sur l'ancienne adresse d'entretien jusqu'à ce que l'accusé de réception de lien soit reçu. La méthode utilisée pour réaliser cet effet dépend de la mise en œuvre et sort du domaine d'application de la présente spécification. Cela implique que la fonction de transmission IP (qui choisit l'interface ou le tunnel à travers lequel un paquet est envoyé) n'est pas fondée seulement sur l'adresse de destination : des paquets IPv6 destinés à l'agent de rattachement sont envoyés via le tunnel existant tandis que les BU sont envoyés en utilisant la nouvelle adresse d'entretien. Comme les BU sont protégés par IPsec, la fonction de transmission ne peut pas nécessairement déterminer le traitement correct à partir des en-têtes de paquet. Donc, la mise en œuvre de DSMIPv6 doit attacher des informations supplémentaires aux BU, et ces informations doivent être préservées après le traitement IPsec et rendues disponibles à la fonction de transmission ou aux extensions DSMIP incluses dans la fonction de transmission. Selon la mise en œuvre du nœud mobile, la satisfaction de cette exigence peut exiger des changements à la mise en œuvre de IPsec.

À réception du message de mise à jour de lien encapsulé dans UDP/IPv4, l'agent de rattachement le traite comme suit. Afin de permettre à la mise en œuvre de DSMIPv6 chez l'agent de rattachement de détecter la présence d'un NAT sur le chemin du nœud mobile, il doit comparer l'adresse de source IPv4 externe avec l'adresse IPv4 dans l'option Adresse d'entretien IPv4. Cela implique que les informations dans l'en-tête externe vont être préservées après le traitement IPsec et rendues disponibles à la mise en œuvre de DSMIPv6 chez l'agent de rattachement. Selon la mise en œuvre de l'agent de rattachement, la satisfaction de cette exigence peut requérir des changements à la mise en œuvre de IPsec.

L'agent de rattachement met à jour son association de sécurité en mode tunnel pour inclure l'adresse d'entretien du nœud mobile comme adresse d'en-tête de tunnel distant et 4500 comme numéro d'accès. L'adresse IPv4 et le numéro d'accès vont probablement être faux ; le nœud mobile fournit les informations correctes dans un échange séparé comme décrit ci-dessous. Quand le nœud mobile est situé dans un réseau IPv4 privé (qui est détecté comme décrit ci-dessus) la nouvelle adresse et le numéro d'accès sont alloués par le NAT. L'agent de rattachement va aussi activer ou désactiver l'encapsulation UDP pour les paquets ESP sortants pour les besoins de la traversée de NAT.

Si le bit K (capacité de gestion de clé de mobilité) était établi dans la mise à jour de lien, et si l'agent de rattachement prend en charge cette caractéristique, l'agent de rattachement met à jour les associations de sécurité IKE pour inclure l'adresse d'entretien du nœud mobile comme adresse de l'homologue et 4500 comme numéro d'accès. L'agent de rattachement peut aussi devoir changer les champs de traversée de NAT dans IKE_SA pour permettre la mise à jour dynamique de l'adresse IP et du numéro d'accès, sur la base de la réception de messages IKE authentifiés ou de paquets authentifiés en utilisant ESP en mode tunnel. Les mises à jour dynamiques sont décrites au paragraphe 2.23 de la [RFC4306]. Comme décrit ci-dessus, quand le nœud mobile est situé dans un réseau IPv4 privé, l'adresse et le numéro d'accès utilisés pour les trafics IPsec et IKE ne sont pas encore connus par l'agent de rattachement à ce moment.

Le nœud mobile met à jour la SA IKE SA d'une de deux façons. Si le fanion K était établi dans le message d'accusé de réception de lien, le nœud mobile DEVRAIT envoyer un message d'information vide, qui résulte en ce que le module IKE dans l'agent de rattachement met à jour dynamiquement les informations de la SA. Il est EXIGÉ de la mise en œuvre IKE dans l'agent de rattachement qu'elle prenne en charge cette caractéristique. Autrement, la SA IKE devrait être renégociée. Noter que mettre à jour la SA IKE DOIT avoir lieu après que le nœud mobile a envoyé la mise à jour de lien et reçu l'accusé de réception de l'agent de rattachement.

Il est important de noter que l'adresse d'entretien IPv4 du nœud mobile vue par le module DSMIPv6 de l'agent de rattachement à réception de la mise à jour de lien peut différer de l'adresse d'entretien IPv4 vue par le module IKE et de l'adresse d'entretien utilisée pour transmettre le trafic IPsec en mode tunnel. Donc, il est probable que différents modules dans l'agent de rattachement vont avoir des adresses d'entretien différentes qui devraient être utilisées pour encapsuler le trafic au nœud mobile.

Après avoir réussi le traitement de la mise à jour de lien, l'agent de rattachement envoie l'accusé de réception de lien à l'adresse d'entretien du nœud mobile comme reçue dans l'en-tête externe du paquet contenant la mise à jour de lien. Noter que si le BU a été rejeté, l'accusé de réception de lien (BAck) est envoyé à la même adresesque celle d'où le BU a été reçu. Cela peut exiger un traitement spécial dans la transmission IP et/ou le traitement IPsec qui ressemble à l'envoi de BU dans le nœud mobile (décrit ci-dessus).

À réception de l'accusé de réception de lien, le nœud mobile met à jour ses informations d'association de sécurité en mode tunnel locales pour inclure l'adresse de source IP de l'en-tête de tunnel, qui est l'adresse du nœud mobile, et la destination IP de l'en-tête de tunnel, qui est l'adresse de l'agent de rattachement. Le nœud mobile peut aussi devoir activer ou désactiver l'encapsulation UDP pour les paquets ESP sortants pour les besoins de la traversée de NAT et l'envoi des maintiens en vie.

Le nœud mobile PEUT utiliser MOBIKE [RFC4555] pour mettre à jour sa SA IKE avec l'agent de rattachement. L'utilisation de MOBIKE exige de négocier cette capacité avec l'agent de rattachement lors de l'établissement de la SA. Dans ce cas, le nœud mobile et l'agent de rattachement NE DOIVENT PAS mettre à jour localement leurs SA IPsec, car cette étape est effectuée par MOBIKE. De plus, l'utilisation de MOBIKE permet au nœud mobile de mettre à jour la SA indépendamment de l'échange de mise à jour de lien. Donc, il n'est pas nécessaire que le nœud mobile attende un accusé de réception de lien avant d'effectuer MOBIKE. L'utilisation de MOBIKE est FACULTATIVE dans la présente spécification.

5.2 Messages de négociation IKE entre le nœud mobile et l'agent de rattachement

La présente spécification définit un certain nombre de formats possibles d'encapsulation de données, selon la connexité du nœud mobile au réseau visité. Quand il est connecté à un réseau à capacité IPv6, les formats de tunnelage sont clairs. Cependant, quand il est connecté à un réseau IPv4 seulement, on devrait faire attention quand on négocie l'association IKE et les formats de tunnelage conséquents utilisés pour le trafic sécurisé et non sécurisé. Cette section illustre l'échange de message IKE entre le nœud mobile et l'agent de rattachement quand le nœud mobile est situé dans un réseau IPv4 seulement. Deux négociations IKE différentes sont considérées :

- o fonctionnement IKEv2 pour sécuriser la signalisation DSMIPv6,
- o fonctionnement IKEv2 pour sécuriser les données sur IPv4.

5.2.1 Fonctionnement de IKEv2 pour sécuriser la signalisation DSMIPv6

Un nœud mobile connecté à un réseau IPv4 seulement DEVRAIT suivre les procédures décrites ci-dessous afin d'établir une SA pour la protection des messages de mise à jour de lien et d'accusé de réception de lien. Noter que V4ADDR se réfère soit à l'adresse d'entretien du nœud mobile dans la liaison visitée soit à l'adresse publique allouée au nœud mobile par le NAT.

Nœud mobile **Agent de rattachement**

```
IPv4(source_addr=V4ADDR, dest_addr=HAADDR)
   UDP (500, 500) HDR, SAi1, KEi, Ni NAT-D, NAT-D -->
                                        <-- IPv4(source_addr=HAADDR, dest_addr=V4ADDR)
                                            UDP(500,X) HDR, SAr1, KEr, Nr, [CERTREQ] NAT-D, NAT-D
IPv4(source_addr=V4ADDR, dest_addr=HAADDR)
    UDP (4500,4500) <Marqueur non ESP> HDR, SK
    {IDi, [CERT,] [CERTREQ,] [IDr,] AUTH, N(USE_TRANSPORT_MODE),
    SAi2, TSi, TSr} ---->
                                        <-- IPv4(source_addr=HAADDR, dest_addr=V4ADDR)
                                            UDP (4500,Y) <Marqueur non ESP> HDR, SK
                                            {IDr, [CERT,] AUTH, N(USE_TRANSPORT_MODE), SAr2, TSi, TSr}
```

Les entrées correspondantes de la base de données de politique de sécurité (SPD) sont montrées ci-dessous :

Nœud mobile SPD-S :
Si local_address = home_address_1 &
remote_address = home_agent_1 &
proto = MH & local_mh_type = BU &
remote_mh_type = BAck

Alors utiliser une SA ESP en mode transport.

Initier en utilisant IDi = user_1 à l'adresse home_agent_1
Agent de rattachement SPD-S :
Si local_address = home_agent_1 &
remote_address = home_address_1 &
proto = MH &
local_mh_type = BAck &
remote_mh_type = BU

Alors utiliser une SA ESP en mode transport mode

Lorsque home_address_1 est l'adresse de rattachement IPv6 enregistrée du nœud mobile et home_agent_1 est l'adresse IP de l'agent de rattachement.

Cela devrait résulter en messages BU/BA avec le BU suivant reçu par l'agent de rattachement :
En-tête IPv4 (src=V4ADDR, dst=HA_V4ADDR)
En-tête UDP (sport=Z, dport=DSMIPv6)
En-tête IPv6 (src=V6HOA, dst=HAADDR)
En-tête ESP en mode transport
En-tête de mobilité
BU [IPv4 HAO]
Option CoA IPv4
(et autres comme nécessaire)

À l'agent de rattachement, suite à la désencapsulation UDP, la mise à jour de lien est livrée au module IPsec comme montré ci-dessous :
En-tête IPv6 (src=V6HOA, dst=HAADDR)
En-tête ESP en mode transport
En-tête Mobilité
BU [IPv4 HAO]
Option CoA IPv4
(et autres comme nécessaire)

De plus, V4ADDR et le sport (Z) doivent être passés avec le paquet pour assurer un traitement correct.

Suite au traitement IPsec, la mise à jour de lien est livrée au module d'agent de rattachement DSMIPv6 comme suit :
En-tête IPv6 (src=V6HOA, dst=HAADDR)
En-tête Mobilité
BU [IPv4 HAO]
Option CoA IPv4
(et autres comme nécessaire)

De plus, V4ADDR et le sport (Z) doivent être passés avec le paquet pour assurer un traitement correct.

L'accusé de réception de lien envoyé par le module d'agent de rattachement au module IPsec est comme suit :
En-tête IPv6 (src=HAADDR, dst=V6HOA)
En-tête Mobilité
BA ([IPv4 ACK], NAT DET)
(et autres comme nécessaire)

De plus, V4ADDR, le sport provenant du BU (Z), et une indication que l'encapsulation UDP doit être utilisée doivent être passés avec le paquet pour assurer un traitement correct.

L'accusé de réception de lien envoyé par l'agent de rattachement au nœud mobile est comme suit :
En-tête IPv4 (src= HA_V4ADDR, dst=V4ADDR)
En-tête UDP (sport=DSMIPv6, dport=Z)
En-tête IPv6 (src=HAADDR, dst=V6HOA)
En-tête ESP en mode transport
En-tête Mobilité
BA ([IPv4 ACK], NAT DET)

5.2.2 Fonctionnement de IKEv2 pour sécuriser les données sur IPv4

Pour sécuriser le trafic de données quand le nœud mobile est situé dans un réseau IPv4 seulement, le nœud mobile DOIT établir une SA fille à cette fin. Noter que V4ADDR se réfère à l'adresse d'entretien du nœud mobile dans la liaison visitée ou à l'adresse publique allouée au nœud mobile par le NAT. La procédure est comme suit :

Nœud mobile **Agent de rattachement**

IPv4(source_addr=V4ADDR, dest_addr=HAADDR)
UDP (4500,4500) <Marqueur non ESP> HDR, SK
{[N], SA, Ni, [KEi], TSi, TSr} -->

<--IPv4(source_addr=HAADDR, dest_addr=V4ADDR)
UDP (4500,Y) <Marqueur non ESP> HDR, SK
SA, Nr, [KEr], TSi, TSr}

Si aucun NAT n'est détecté, l'encapsulation utilisée va être :
IPv4 (source_addr=v4CoA, dest_addr=HAAddr)
ESP
IP (source_addr=HoA, set_addr=CNAddr)
HDR de couche supérieure

Où IP est IPv4 ou IPv6 et HoA est l'adresse de rattachement IPv4 ou IPv6.

Si un NAT est détecté, l'encapsulation utilisée va être :
IPv4 (source_addr=v4Addr, dest_addr=HAAddr)
UDP (sport=Y, dport=4500)
ESP
IP (source_addr=HoA, set_addr=CNAddr)
HDR de couche supérieure

Où v4CoA peut être l'adresse IPv4 externe du NAT, IP est un en-tête IPv4 ou IPv6, et HoA est l'adresse de rattachement

IPv4 ou IPv6. Le format ci-dessus montre le paquet comme il est vu par l'agent de rattachement.

Le SPD, qu'un NAT soit détecté ou non, est réglé comme suit. Noter que cette règle est conçue pour confronter toutes les données provenant du MN aux nœuds autres que l'agent de rattachement. Ceci est fait afin que cette règle ne se chevauche pas avec la règle antérieure de sécurisation de la signalisation de BU/BA entre le MN et la HA.

Nœud mobile SPD-S :
SI local_address = home_address &
remote_address != home_agent &
proto=any

Alors utiliser une SA ESP en mode tunnel.

Initier l'utilisation de IDi = user_1 à l'adresse home_agent_1

Agent de rattachement SPD-S :
SI local_address != home_agent &
remote_address = home_address &
proto=any

Alors utiliser une SA ESP en mode tunnel.

Où home_address est l'adresse de rattachement IPv6 ou IPv4 enregistrée du nœud mobile et home_agent est l'adresse IPv6 ou IPv4 de l'agent de rattachement.

6. Constantes du protocole

NATKATIMEOUT = 110 secondes.

7. Remerciements

Merci aux membres (par ordre alphabétique) des groupes de travail MIP6 et NEMO pour leurs contributions, discussions, et relectures : Jari Arkko, Sri Gundavelli, Wassim Haddad, Alfred Hoenes, Conny Larsson, Acee Lindem, Ahmad Muhanna, Vidya Narayanan, Karen Nielsen, et Keiichi Shima. Merci à Karen Nielsen, Pasi Eronen, et Christian Kaas-Petersen qui ont soulevé le problème des interactions de IKEv2 et proposé la solution incluse dans le présent document. Merci à Pasi Eronen pour ses nombreuses relectures attentives du présent document.

8. Considérations relatives à l'IANA

L'IANA a fait les allocations suivantes sur la présente spécification :

L'accès UDP (4191) a été alloué au mécanisme de traversée de NAT décrit au paragraphe 4.2.

La valeur 29 a été allouée à l'option Adresse de rattachement IPv4 décrite au paragraphe 3.1.1. Cette option est incluse dans l'en-tête de mobilité décrit dans la [RFC3775].

La valeur 30 a été allouée à l'option Accusé de réception d'adresse IPv4 décrite au paragraphe 3.2.1. Cette option est incluse dans l'en-tête de mobilité décrit dans la [RFC3775].

La valeur 31 a été allouée à l'option Détection de NAT décrite au paragraphe 3.2.2. Cette option est incluse dans l'en-tête de mobilité décrit dans la [RFC3775].

La valeur 32 a été allouée à l'option Adresse d'entretien IPv4 décrite au paragraphe 3.1.2. Cette option est incluse dans l'en-tête de mobilité décrit dans la [RFC3775].

Le champ Statut dans l'option Adresse de rattachement IPv4 a été alloué par l'IANA sous le nouveau registre "Codes d'état d'option d'adresse de rattachement IPv4 DSMIPv6".

Les valeurs du champ Statut sont allouées en utilisant la procédure suivante :

1. Les nouvelles valeurs de champ Statut sont allouées sur revue de l'IETF. C'est pour tous les types de RFC incluant les statut de "sur la voie de la normalisation", "information", et "expérimental" qui ont pour origine l'IETF et ont été approuvées par l'IESG pour publication.

2. Les demandes d'allocation de nouvelle valeur de type d'option provenant de l'extérieur de l'IETF sont seulement faites par la publication d'un document de l IETF, selon le point 1 ci-dessus. Noter aussi que les documents publiés comme "contributions indépendantes de l'éditeur des RFC" [RFC4844] ne sont pas considérées être des documents de l'IETF.

9. Références

9.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. DOI 10.17487/RFC2119, *(MàJ par* RFC8174)

RFC2473] A. Conta, S. Deering, "Spécification du tunnelage générique de paquet dans IPv6", DOI 10.17487/RFC2473, décembre 1998. *(P.S.)*

[RFC3168] K. Ramakrishnan et autres, "Ajout de la notification explicite d'encombrement (ECN) à IP", DOI 10.17487/RFC3168, septembre 2001. *(P.S. ; MàJ par* RFC8311)

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

[RFC3948] A. Huttunen et autres, "Encapsulation UDP de paquets ESP d'IPsec", janvier 2005. *(P.S.)*

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

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

[RFC4436] B. Aboba et autres, "Détection des rattachements au réseau dans IPv4 (DNAv4)", mars 2006. *(P.S.)*

[RFC4555] P. Eronen, "Protocole IKEv2 de mobilité et de rattachement plusieurs (MOBIKE)", juin 2006. *(P.S.)*

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

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

[RFC5026] G. Giaretta et autres, "Amorçage IPv6 mobile dans un scénario de partage", octobre 2007. *(P.S.)*

9.2 Références pour information

[RFC2983] D. Black, "Services différenciés et tunnels", DOI 10.17487/RFC2983, octobre 2000. *(Information)*

[RFC3344] C. Perkins, éd., "Prise en charge de la mobilité IP pour IPv4", août 2002. (*Obsolète, voir* RFC5944) *(P.S.)*

[RFC3519] H. Levkowetz, S. Vaarala, "Traversée des appareils de traduction d'adresse réseau (NAT) par IP mobile", avril 2003. *(P.S.)*

[RFC4459] P. Savola, "Questions de MTU et de fragmentation liées au tunnelage réseau", avril 2006. *(Information)*

[RFC4844] L. Daigle, éd., Internet Architecture Board, "La série des RFC et l'éditeur des RFC", juillet 2007. *(Information)*

[RFC4977] G. Tsirtsis, H. Soliman, "Position du problème de la mobilité sur les deux piles de protocoles", août 2007. *(Information)*

[RFC5380] H. Soliman et autres, "Gestion de la mobilité dans IPv6 mobile hiérarchisé (HMIPv6)", octobre 2008. (*Remplace* RFC4140) *(P.S.)*

[RFC5389] J. Rosenberg et autres, "Utilitaires de traversée de session pour les NAT (STUN)", octobre 2008, DOI 10.17487/RFC5389. *(P.S. ; remplace* RFC3489 *; remplacée par RFC*8489)

[RFC5405] L. Eggert, G. Fairhurst, "Lignes directrices pour l'utilisation d'UDP en envoi individuel pour les concepteurs d'applications", novembre 2008. (BCP0145 *; MàJ par* RFC8085)

[RFC6611] K. Chowdhury, A. Yegin, "Amorçage de IPv6 mobile (MIPv6) pour le scénario intégré", mai 2012. *(P.S.)*

10. Contributeurs

Le présent document reflète les discussions et contributions de plusieurs personnes incluant (en ordre alphabétique) :
Vijay Devarapalli : vijay.devarapalli@azairenet.com
James Kempf : kempf@docomolabs-usa.com
Henrik Levkowetz : henrik@levkowetz.com
Pascal Thubert : pthubert@cisco.com
George Tsirtsis : G.Tsirtsis@Qualcomm.com
Ryuji Wakikawa : ryuji@sfc.wide.ad.jp

Adresse de l'auteur

Hesham Soliman (éditeur)
Elevate Technologies
mél : hesham@elevatemobile.com