Groupe de travail Réseau
**Request for Comments : 5568**
RFC rendue obsolète : 5268
Catégorie : Sur la voie de la normalisation

R. Koodli, éditeur, Starent Networks

juillet 2009
Traduction Claude Brière de L'Isle

# Transferts IPv6 mobile rapides

**Résumé**
IPv6 mobile permet à un nœud mobile (MN, *Mobile Node*) de maintenir sa connexité à l'Internet quand il se déplace d'un routeur d'accès à un autre, processus appelé un transfert inter cellulaire *(handover)*. Durant un transfert, il y a une période pendant laquelle le nœud mobile est incapable d'envoyer ou recevoir des paquets à cause du délai de commutation de liaison et des opérations du protocole IP. Cette "latence de transfert" résultant des procédures standard de IPv6 mobile (à savoir la détection de mouvement, la nouvelle configuration d'adresse d'entretien, et la mise à jour de lien) est souvent inacceptable pour le trafic en temps réel comme la voix sur IP (VoIP, *Voice over IP*). Réduire la latence de transfert pourrait être bénéfique aussi pour les applications non en temps réel, sensibles au débit. Le présent document spécifie un protocole pour améliorer la latence de transfert due aux procédures de IPv6 mobile. Le présent document ne traite pas de l'amélioration de la latence de commutation de liaison.

Le présent document met à jour les formats de paquet pour les messages Initiation de transfert (HI, *Handover Initiate*) et Accusé de réception de transfert (Hack, *Handover Acknowledge*) dans le type d'en-tête de mobilité.

**Statut de ce 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.

Le présent document a été produit par l'équipe d'ingénierie de l'Internet (IETF). Il représente le consensus de la communauté de l'IETF. Il a subi une révision publique et sa publication a été approuvée par le groupe de pilotage de l'ingénierie de l'Internet (IESG). Tous les documents approuvés par l'IESG ne sont pas candidats à devenir une norme de l'Internet ; voir la Section 2 de la RFC5741.

Les informations sur le statut actuel du présent document, tout errata, et comment fournir des réactions sur lui peuvent être obtenues à http://www.rfc-editor.org/info/rfc5568



## Table des matières

1. Introduction....2
2. Terminologie....3
3. Vue d'ensemble du protocole....4
  3.1 traitement de la latence de transfert....4
  3.2 Fonctionnement du protocole....5
  3.3 Fonctionnement du protocole durant le transfert inititié par le réseau....7
4. Détails du protocole....7
5. Autres considérations....9
  5.1 Échange de capacités de transfert....9
  5.2 Détermination de la nouvelle adresse d'entretien....9
  5.3 Gestion de préfixe....10
  5.4 Perte de paquet....10
  5.5 Traitement de DAD....11
  5.6 Mouvement rapide ou erroné....11

6. Formats de message ....11
6.1 Nouveaux messages de découverte de voisin....12
6.2 Nouveaux messages d'en-tête de mobilité....14
6.3 Annonce de voisin non sollicitée (UNA)....19
6.4 Nouvelles options....19
7. Considérations relatives au protocole et à l'appareil....23
8. Évolution et compatibilité par rapport à la RFC 4068....23
9. Paramètres configurables....24
10. Considérations sur la sécurité....25
10.1 Entrées de base de données d'authorisation d'homologue avec IKEv2....26
10.2 Entrées de base de données de politique de sécurité....26
11. Considérations relatives à l'IANA ....27
12. Remerciements....27
13. Références....27
13.1 Références normatives....27
13.2 Références pour information....28
Appendice A. Contributeurs....29
Appendice B. Changements depuis la RFC 5268....29
Appendice C. Changements depuis la RFC 4068....29
Adresse de l'auteur....30

## 1. Introduction

IPv6 mobile [RFC3775] décrit les opérations de protocole pour qu'un nœud mobile maintienne la connexité à l'Internet durant son transfert d'un routeur d'accès à un autre. Ces opérations impliquent des procédures de couche de liaison, la détection de mouvement, la configuration d'adresse IP, et la mise à jour de localisation. La latence de transfert combinée est souvent suffisante pour affecter les applications en temps réel. Les applications sensibles au débit peuvent aussi tirer profit de la réduction de cette latence. Ce document décrit un protocole pour réduire la latence de transfert.

La présente spécification traite des problèmes suivants : comment permettre à un nœud mobile d'envoyer des paquets aussitôt qu'il détecte une nouvelle liaison de sous réseau et comment livrer des paquets à un nœud mobile aussitôt que son rattachement est détecté par le nouveau routeur d'accès. Le protocole définit les messages du protocole IP nécessaires pour son fonctionnement sans considération de la technologie de la liaison. Il fait cela sans dépendre de caractéristiques spécifiques de la couche de liaison tout en permettant une personnalisation spécifique de la liaison. Par définition, la présente spécification prend en compte les transferts qui interagissent avec IP mobile. Une fois rattaché à son nouveau routeur d'accès, un MN engage les opérations IP mobile incluant l'acheminement de retour [RFC3775]. Il n'y a pas d'exigence particulière qu'un nœud mobile se comporte différemment par rapport à son fonctionnement dans IP mobile standard.

La présente spécification est applicable quand un nœud mobile doit effectuer des opérations de couche IP par suite de transferts. Elle ne traite pas de l'amélioration de la latence de commutation de liaison. Elle ne modifie pas ni n'optimise les procédures relatives à la signalisation avec l'agent de rattachement d'un nœud mobile. Bien sûr, quoique ciblant IPv6 mobile, elle pourrait être utilisée avec tout mécanisme qui permet à la communication de continuer en dépit des mouvements. Finalement, cette spécification ne traite pas du mouvement brut des nœuds qui utilisent des préfixes agrégés.

Le présent document met à jour le format d'en-tête de protocole pour les messages Initier le transfert (HI, *Handover Initiate*) et Accusé de réception de transfert (HAck, *Handover Acknowledge*) définis dans la [RFC5268]. Le protocole de mandataire IPv6 mobile (PMIPv6, *Proxy IPv6 mobile*) [RFC5213] et le protocole IPv6 mobile utilisent tous deux l'en-tête de mobilité (MH, *Mobility Header*) comme type pour porter la signalisation relative à la mise à jour de chemin. Bien que le protocole de transfert rapide utilise l'en-tête de mobilité pour les besoins de la signalisation du nœud mobile, il a utilisé ICMP pour la communication inter routeurs d'accès. Spécifier l'en-tête de mobilité pour les messages HI et HAck permet le déploiement du protocole à côté des protocoles PMIP6 et MIP6 ; les raisons qui ont conduit à ce changement sont décrites à l'Appendice B. Donc, le présent document spécifie les formats d'en-tête de mobilité pour les messages HI et HAck (paragraphe 6.2.1) et le format de l'option d'en-tête de mobilité pour l'option Adresse/préfixe IPv6 (paragraphe 6.4.2) et déconseille l'utilisation de ICMP pour les messages HI et HAck. Les mises en œuvre de cette spécification NE DOIVENT PAS envoyer de messages ICMPv6 HI et HAck comme défini dans la [RFC5268]. Si les mises en œuvre de cette spécification reçoivent des messages ICMPv6 HI et HAck comme défini dans la [RFC5268], elles PEUVENT interpréter les messages comme défini dans la [RFC5268].

## 2. Terminologie

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

L'utilisation du terme "ignore en silence" n'est pas définie dans la RFC 2119. Cependant, ce terme est utilisé dans ce document et peut être construit de façon similaire.

La terminologie et les abréviations suivantes sont utilisées dans ce document en plus de celles définies dans la [RFC3775]. Le scénario de transfert de référence est illustré dans la Figure 1.

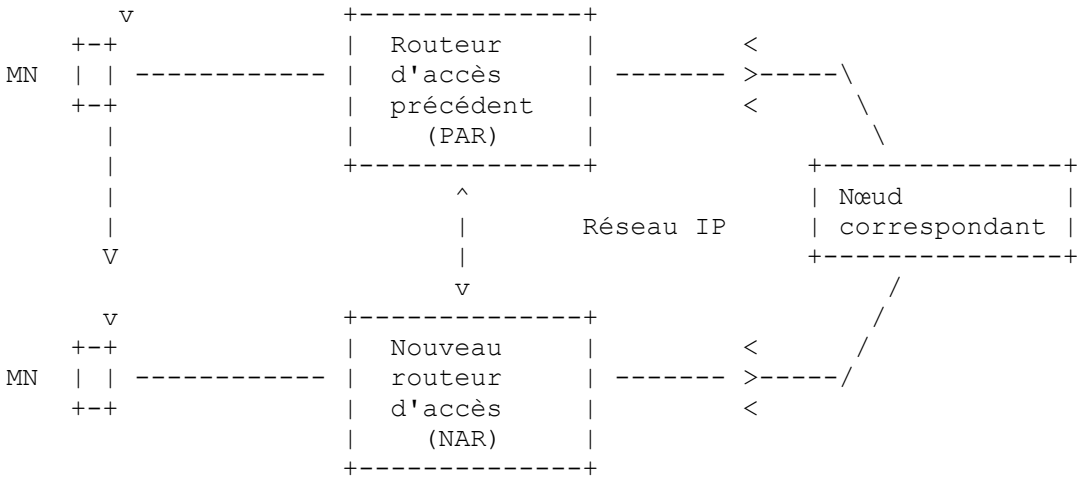


**Figure 1 : Scénario de référence pour transfert**

MN *(Mobile Node)* : nœud mobile, hôte IPv6 mobile.

AP *(Access Point)* : point d'accès. Appareil de couche 2 connecté à un sous réseau IP qui offre la connexité sans fil à un MN. Un identifiant de point d'accès (AP-ID, *Access Point Identifier*) se réfère à l'adresse de couche 2 du point d'accès. Parfois, AP-ID est aussi appelé un identifiant d'ensemble de services de base (BSSID, *Basic Service Set IDentifier*).

AR *(Access Router)* : routeur d'accès, le routeur par défaut du MN.

PAR *(Previous Access Router)* : routeur d'accès précédent, le routeur par défaut du MN avant son transfert.

NAR *(New Access Router)* : nouveau routeur d'accès, le routeur par défaut prévu du MN suite à son transfert.

PCoA *(Previous CoA)* : adresse d'entretien précédente, l'adresse d'entretien du MN valide sur le sous réseau du PAR.

NCoA *(New CoA)* : nouvelle adresse d'entretien, l'adresse d'entretien du MN valide sur le sous réseau du NAR.

Transfert : processus de terminaison de la connexité existante et d'obtention d'une nouvelle connexité IP.

RtSolPr *(Router Solicitation for Proxy Advertisement)* : sollicitation de routeur pour annonce de mandataire, message du MN au PAR demandant des informations pour un potentiel transfert.

PrRtAdv *(Proxy Router Advertisement)* : annonce de routeur mandataire. Message du PAR au MN qui donne des informations sur les liaisons du voisinage qui facilitent la détection de mouvement. Le message peut aussi agir comme déclencheur d'un transfert initié par le réseau.

Couple [AP-ID, AR-Info] : contient les adresses IP et de couche 2 d'un routeur d'accès, et le préfixe valide sur l'interface à laquelle est rattaché le point d'accès (identifié par l'AP-ID). Le triplet [adresse de couche 2 du routeur, adresse IP du routeur, et préfixe] est appelé "AR-Info". Voir aussi le paragraphe 5.3.

Découverte de voisin : processus de résolution des AP-ID du voisinage en AR-Info.

Adressage alloué : type particulier de configuration de nouvelle adresse d'entretien dans laquelle le NAR alloue une adresse IPv6 pour le MN. La méthode par laquelle le NAR gère son réservoir d'adresses n'est pas spécifié dans ce document.

FBU *(Fast Binding Update)* : mise à jour rapide de lien, message du MN ordonnant à son PAR de rediriger son trafic (vers le NAR).

FBack *(Fast Binding Acknowledgment)* : accusé de réception de lien rapide, message du PAR en réponse à une FBU.

Transfert rapide prédictif : transfert rapide dans lequel un MN est capable d'envoyer une FBU quand il est rattaché au PAR, qui établit alors la transmission de son trafic (même avant que le MN se rattache au NAR).

Transfert rapide réactif : transfert rapide dans lequel un MN n'est capable d'envoyer la FBU qu'après s'être rattaché au NAR.

UNA *(Unsolicited Neighbor Advertisement)* : annonce de voisin non sollicitée, message de découverte de voisin avec le bit 'O' à zéro.

FNA *(Fast Neighbor Advertisement)* : annonce de voisin rapide ; ce message de la [RFC4068] est déconseillé. Le message UNA est le message préféré dans cette spécification.

HI *(Handover Initiate)* : initier le transfert ; message du PAR au NAR concernant un transfert de MN.

HAck *(Handover Acknowledge)* : accusé de réception de transfert ; message du NAR au PAR en réponse à HI.

## 3. Vue d'ensemble du protocole

### 3.1 Traitement de la latence de transfert

La capacité d'envoyer immédiatement des paquets à partir d'une nouvelle liaison de sous réseau dépend de la latence de la "connexité IP", qui à son tour dépend de la latence de la détection de mouvement et de la latence de la configuration de la nouvelle adresse d'entretien. Une fois qu'une MN a la capacité IP sur la nouvelle liaison de sous réseau, elle peut envoyer une mise à jour de lien à son agent de rattachement et à un ou plusieurs correspondants. Une fois que les correspondants ont réussi à traiter la mise à jour de lien, ce qui implique normalement la procédure de capacité d'acheminement de retour *(Return Routability)* le MN peut recevoir des paquets à la nouvelle adresse d'entretien. Donc, la capacité de recevoir des paquets des correspondants directement à sa nouvelle CoA dépend de la latence de la mise à jour de lien ainsi que de la latence de la connexité IP.

Le protocole permet à un MN de détecter rapidement qu'il s'est déplacé à un nouveau sous réseau en donnant les informations de nouveau point d'accès et de préfixe de sous réseau associé quand le MN est encore connecté à son sous réseau actuel (c'est-à-dire, le PAR à la Figure 1). Par exemple, un MN peut découvrir les points d'accès disponibles en utilisant des mécanismes spécifique de la couche de liaison (par exemple, un "scan" dans un réseau de zone locale sans fil (WLAN, *Wireless Local Area Network*)) et ensuite demander les informations de sous réseau correspondant à un ou plusieurs de ces points d'accès découverts. Le MN peut faire cela après avoir effectué la découverte de routeur ou à tout moment pendant qu'il est connecté à son routeur actuel. Le résultat de la résolution d'un identifiant associé à un point d'accès est un couple [AP-ID, AR-Info], qu'un MN peut utiliser pour détecter directement le mouvement. Quand le rattachement à un point d'accès avec AP-ID a lieu, le MN connaît les coordonnées correspondantes du nouveau routeur, incluant son préfixe, adresse IP, et adresse de couche 2. Les messages "Sollicitation de routeur pour annonce de mandataire (RtSolPr)" et "Annonce de routeur mandataire (PrRtAdv)" du paragraphe 6.1 sont utilisés pour aider à la détection de mouvement.

Avec les messages RtSolPr et PrRtAdv, le MN formule aussi une nouvelle adresse d'entretien (NCoA) prospective quand il est encore présent sur la liaison du PAR. Donc, la latence due à la découverte du nouveau préfixe suivant le transfert est éliminée. De plus, cette adresse prospective peut être utilisée immédiatement après le rattachement à la nouvelle liaison de sous réseau (c'est-à-dire, la liaison du NAR) quand le MN a reçu un message d'accusé de réception de lien rapide (Fback, *Fast Binding Acknowledgment*) (voir au paragraphe 6.2.3) avant son mouvement. Dans le cas où il se déplace sans recevoir de FBack, le MN peut encore commencer en utilisant la NCoA après avoir annoncé son rattachement par un message d'annonce de voisin non sollicitée (avec le bit 'O' réglé à zéro) [RFC4861] ; le NAR répond à ce message UNA dans le cas où il souhaite fournir une adresse IP différente à utiliser. De cette façon, la latence de configuration de la NCoA est réduite.

Les informations fournies dans le message PrRtAdv peuvent être utilisées même quand DHCP [RFC3315] est utilisé pour configurer une NCoA sur la liaison du NAR. Dans ce cas, le protocole prend en charge la transmission en utilisant la PCoA, et le MN effectue DHCP une fois qu'il se rattache à la liaison du NAR. Le MN formule quand même une NCoA pour le traitement de la FBU ; cependant, il NE DOIT PAS envoyer de paquets de données en utilisant la NCoA dans la FBU.

Afin de réduire la latence de la mise à jour de lien, le protocole spécifie un lien entre la précédente CoA (PCoA) et la NCoA. Un MN envoie un message de "mise à jour rapide de lien" (voir le paragraphe 6.2.2) à son routeur d'accès précédant pour établir ce tunnel. Quand c'est faisable, le MN DEVRAIT envoyer une FBU à partir de la liaison du PAR. Autrement, le MN devrait envoyer la FBU immédiatement après avoir détecté le rattachement au NAR. Un message de FBU DOIT contenir l'option Données d'autorisation de lien pour FMIPv6 (BADF, *Binding Authorization Data for FMIPv6*) (voir au paragraphe 6.4.5) afin de s'assurer que seul un MN légitime qui possède la PCoA est capable d'établir un lien. Les paragraphes qui suivent décrivent la mécanique du protocole. Dans tous les cas, le résultat est que le PAR commence à tunneler les paquets qui arrivent pour la PCoA à la NCoA. Un tel tunnel reste actif jusqu'à ce que le MN termine la mise à jour de lien avec ses correspondants. Dans la direction opposée, le MN DEVRAIT inverser le tunnel de paquets au PAR, jusqu'à ce qu'il achève la mise à jour de lien. Et, le PAR DOIT transmettre le paquet interne dans le tunnel à sa destination (c'est-à-dire, au correspondant du MN). Un tel tunnel inverse assure que les paquets qui contiennent une PCoA comme adresse IP de source ne sont pas éliminés à cause du filtrage d'entrée. Même si le MN a la capacité IP sur la nouvelle liaison, il ne peut pas utiliser directement la NCoA avec ses correspondants sans que les correspondants établissent d'abord une entrée d'antémémoire de lien (pour la NCoA). La prise en charge de la transmission pour la PCoA est fournie par un tunnel inverse entre le MN et le PAR.

Établir un tunnel seul n'assure pas que le MN reçoive les paquets aussitôt qu'il est rattaché à une nouvelle liaison de sous réseau, sauf si le NAR peut détecter la présence du MN. Une opération de découverte de voisin impliquant une résolution d'adresse de voisin (c'est-à-dire, Sollicitation de voisin et Annonce de voisin) résulte normalement en de considérables délais, durant parfois plusieurs secondes. Par exemple, quand l'arrivée de paquets déclenche chez le NAR l'envoi d'une sollicitation de voisin avant que le MN se rattache, les retransmissions suivantes de la résolution d'adresse sont séparées par une période par défaut d'une seconde chacune. Afin de contourner ce délai, un MN annonce son rattachement immédiatement avec un message UNA qui permet au NAR de transmettre directement les paquets au MN. Par l'établissement du tunnel pour la PCoA et l'annonce rapide, le protocole fournit une transmission expéditive des paquets au MN.

Le protocole fournit aussi les fonctions importantes suivantes. Les routeurs d'accès peuvent échanger des messages pour confirmer qu'une NCoA proposée est acceptable. Par exemple, quand un MN envoie une FBU d'une liaison du PAR, le FBack peut être livré après que le NAR considère que la NCoA est acceptable. Ceci est particulièrement utile quand les adresses sont allouées par le routeur d'accès. Le NAR peut aussi s'appuyer sur sa relation de confiance avec le PAR avant de fournir la prise en charge de la transmission pour le MN. C'est-à-dire, il peut créer une entrée de transmission pour la NCoA, sous réserve de "l'approbation" du PAR, qui est de confiance. De plus, la mise en mémoire tampon du trafic de transfert au NAR peut être souhaitable. Bien que le protocole de découverte de voisin fournisse une petite mémoire tampon (normalement d'un ou deux paquets) pour les paquets qui attendent la résolution d'adresse, cette mémoire tampon peut être inadéquate pour le trafic, comme celui de VoIP, déjà en cours. Les routeurs peuvent aussi souhaiter maintenir une mémoire tampon séparée pour servir le trafic de transfert. Finalement, les routeurs d'accès pourraient transférer les contextes résidents sur le réseau, comme le contrôle d'accès, la qualité de service (QS) et la compression d'en-tête, en conjonction avec le transfert (bien que le processus de transfert de contexte lui-même ne soit pas spécifié dans ce document). Pour toutes ces opérations, le protocole fournit les messages "Initier le transfert (HI)" et "Accusé de réception de transfert (HAck)" (voir le paragraphe 6.2.1). Ces deux messages DEVRAIENT être utilisés. Les routeurs d'accès DOIVENT avoir les associations de sécurité nécessaires établies par des moyens qui sortent du domaine d'application de ce document.

### 3.2 Fonctionnement du protocole

Le protocole commence quand un MN envoie un message RtSolPr à son routeur d'accès pour résoudre un ou plusieurs identifiants de point d'accès en informations spécifiques du sous réseau. En réponse, le routeur d'accès (par exemple, le PAR dans la Figure 1) envoie un message PrRtAdv contenant un ou plusieurs couples [AP-ID, AR-Info]. Le MN peut envoyer un RtSolPr à tout moment qui lui convient, par exemple en réponse à un événement spécifique de la liaison (un "déclencheur") ou simplement après avoir effectué une découverte de routeur. Cependant, on s'attend à ce que avant d'envoyer un message RtSolPr, le MN ait découvert les points d'accès disponibles par des méthodes spécifiques de la liaison. Les messages RtSolPr et PrRtAdv n'établissent aucun état au routeur d'accès ; leur format de paquet est défini au paragraphe 6.1.

Avec les informations fournies dans le message PrRtAdv, le MN formule une NCoA prospective et envoie un message de FBU au PAR. L'objet de la FBU est d'autoriser le PAR à lier la PCoA à la NCoA, afin que les paquets arrivants puissent être tunnelés à la nouvelle localisation du MN. La FBU devrait être envoyée de la liaison du PAR chaque fois que c'est faisable. Par exemple, un déclenchement interne spécifique de la liaison pourrait permettre la transmission de la FBU à partir de la liaison précédente.

Quand ce n'est pas faisable, la FBU est envoyée de la nouvelle liaison.

Le format et la sémantique du traitement de la FBU sont spécifiés au paragraphe 6.2.2. Le message de FBU DOIT contenir l'option BADF (voir au paragraphe 6.4.5) pour sécuriser le message.

Selon qu'un FBack est reçu sur la liaison précédente (ce qui dépend clairement de si la FBU a été envoyée en premier) il y a deux modes de fonctionnement.

1. Le MN reçoit le FBack sur la liaison précédente. Cela signifie que le tunnelage de paquets est déjà en cours au moment où le MN passe au NAR. Le MN DEVRAIT envoyer la UNA immédiatement après son rattachement au NAR, afin que les paquets arrivants ainsi que les paquets en mémoire tampon puissent être transmis tout de suite au MN. Avant d'envoyer un FBack au MN, le PAR peut déterminer si la NCoA est acceptable pour le NAR par l'échange des messages HI et HAck. Quand l'adressage alloué (c'est-à-dire, où les adresses sont allouées par le routeur) est utilisé, la NCoA proposée dans la FBU est portée dans un message HI (du PAR au NAR) et le NAR PEUT allouer la NCoA proposée. Une telle NCoA allouée DOIT être retournée dans la HAck (du NAR au PAR) et le PAR DOIT à son tour fournir la NCoA allouée dans le FBack. Si il y a une NCoA allouée retournée dans la FBack, le MN DOIT utiliser l'adresse allouée (et non l'adresse proposée dans la FBU) lorsque il se rattache au NAR.

2. Le MN ne reçoit pas le FBack sur la liaison précédente parce que le MN n'a pas envoyé la FBU ou qu'il a quitté la liaison après l'envoi de la FBU (qui peut elle-même être perdue) mais avant de recevoir un FBack. Sans réception d'un FBack dans ce dernier cas, le MN ne peut pas être certain que le PAR a traité avec succès la FBU. Donc, le MN envoie à nouveau le message de FBU au PAR immédiatement après l'envoi du message UNA. Si le NAR choisit de fournir une adresse IP différente de la NCoA à utiliser, il PEUT envoyer une annonce de routeur avec l'option "accusé de réception d'annonce de voisin" (NAACK, *Neighbor Advertisement Acknowledge*) dans laquelle il va inclure une autre adresse IP pour que le MN l'utilise. Les règles détaillées de traitement de UNA sont spécifiées au paragraphe 6.3.

Le scénario dans lequel un MN envoie une FBU et reçoit un FBack sur la liaison du PAR est illustré à la Figure 2. Pour des raisons pratiques, ce scénario est caractérisé comme le mode de fonctionnement "prédictif". Le scénario dans lequel le MN envoie une FBU à partir de la liaison du NAR est illustrée à la Figure 3. Pour les mêmes raisons, ce scénario est appelé le mode de fonctionnement "réactif". Noter que le mode réactif inclut aussi le cas dans lequel une FBU a été envoyée de la liaison du PAR, mais un FBack n'a pas encore été reçu. La figure est destinée à illustrer que la FBU est transmise à travers le NAR, mais elle n'est traitée que par le PAR.

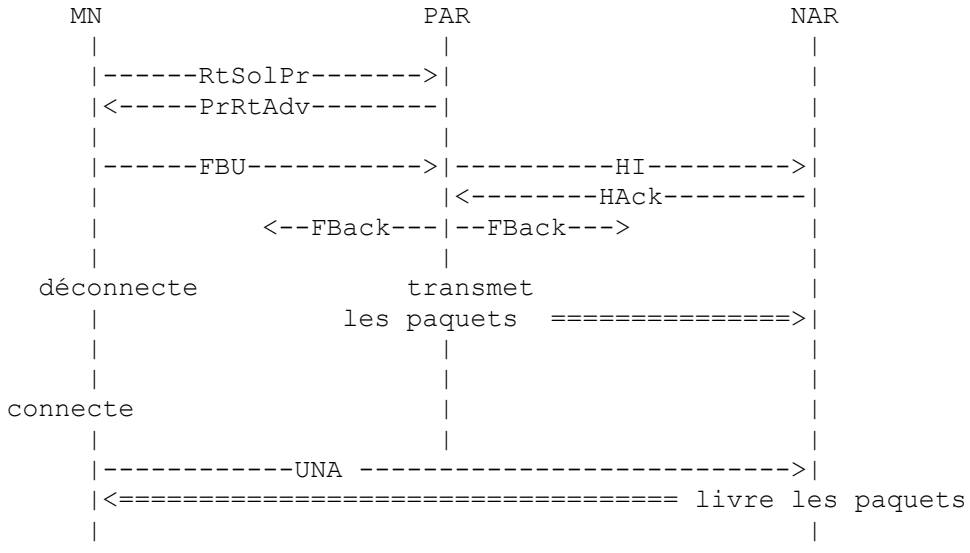


**Figure 2 : Transfert rapide prédictif**

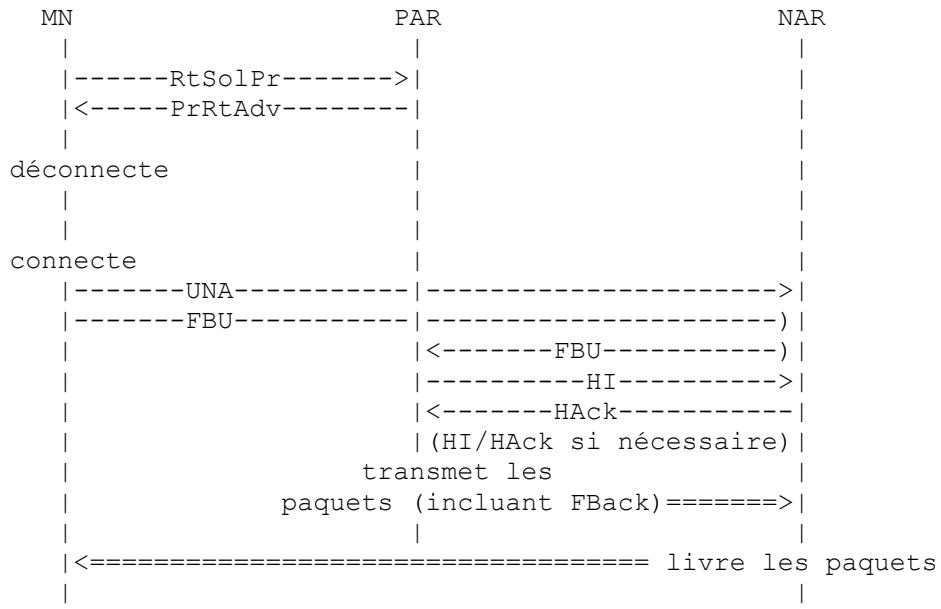


**Figure 3 : Transfert rapide réactif**

Finalement, le message PrRtAdv peut être envoyé non sollicité, c'est-à-dire, sans que le MN envoie d'abord un RtSolPr. Ce mode est décrit au paragraphe 3.3.

### 3.3 Fonctionnement du protocole durant le transfert inititié par le réseau

Dans certaines technologies sans fil, le contrôle du transfert peut résider dans le réseau même si la décision d'entreprendre le transfert peut être mutuellement arrangée entre le MN et le réseau. Dans de tels réseaux, le PAR peut envoyer une PrRtAdv non sollicitée contenant l'adresse de couche de liaison, l'adresse IP, et le préfixe de sous réseau du NAR quand le réseau décide qu'un transfert est imminent. Le MN DOIT traiter cette PrRtAdv pour configurer une nouvelle adresse d'entretien sur le nouveau sous réseau et DOIT envoyer une FBU au PAR avant de passer à la nouvelle liaison. Après avoir transmis la PrRtAdv, le PAR DOIT continuer de transmettre les paquets au MN sur sa liaison courante jusqu'à ce que la FBU soit reçue. Le reste de l'opération est le même que décrit au paragraphe 3.2.

La PrRtAdv non sollicitée permet aussi au réseau d'informer le MN sur les sous réseaux géographiquement adjacents sans que le MN ait à demander explicitement ces informations. Cela peut réduire la quantité de trafic sans fil requis pour que le MN obtienne une carte topologique du voisinage des liaisons et sous réseaux. Un tel usage de PrRtAdv est découplé du transfert réel ; voir au paragraphe 6.1.2.

## 4. Détails du protocole

Toutes les descriptions se réfèrent à la Figure 1.

Après avoir découvert un ou plusieurs points d'accès du voisinage, le MN envoie un message RtSolPr au PAR afin de résoudre les identifiants de point d'accès en informations de routeur de sous réseau. Un moment approprié pour faire cela est après avoir effectué la découverte de routeur. Cependant, le MN peut envoyer le RtSolPr à tout moment, par exemple, quand un ou plusieurs nouveaux points d'accès sont découverts. Le MN peut aussi envoyer le RtSolPr plus d'une fois durant son rattachement au PAR. Le déclencheur pour l'envoi de RtSolPr peut avoir son origine dans un événement spécifique de la liaison, comme la promesse d'un signal plus fort provenant d'un autre point d'accès couplé avec une qualité de signal faiblissante sur le point d'accès actuel. De tels événements, souvent appelés des "déclencheurs de couche 2", sortent du domaine d'application de ce document. Néanmoins, ils servent d'événements qui invoquent ce protocole. Par exemple, quand une indication "liaison active" est obtenue sur la nouvelle liaison, les messages de protocole (par exemple, UNA) peuvent être immédiatement transmis. Les mises en œuvre DEVRAIENT utiliser de tels déclencheurs chaque fois qu'ils sont disponibles.

Le message RtSolPr contient un ou plusieurs AP-ID. Un caractère générique demande tous les couples disponibles.

En réponse à RtSolPr, le PAR envoie un message PrRtAdv qui indique une des conditions possibles suivantes :

1. Si le PAR n'a pas d'entrée correspondant au nouveau point d'accès, il DOIT répondre en indiquant que le nouveau point d'accès est inconnu. Le MN DOIT arrêter les opérations de protocole de transfert rapide sur la liaison en cours. Le MN PEUT envoyer une FBU à partir de sa nouvelle liaison.

2. Si le nouveau point d'accès est connecté à l'interface courante du PAR (à laquelle le MN est rattaché) le PAR DOIT répondre avec une valeur de code indiquant que le nouveau point d'accès est connecté à l'interface courante, mais ne pas envoyer d'informations de préfixe. Ce scénario pourrait survenir, par exemple, quand plusieurs points d'accès sans fil sont pontés dans un réseau filaire. Aucune autre action du protocole n'est nécessaire.

3. Si le nouveau point d'accès est connu et si le PAR a des informations sur lui, alors le PAR DOIT répondre en indiquant que le nouveau point d'accès est connu et fournir le couple [AP-ID, AR-Info]. Si le nouveau point d'accès est connu, mais ne prend pas en charge le transfert rapide, le PAR DOIT l'indiquer avec le code 3 (voir au paragraphe 6.1.2).

4. Si un caractère générique est fourni comme identifiant pour le nouveau point d'accès, le PAR DEVRAIT fournir les couples [AP-ID, AR-Info] du voisinage qui sont sujets à des restriction de la MTU de chemin (c'est-à-dire, fournir des couples 'n' sans excéder la MTU de la liaison).

Quand d'autres actions du protocole sont nécessaires, certaines mises en œuvre PEUVENT choisir de commencer à mettre en mémoire tampon des copies des paquets entrants au PAR. Si une mise en mémoire tampon de type "premier entré, premier sorti" (FIFO, *First In First Out*) est utilisé, le PAR DOIT continuer la transmission des paquets à la PCoA (c'est-à-dire, mettre en mémoire tampon et transmettre). Bien que le protocole n'interdise pas une telle mise en œuvre, il faut veiller à s'assurer que le PAR continue de transmettre les paquets à la PCoA (c'est-à-dire, utilise l'approche de mise en mémoire tampon et transmission). Le PAR DEVRAIT arrêter la mise en mémoire tampon quand il commence à transmettre les paquets à la NCoA.

La méthode par laquelle les routeurs d'accès échangent des informations sur leurs voisins et permettent ainsi la construction des annonces de routeur mandataire avec des informations sur les sous réseaux du voisinage sort du domaine d'application du présent document.

Les messages RtSolPr et PrRtAdv DOIVENT être mis en œuvre par un MN et un routeur d'accès qui prennent en charge les transferts rapides. Cependant, quand les paramètres nécessaires pour que le MN envoie les paquets immédiatement après le rattachement au NAR sont fournis par le mécanisme de transfert de couche de liaison lui-même, l'utilisation de ces messages est facultative sur ces liaisons.

Après le traitement d'un message PrRtAdv, le MN envoie une FBU à un moment déterminé par des événements spécifiques de la liaison, et inclut la NCoA proposée. Le MN DEVRAIT envoyer la FBU à partir de la liaison du PAR chaque fois que "l'anticipation" de transfert est faisable. Quand l'anticipation n'est pas faisable ou quand il n'a pas reçu de FBack, le MN envoie une FBU immédiatement après s'être rattaché à la liaison du NAR. En réponse à la FBU, le PAR établit un lien entre la PCoA ("Adresse de rattachement") et la NCoA, et envoie le FBack au MN. Avant d'établir ce lien, le PAR DEVRAIT envoyer un message HI au NAR, et recevoir un HAck en réponse. Afin de déterminer l'adresse du NAR pour le message HI, le PAR peut effectuer une confrontation de plus long préfixe de la NCoA (dans la FBU) avec la liste de préfixes des routeurs d'accès du voisinage. Quand l'adresse IP de source de la FBU est la PCoA, c'est-à-dire, quand la FBU est envoyée de la liaison du PAR, le message HI DOIT avoir sa valeur de code réglée à 0 ; voir au paragraphe 6.2.1.1. Quand l'adresse IP de source de la FBU n'est pas la PCoA, c'est-à-dire, quand la FBU est envoyée de la liaison du NAR, le message HI DOIT avoir une valeur de code de 1 ; voir au paragraphe 6.2.1.1.

Le message HI contient la PCoA, l'adresse de couche de liaison et la NCoA du MN. En réponse au traitement d'un message HI avec le code 0, le NAR :

1. Détermine si la NCoA fournie dans le message HI est unique avant de commencer )à la défendre. Il envoie une sonde de détection d'adresse dupliquée (DAD, *Duplicate Address Detection*) [RFC4862] pour la NCoA pour vérifier l'unicité. Cependant, dans les déploiements où la probabilité de collisions d'adresses est considérée comme extrêmement faible (et donc ne pas être un problème) le paramètre DupAddrDetectTransmits (voir la [RFC4862]) est réglé à zéro sur le NAR, lui permettant d'éviter d'effectuer la DAD sur la NCoA. Le NAR règle de façon similaire DupAddrDetectTransmits à zéro dans les autres déploiements où la DAD n'est pas un problème. Une fois la NCoA déterminée comme unique, le NAR commence à déléguer [RFC4861] l'adresse pour une durée de PROXY_ND_LIFETIME durant laquelle le MN est supposé se connecter au NAR. Dans le cas où une NCoA est déjà présente dans sa structure de données (par exemple, il a déjà traité un message HI plus tôt) le NAR PEUT vérifier si la LLA est la même que la sienne propre ou celle du MN lui-même. Si il en est ainsi, le NAR PEUT permettre l'utilisation

de la NCoA.

2. Alloue la NCoA pour le MN quand Adressage alloué est utilisé, crée une entrée d'antémémoire de voisin mandataire, et commence à la défendre. Le NAR PEUT allouer la NCoA proposée dans HI.

3. PEUT créer une entrée de chemin d'hôte pour la PCoA (sur l'interface sur laquelle le MN se rattache) dans le cas où la NCoA ne peut pas être acceptée ou allouée. Cette entrée de chemin d'hôte DEVRAIT être mise en œuvre de telle façon que jusqu'à ce que la présence du MN soit détectée, par annonce explicite du MN ou par d'autres moyens, les paquets arrivants n'invoquent pas la découverte de voisin. Dans ce cas le NAR DEVRAIT aussi établir un tunnel inverse au PAR.

4. Fournir l'état de la demande de transfert dans le message Accusé de réception de transfert (HAck) pour le PAR.

Quand la valeur de code dans HI est 1, le NAR DOIT sauter les opérations ci-dessus. Envoyer un message HI avec le code 1 permet au NAR de valider l'entrée d'antémémoire de voisin qu'il crée pour le MN durant le traitement de UNA. C'est-à-dire, le NAR peut utiliser la connaissance que son homologue de confiance (c'est-à-dire, le PAR) a une relation de confiance avec le MN.

Si HAck contient une NcoA allouée, le FBack DOIT l'inclure, et le MN DOIT utiliser l'adresse fournie dans le FBack. Le PAR PEUT aussi envoyer le FBack à la liaison précédente pour faciliter une réception plus rapide dans le cas où le MN serait encore présent. Le résultat du traitement de la FBU et de FBack est que le PAR commence à tunneler les paquets du MN à la NCoA. Si le MN ne reçoit pas un message FBack même après la retransmission de la FBU pour FBU_RETRIES, il doit supposer que la prise en charge du transfert rapide n'est pas disponible et arrêter le fonctionnement du protocole.

Aussitôt que le MN établit la connexité de la liaison avec le NAR, il :
1. envoie un message UNA (voir au paragraphe 6.3). Si le MN n'a pas reçu de FBack au moment de l'envoi de l'UNA, il DEVRAIT envoyer un message FBU à la suite du message UNA,
2. se joint au groupe de diffusion groupée Tous les nœuds et au groupe de diffusion groupée Nœud sollicité correspondant à la NCoA,
3. commence une sonde de DAD pour la NcoA ; voir la [RFC4862].

Quand un NAR reçoit un message UNA, il :
1. Supprime son entrée d'antémémoire de voisin mandataire, si elle existe, met à jour l'état à STALE *(périmé)* [RFC4861], et transmet les paquets arrivants et en mémoire tampon.
2. Met à jour une entrée dans l'état INCOMPLET [RFC4861], si il en existe, en STALE et transmet les paquets arrivants et en mémoire tampon. Cela serait le cas si le NAR avait précédemment envoyé une sollicitation de voisin qui serait restée sans réponse peut-être parce que le MN n'était pas encore rattaché à la liaison.

La mémoire tampon pour le trafic de transfert devrait être liée à ce traitement de UNA. Le mécanisme exact dépend de la mise en œuvre.

Le NAR peut choisir de fournir une adresse IP différente de la NCoA. Cela est possible si il est mandataire pour la NCoA. Dans ce cas, il PEUT envoyer une annonce de routeur avec l'option NAACK dans laquelle il inclut une autre adresse IP à utiliser. Ce message DOIT être envoyé à l'adresse IP de source présente dans l'UNA en utilisant la même adresse de couche 2 que présente dans l'UNA.

Si le MN reçoit une adresse IP dans l'option NAACK, il DOIT l'utiliser et envoyer une FBU en utilisant la nouvelle CoA. Dans un cas particulier, l'adresse fournie dans le NAACK pourrait être la PCoA elle-même, et alors le MN NE DOIT PAS envoyer d'autre FBU. Les codes d'état pour l'option NAACK sont spécifiés au paragraphe 6.4.6.

Une fois que le MN a confirmé sa NCoA (par une DAD ou quand elle est fournie par le NAR) il DEVRAIT envoyer un message d'annonce de voisin avec le bit 'O' établi, à l'adresse de diffusion groupée Tous les nœuds. Ce message permet aux voisins du MN de mettre à jour leurs entrées d'antémémoire de voisins.

Pour la transmission des données, le PAR tunnelle les paquets en utilisant son adresse IP mondiale valide sur l'interface à laquelle le MN était rattaché. Le MN tunnelle à l'inverse ses paquets à la même adresse mondiale du PAR. Les adresses de bout en bout du tunnel doivent être configurées en conséquence. Quand le PAR reçoit un paquet du tunnel inverse, il doit vérifier si un lien sûr existe pour le MN identifié par la PCoA dans le paquet tunnelé, avant de le transmettre.

# 5. Autres considérations

## 5.1 Échange de capacités de transfert

Le MN attend un PrRtAdv en réponse à son message RtSolPr. Si le MN ne reçoit pas de message PrRtAdv même après RTSOLPR_RETRIES, il doit supposer que le PAR ne prend pas en charge le protocole de transfert rapide et arrête d'envoyer d'autres messages RtSolPr.

Même si le routeur d'accès en cours du MN est capable de fournir la prise en charge du transfert rapide, le nouveau routeur d'accès auquel le MN se rattache peut être incapable de transfert rapide. Cela est indiqué au MN durant le "démarrage", par le message PrRtAdv avec le code 3 (voir au paragraphe 6.1.2).

## 5.2 Détermination de la nouvelle adresse d'entretien

Normalement, le MN formule sa NCoA prospective en utilisant les informations fournies dans un message PrRtAdv et envoie la FBU. Le PAR DOIT utiliser la NCoA présente dans la FBU dans son message HI. Le NAR DOIT vérifier si la NCoA présente dans le HI est déjà utilisée. Dans tous les cas, le NAR DOIT répondre au HI en utilisant un HAck, dans lequel il peut inclure une autre NCoA à utiliser, en particulier quand la configuration d'adresse allouée est utilisée. Si il y a une CoA présente dans le HAck, le PAR DOIT l'inclure dans le message FBack. Cependant, le MN lui-même n'a pas à attendre sur la liaison du PAR que cet échange ait lieu. Il peut se transférer à tout moment après l'envoi du message de FBU ; parfois, il peut être forcé de se transférer sans envoyer de FBU. Dans tous les cas, il peut quand même le confirmer en utilisant la NCoA provenant de la liaison du NAR en envoyant le message UNA.

Si un message PrRtAdv porte une NCoA, le MN DOIT l'utiliser comme sa NCoA prospective.

Quand DHCP est utilisé, le protocole prend en charge la transmission pour la seule PCoA. Dans ce cas, le MN DOIT effectuer les opérations DHCP une fois qu'il s'est rattaché au NAR même si il formule une NCoA pour transmettre la FBU. Cela est indiqué dans le message PrRtAdv avec le code 5.

## 5.3 Gestion de préfixe

Comme défini à la Section 2, la partie préfixe des "AR-Info" est le préfixe valide sur l'interface à laquelle le AP est rattaché. Le présent document ne spécifie pas comment ce préfixe est géré, sa longueur, ou ses politiques d'allocation. L'opération de protocole spécifiée dans ce document fonctionne sans considération de ces questions. Souvent, mais pas nécessairement toujours, ce préfixe peut être le préfixe agrégé (comme /48) valide sur l'interface. Dans certains déploiements, chaque MN peut avoir son propre préfixe par mobile (comme un /64) utilisé pour générer la NCoA. Certaines liaisons point à point peuvent utiliser un tel déploiement.

Quand l'allocation de préfixe par mobile est utilisée, les "AR-Info" annoncées dans le PrRtAdv incluent quand même le préfixe (agrégé) valide sur l'interface à laquelle l'AP cible est rattaché, sauf si les routeurs d'accès communiquent l'un avec l'autre (en utilisant les messages HI et HAck) pour gérer le préfixe par mobile. Le MN formule quand même une NCoA en utilisant le préfixe agrégé. Cependant, une autre NCoA fondée sur le préfixe par mobile est retournée par le NAR dans le message HAck. Cette NCoA de remplacement est fournie au MN dans le message FBack ou dans l'option NAACK.

## 5.4 Perte de paquet

Un transfert implique une commutation de liaison, qui ne peut pas être exactement coordonnée avec la signalisation du transfert rapide. De plus, le schéma d'arrivée des paquets dépend de nombreux facteurs, incluant les caractéristiques de l'application, les comportements de traitement des files d'attentes dans le réseau, etc. Donc, les paquets peuvent arriver au NAR avant que le MN soit capable d'y établir sa liaison. Ces paquets vont être perdus sauf si ils sont mis en mémoire tampon par le NAR. De même, si le MN se rattache au NAR et envoie ensuite un message de FBU, les paquets qui arrivent au PAR jusqu'à ce que la FBU soit traitée vont être perdus sauf si ils sont mis dans une mémoire tampon. Ce protocole fournit une option pour indiquer une demande de mise en mémoire tampon au NAR dans le message HI. Quand le PAR demande ce dispositif (pour le MN) il DEVRAIT aussi fournir son propre support de mise en mémoire tampon.

Alors que la mise en mémoire tampon peut permettre un transfert en douceur, la taille de la mémoire tampon et le taux auquel les paquets en mémoire tampon sont finalement transmis sont des considérations importantes quand on fournit la prise en charge de la mise en mémoire tampon. Un certain nombre d'aspects sont à considérer :

- Certaines applications transmettent moins de données sur un certaine période que d'autres, et cela implique des exigences différentes de mise en mémoire tampon. Par exemple, la voix sur IP a normalement besoin de plus petites mémoires tampon qu'un flux de vidéo à haute résolution, car cette dernière a de plus grandes tailles de paquet et de plus forts taux d'arrivée.

- Quand le nœud mobile apparaît sur la nouvelle liaison, si le routeur qui met en mémoire tampon envoie un grand nombre de paquets en succession rapide, il peut submerger les ressources du routeur, du nœud mobile lui-même, ou du chemin entre les deux.
  En particulier, transmettre une grande quantité des paquets mis en mémoire tampon à la suite peut encombrer le chemin entre le routeur de mise en mémoire tampon et le nœud mobile. De plus, les nœuds (comme une station de base) sur le chemin entre le routeur de mise en mémoire tampon et le nœud mobile peuvent éliminer de tels paquets. Si une station de base met en mémoire tampon trop de ces paquets, ils peuvent contribuer à de la gigue supplémentaire pour les paquets qui arrivent derrière eux, ce qui est indésirable pour une communication en temps réel.

- Comme les routeurs ne sont pas impliqués dans la communication de bout en bout, ils n'ont pas connaissance des conditions de transport.

- La connexité sans fil du nœud mobile peut varier dans le temps. Il peut bénéficier d'un plus petite ou plus grande bande passante sur la nouvelle liaison, la force du signal peut être faible au moment où il entre dans la zone de ce point d'accès, et ainsi de suite.

Il en résulte qu'il est difficile de désigner un algorithme qui transmettrait les paquets mis en mémoire tampon à l'espacement approprié pour tous les scénarios. L'objet des transferts rapides est d'éviter des pertes de paquet. Sortir trop rapidement les paquets mis en mémoire tampon peut, par soi-même, causer la perte de paquets, ainsi que bloquer ou perdre les paquets suivants destinés au nœud mobile.

La présente spécification n'interdit pas aux mises en œuvre de fournir une prise en charge spécialisée de la mise en mémoire tampon pour toute situation spécifique. Cependant, il faut faire attention au taux de transmission des paquets mis en mémoire tampon au MN une fois le rattachement achevé. Les routeurs qui mettent en œuvre la présente spécification DOIVENT mettre en œuvre au moins l'algorithme par défaut, qui se fonde sur les taux d'arrivée originaux des paquets mis en mémoire tampon. Un maximum de 5 paquets PEUVENT être envoyés l'un après l'autre, mais tous les paquets suivants DEVRAIENT utiliser un taux d'envoi qui est déterminé par la mesure du taux auquel les paquets sont entrés dans la mémoire tampon, éventuellement en utilisant des techniques de lissage comme l'activité récente sur une fenêtre temporelle glissante et des moyennes pondérées [RFC3290].

On devrait cependant noter que cet algorithme par défaut est brutal et peut ne pas convenir pour toutes les situations. De futures révisions de la présente spécification pourront fournir des algorithmes supplémentaires quand assez d'expérience des diverses conditions sera obtenue sur les réseaux où il est déployé.

### 5.5 Traitement de DAD

La détection d'adresse dupliquée (DAD, *Duplicate Address Detection*) a été définie dans la [RFC4862] pour éviter la duplication d'adresse sur les liaisons quand l'auto-configuration d'adresse sans état est utilisée. L'utilisation de DAD pour vérifier l'unicité d'une adresse IPv6 configurée par auto-configuration sans état ajoute des délais à un transfert. La probabilité de la duplication d'un identifiant d'interface sur le même sous réseau est très faible ; cependant, elle ne peut pas être ignorée. Donc, le protocole spécifié dans ce document DEVRAIT n'être utilisé que dans des déploiements où la probabilité de telles collisions d'adresses est extrêmement faible ou n'est pas un souci (à cause de la procédure de gestion d'adresses déployée). Le protocole exige que le NAR envoie une sonde de DAD avant qu'il commence à défendre la NCoA. Cependant, ce délai de DAD peut être contourné en réglant DupAddrDetectTransmits à zéro sur le NAR ([RFC4862]).

Le présent document spécifie les messages qui peuvent être utilisés pour fournir des adresses sans dupliquées, mais le document ne spécifie pas comment créer ou gérer de telles adresses. Dans certains cas, le NAR peut avoir déjà les connaissances requises pour assurer si l'adresse du MN est ou non un dupliqué avant que le MN passe au nouveau sous réseau. Par exemple, dans certains déploiements, le NAR peut tenir un réservoir d'adresses sans duplication dans une liste pour les besoins des transferts. Dans ce cas, le NAR peut fournir cette disposition dans le message HAck (voir au paragraphe 6.2.1.2) ou dans l'option NAACK (voir au paragraphe 6.4.6).

### 5.6 Mouvement rapide ou erroné

Bien que la présente spécification soit pour le transfert rapide, le protocole est limité quant à la rapidité avec laquelle un MN peut se déplacer. Un cas particulier de mouvement rapide est le ping-pong, où un MN bouge rapidement entre les deux mêmes points d'accès. Une autre instance du même problème est le mouvement erroné, c'est-à-dire, le MN reçoit les informations avant un transfert qu'il passe à un nouveau point d'accès, mais il passe à un point d'accès différent ou il interrompt le mouvement. Tous les comportements ci-dessus sont généralement le résultat d'idiosyncrasies de couche de liaison et sont donc souvent résolus à la couche de liaison elle-même.

La mobilité de couche IP introduit cependant ses propres limites. Les transferts de couche IP devraient se produire à un taux convenable pour que le MN mette à jour le lien de, au moins, son agent de rattachement et de préférence celui de chaque nœud correspondant (CN) avec lequel il est en communication. Un MN qui se déplace plus vite que nécessaire pour que cette signalisation s'achève (qui peut être de l'ordre de quelques secondes) peut commencer à perdre des paquets. Le coût de signalisation sur l'interface radio et dans le réseau peut augmenter de façon significative, en particulier dans le cas d'un mouvement rapide entre plusieurs routeurs d'accès. Pour éviter les frais généraux de signalisation, les mesures suivantes sont suggérées.

Un MN retournant au PAR avant la mise à jour des liens nécessaires quand il est présent sur le NAR DOIT envoyer une mise à jour rapide de lien avec l'adresse de rattachement égale à la PCoA du MN et une durée de vie de zéro au PAR. Le MN devrait avoir une association de sécurité avec le PAR car il a effectué un transfert rapide au NAR. Le PAR, à réception de cette mise à jour rapide de lien, va vérifier son ensemble de tunnels sortants (transfert rapide temporaire). Si il trouve une correspondance, il DEVRAIT terminer ce tunnel; c'est-à-dire, commencer plutôt à livrer les paquets directement au nœud. Afin que le PAR traite cette FBU, la durée de vie de l'association de sécurité doit être au moins celle du tunnel lui-même.

Les tunnels temporaires pour les besoins des transferts rapides devraient utiliser de courtes durées de vie (de l'ordre du dixième de seconde). La durée de vie de ces tunnels devrait être suffisante pour permettre au MN de mettre à jour tous ses liens actifs. La durée de vie par défaut du tunnel devrait être la même que la valeur de durée de vie dans le message FBU.

L'effet d'un mouvement erroné est normalement limité à la perte de paquets car l'acheminement peut changer et le PAR peut transmettre des paquets vers un autre routeur avant que le MN se connecte réellement à ce routeur. Si le MN se découvre sur un routeur d'accès imprévu, il DEVRAIT envoyer une nouvelle mise à jour rapide de lien au PAR. Cette FBU se substitue au lien existant avec le PAR, et les paquets vont être redirigés sur la nouvelle localisation confirmée du MN.

## 6. Formats de message

Tous les messages ICMPv6 ont un type commun spécifié dans la [RFC4443]. Les messages sont distingués sur la base du champ Sous type (voir ci-dessous). Pour tous les messages ICMPv6, la somme de contrôle est définie dans la [RFC4443].

### 6.1 Nouveaux messages de découverte de voisin

#### 6.1.1 Sollicitation de routeur pour annonce de mandataire (RtSolPr)

Les nœuds mobiles envoient des messages de sollicitation de routeur pour annonce de mandataire afin d'inviter les routeurs à faire des annonces de routeur mandataire. Toutes les options d'adresse de couche de liaison ont le format défini au paragraphe 6.4.3.

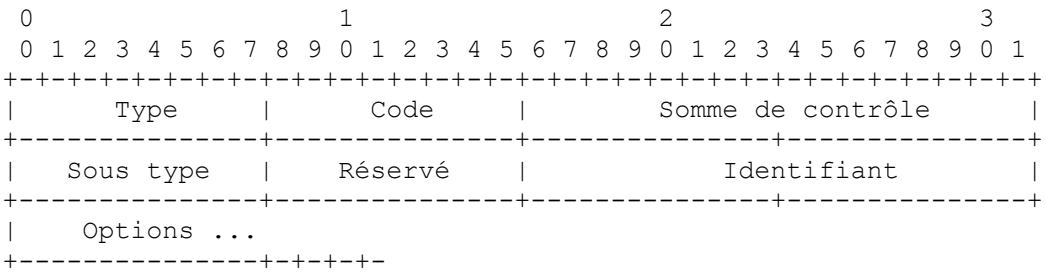


**Figure 4 : Message Sollicitation de routeur pour annonce de mandataire (RtSolPr)**

Champs IP :
Adresse de source : adresse IP allouée à l'interface envoyeuse.
Adresse de destination : adresse du routeur d'accès ou adresse de diffusion groupée Tous les routeurs.
Limite de bonds : 255, voir la RFC 2461.

Champs ICMP :
Type : 154
Code : 0
Somme de contrôle : somme de contrôle ICMPv6.
Sous type : 2
Réservé : DOIT être réglé à zéro par l'envoyeur et ignoré par le receveur.
Identifiant : DOIT être réglé par l'envoyeur de façon à ce que les réponses puissent être confrontées à cette sollicitation.

Options valides :
Adresse de source de couche de liaison : quand elle est connue, l'adresse de couche de liaison de l'envoyeur DEVRAIT être incluse en utilisant l'option Adresse de couche de liaison (LLA). Voir le format de l'option LLA ci-dessous.

Adresse de couche de liaison du nouveau point d'accès : adresse de couche de liaison ou identification du point d'accès pour lequel le MN demande les informations d'annonce d'acheminement. Elle DOIT être incluse dans tous les messages RtSolPr. Plus d'une telle adresse ou identifiant peut être présente. Ce champ peut aussi être une adresse générique. Voir l'option LLA ci-dessous.

De futures versions de ce protocole pourront définir de nouveaux types d'option. Les receveurs DOIVENT ignorer en silence toute option qu'il ne reconnaissent pas et continuer le traitement du reste du message.

Inclure l'option LLA de source permet au receveur d'enregistrer l'adresse de couche 2 de l'envoyeur afin que la découverte de voisin puisse être évitée quand le receveur a besoin de renvoyer des paquets à l'envoyeur (du message RtSolPr).

Quand un caractère générique est utilisé pour la LLA du nouveau point d'accès, aucune autre option LLA de nouveau point d'accès ne doit être présente.

Un message Annonce de routeur mandataire (PrRtAdv) devrait être reçu par le MN en réponse à un RtSolPr. Si un tel message n'est pas reçu à temps (pas moins de deux fois le temps normal d'aller retour (RTT, *Round Trip Time*) sur la liaison d'accès, ou 100 millisecondes si le RTT n'est pas connu) il DEVRAIT renvoyer le message RtSolPr. Les retransmissions suivantes peuvent être jusqu'à RTSOLPR_RETRIES, mais DOIVENT utiliser un retard à croissance exponentielle dans lequel la période de temporisation (c'est-à-dire, 2xRTT ou 100 millisecondes) est doublée avant chaque instance de retransmission. Si une annonce de routeur mandataire n'est pas reçue au moment où le MN se déconnecte du PAR, le MN DEVRAIT envoyer une FBU immédiatement après la configuration d'une nouvelle CoA.

Quand les messages RtSolPr sont envoyés plus d'une fois, ils DOIVENT être limités en débit à MAX_RTSOLPR_RATE par seconde. Durant chaque utilisation d'un RtSolPr, le retard exponentiel est utilisé pour les retransmissions.

### 6.1.2 Annonce de routeur mandataire (PrRtAdv)

Les routeurs d'accès envoient des messages d'annonce de routeur mandataire gratuitement si le transfert est initié par le réseau ou en réponse à un message RtSolPr provenant du MN, fournissant l'adresse de couche de liaison, l'adresse IP, et les préfixes de sous réseau des routeurs du voisinage. Toutes les options d'adresse de couche de liaison ont le format défini au paragraphe 6.4.3.

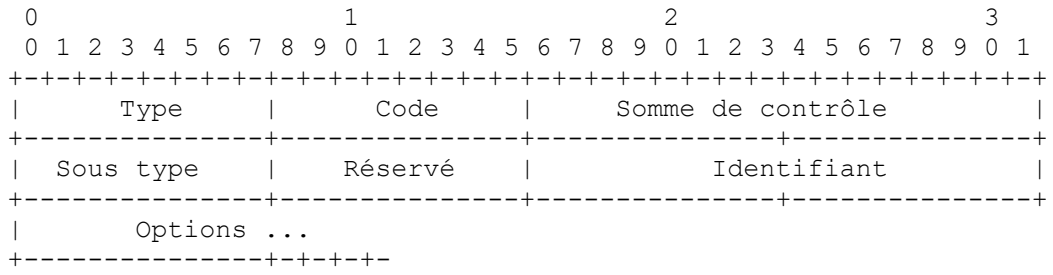


**Figure 5 : Message Annonce de routeur mandataire (PrRtAdv)**

Champs IP :
Adresse de source : DOIT être l'adresse de liaison locale allouée à l'interface d'où ce message est envoyé.
Adresse de destination : adresse de source d'une sollicitation de routeur d'annonce de mandataire invocatrice ou adresse du nœud que le routeur d'accès ordonne de transférer.
Limite de bonds : 255. Voir la RFC 2461.

Champs ICMP :
Type : 154
Code : 0, 1, 2, 3, 4, ou 5. Voir ci-dessous.
Somme de contrôle : somme de contrôle ICMPv6.
Sous type : 3
Réservé : DOIT être réglé à zéro par l'envoyeur et ignoré par le receveur.
Identifiant : copié de la sollicitation de routeur d'annonce de mandataire ou réglé à zéro si non sollicité.

Options valides dans l'ordre suivant :

Adresse de source de couche de liaison : quand elle est connue, l'adresse de couche de liaison de l'envoyeur DEVRAIT être incluse en utilisant l'option Adresse de couche de liaison. Voir le format de l'option LLA ci-dessous.

Adresse de couche de liaison du nouveau point d'accès : l'adresse de couche de liaison ou l'identification du point d'accès est copiée du message RtSolPr. Cette option DOIT être présente.

Adresse de couche de liaison du nouveau routeur : adresse de couche de liaison du routeur d'accès pour lequel ce message est mandaté. Cette option DOIT être incluse quand le code est 0 ou 1.

Adresse IP du nouveau routeur : adresse IP du NAR. Cette option DOIT être incluse quand le code est 0 ou 1.

Option Informations de préfixe du nouveau routeur : spécifie le préfixe du routeur d'accès auquel le message est mandaté et est utilisé pour l'auto-configuration d'adresse. Cette option DOIT être incluse quand le code est 0 ou 1. Cependant, quand ce préfixe est le même que celui utilisé dans l'option Adresse IP du nouveau routeur (ci-dessus) l'option Informations de préfixe n'a pas besoin d'être présente.

Option Nouvelle CoA : PEUT être présente quand PrRtAdv est envoyée sans sollicitation. Le PAR PEUT calculer une nouvelle CoA en utilisant les informations de préfixe du NAR et l'adresse de couche 2 du MN ou par tout autre moyen.

De futures versions de ce protocole pourront définir de nouveaux types d'option. Les receveurs DOIVENT ignorer en silence toute option qu'ils ne reconnaissent pas et continuer le traitement du message.

Actuellement, les valeurs de code 0, 1, 2, 3, 4, et 5 sont définies.

Une annonce de routeur mandataire avec le code 0 signifie que le MN devrait utiliser le couple [AP-ID, AR-Info] (présent dans les options ci-dessus) pour la détection de mouvement et la formulation de la NCoA. Dans ce cas, le champ Code d'option dans l'option LLA de nouveau point d'accès est 1 pour refléter la LLA du point d'accès pour lequel se rapporte le reste des options. Plusieurs couples peuvent être présents.

Une annonce de routeur mandataire avec le code 1 signifie que le message a été envoyé sans sollicitation. Si une option Nouvelle CoA est présente à la suite de l'option Informations de préfixe du nouveau routeur, le MN DOIT utiliser la NCoA fournie et envoyer immédiatement une FBU ou autrement rester au service perdu. Ce message agit comme un déclencheur de transfert initié par le réseau ; voir au paragraphe 3.3. Dans ce cas, le champ Code d'option dans l'option LLA du nouveau point d'accès (voir ci-dessous) est 1 pour refléter la LLA du point d'accès pour lequel se rapporte le reste des options.

Une annonce de routeur mandataire avec le code 2 signifie qu'aucune nouvelle information de routeur n'est présente. Chaque option LLA de nouveau point d'accès contient une valeur de code d'option (décrite ci-dessous) qui indique un résultat spécifique.

Quand le champ Code d'option dans l'option LLA du nouveau point d'accès est 5, le transfert à ce point d'accès n'exige pas de changement de la CoA. Cela serait le cas, par exemple, quand un certain nombre de points d'accès sont connectés à la même interface de routeur, ou quand des mécanismes de gestion de la mobilité fondée sur le réseau assurent que le nœud mobile spécifique respecte toujours le même préfixe sans considérer si il y a un routeur différent rattaché au point d'accès cible.

Aucune autre option n'est exigée dans ce cas.

Quand le champ Code d'option dans l'option LLA de nouveau point d'accès est 6, le PAR ne connaît pas les informations de préfixe demandées. Le MN DEVRAIT tenter d'envoyer une FBU aussitôt qu'il retrouve la connexité avec le NAR. Aucune autre option n'est exigée dans ce cas.

Quand le champ Code d'option dans l'option LLA de nouveau point d'accès est 7, cela signifie que le NAR ne prend pas en charge le transfert rapide. Le MN DOIT arrêter les opérations du protocole de transfert rapide. Aucune autre option n'est exigée dans ce cas.

Une annonce de routeur mandataire avec le code 3 signifie que de nouvelles informations de routeur sont présentes seulement pour un sous ensemble des points d'accès demandés. Les valeurs du champ Code d'option (celles définies ci-dessus, ainsi que la valeur 1) distinguent les différents résultats pour les points d'accès individuels.

Une annonce de routeur mandataire avec le code 4 signifie que les informations de sous réseau concernant les points d'accès du voisinage sont envoyées non sollicitées, mais le message n'est pas un déclencheur de transfert, à la différence de quand le message est envoyé avec le code 1. Plusieurs couples peuvent être présents.

Une annonce de routeur mandataire avec le code 5 signifie que le MN peut utiliser les informations de nouveau routeur présentes pour détecter le mouvement à un nouveau sous réseau, mais le MN doit effectuer DHCP [RFC3315] lors du rattachement à la liaison du NAR. Le PAR et le NAR vont transmettre des paquets à la PCoA du MN. Le MN doit quand même formuler une NCoA pour transmettre la FBU (en utilisant les informations envoyées dans ce message) mais cette NCoA ne va pas être utilisée pour transmettre des paquets.

Quand un identifiant d'AP avec un caractère générique est utilisé dans le message RtSolPr, le message PrRtAdv devrait inclure tous les 'n' triplets [identifiant de point d'accès, option Adresse de couche de liaison, option Informations de préfixe] correspondant au voisinage du PAR.

### 6.2 Nouveaux messages d'en-tête de mobilité

IPv6 mobile utilise un nouveau type d'en-tête IPv6 appelé en-tête de mobilité [RFC3775]. Les messages Initier le transfert, Accusé de réception de transfert, Mise à jour rapide de lien, Accusé de réception de lien rapide, et Annonce de voisin rapide (déconseillé) utilisent l'en-tête de mobilité.

#### 6.2.1 Messages inter routeurs d'accès

##### 6.2.1.1 Initier le transfert (HI)

Le message Initier le transfert (HI) est un message d'en-tête de mobilité envoyé par un routeur d'accès (normalement un PAR) à un autre routeur d'accès (normalement un NAR) pour initier le processus de transfert d'un MN.

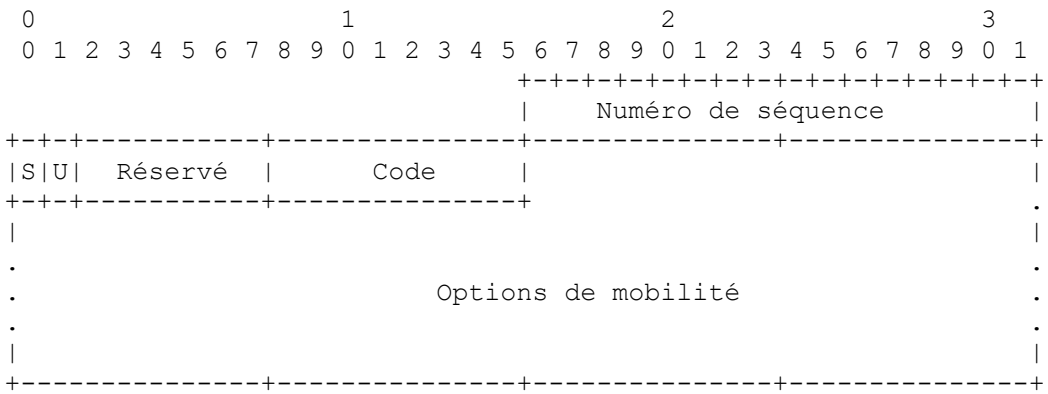


**Figure 6 : Message Initier le transfert (HI)**

Champs IP :
Adresse de source : adresse IP du PAR.

Adresse de destination : adresse IP du NAR.
Numéro de séquence : DOIT être réglé par l'envoyeur de façon que les réponses puissent être confrontées à ce message.
Fanion 'S' : fanion de configuration d'adresse allouée. Quand il est réglé à un, ce message demande qu'une nouvelle CoA soit retournée par la destination. PEUT être établi quand le code = 0. DOIT être 0 quand le code = 1.

Fanion 'U' : fanion de mémoire tampon. Quand il est établi, la destination DEVRAIT mettre en mémoire tampon tous les paquets vers le nœud indiqué dans les options de ce message. Utilisé quand Code = 0, DEVRAIT être réglé à 0 quand le code = 1.

Code : 0 ou 1. Voir ci-dessous.

Réservé : DOIT être réglé à zéro par l'envoyeur et ignoré par le receveur.

Options valides :
Adresse de couche de liaison du MN : adresse de couche de liaison du MN qui subit un transfert à la destination (c'est-à-dire, le NAR). Cette option DOIT être incluse afin que la destination puisse reconnaître le MN.

Précédente adresse d'entretien : adresse IP utilisée par le MN lorsque il est rattaché au routeur d'origine. Cette option DEVRAIT être incluse afin qu'un chemin pour l'hôte puisse être établi si nécessaire.

Nouvelle adresse d'entretien : adresse IP que le MN souhaite utiliser quand il sera connecté à la destination. Quand le bit 'S' est établi, le NAR PEUT allouer cette adresse.

Le PAR utilise une valeur de code de 0 quand il traite une FBU avec la PCoA comme adresse IP de source. Le PAR utilise une valeur de code de 1 quand il traite une FBU dont l'adresse IP de source n'est pas la PCoA.

Si un message Accusé de réception de transfert (HAck) n'est pas reçu en réponse dans un bref délai (pas moins de deux fois le délai d'aller-retour (RTT) normal entre la source et la destination, ou 100 millisecondes si le RTT n'est pas connu) le message Initier le transfert DEVRAIT être envoyé à nouveau. Les retransmissions suivantes peuvent être jusqu'à HI_RETRIES, mais DOIVENT utiliser le retard exponentiel dans lequel la période de temporisation (c'est-à-dire, 2xRTT ou 100 millisecondes) est doublée à chaque instance de retransmission.

#### 6.2.1.2 Accusé de réception de transfert (HAck)

Le message Accusé de réception de transfert (Hack) est un nouveau message d'en-tête de mobilité qui DOIT être envoyé (normalement par le NAR au PAR) en réponse au message Initier le transfert.

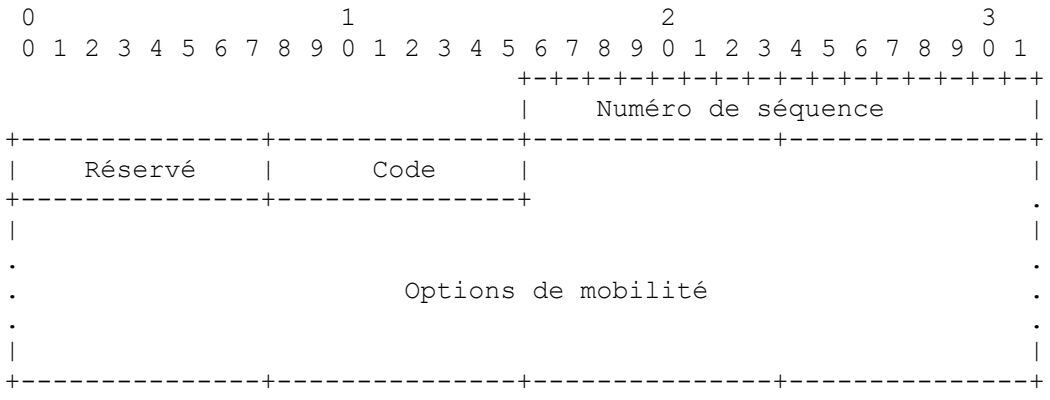


**Figure 7 : Message Accusé de réception de transfert (Hack)**

Champs IP :
Adresse de source : copié de l'adresse de destination du message Initier le transfert auquel ce message répond.
Adresse de destination : copié de l'adresse de source du message Initier le transfert auquel ce message répond.
Numéro de séquence : copié du champ correspondant dans le message HI auquel ce message répond, pour permettre au receveur de confronter de message HAck avec un message HI en instance.

Code : 0 : transfert accepté, NCoA valide.

1 : transfert accepté, NCoA non valide ou utilisée.
2 : transfert accepté, NCoA allouée (utilisé dans l'adressage alloué)
3 : transfert accepté, utiliser la PcoA.
4 : Message envoyé non sollicité, généralement pour déclencher un message HI.
128 : transfert non accepté, raison non spécifiée.
129 : administrativement interdit.
130 : ressources insuffisantes.

Réservé : DOIT être réglé à zéro par l'envoyeur et ignoré par le receveur.

Options valides :
Nouvelle adresse d'entretien : si le fanion 'S' dans le message Initier le transfert est établi, cette option DOIT être utilisée pour fournir la NCoA que le MN devrait utiliser pour se connecter à ce routeur. Cette option PEUT être incluse, même quand le bit 'S' n'est pas établi, par exemple, le code 2 ci-dessus.

À réception d'un message HI, le NAR DOIT répondre avec un message Accusé de réception de transfert. Si le fanion 'S' est établi dans le message HI, le NAR DEVRAIT inclure l'option Nouvelle adresse d'entretien et un code 3.

Le NAR PEUT fournir la prise en charge de la PCoA (au lieu d'accepter ou allouer une NCoA) établir une entrée de chemin d'hôte pour la PCoA, et établir un tunnel au PAR pour transmettre les paquets du MN envoyés avec la PCoA comme adresse IP de source. Cette entrée de chemin d'hôte DEVRAIT être utilisée pour transmettre les paquets une fois que le NAR a détecté que ce MN particulier est rattaché à sa liaison. Le NAR indique la prise en charge de la transmission pour la PCoA en utilisant la valeur de code 3 dans le message HAck. Ensuite, le PAR établit un tunnel au NAR afin de transmettre les paquets qui arrivent pour la PCoA.

Quand on répond à un message HI contenant une valeur de code 1, les valeurs de code 1, 2, et 4 dans le message HAck ne sont pas pertinentes.

Finalement, le nouveau routeur d'accès peut toujours refuser le transfert, et dans ce cas il DOIT indiquer la raison dans une des valeurs de code disponibles.

### 6.2.2 Mise à jour de lien rapide (FBU)

Le message Mise à jour rapide de lien a une valeur de type d'en-tête de mobilité de 8. La FBU est identique au message Mise à jour de lien IPv6 mobile (BU, *Binding Update*). Cependant, les règles de traitement sont légèrement différentes. De plus, les fanions supplémentaires (au titre du champ Réservé ci-dessous) définis par d'autres protocoles en relation ne sont pas pertinents dans ce message, et DOIVENT être mis à zéro.

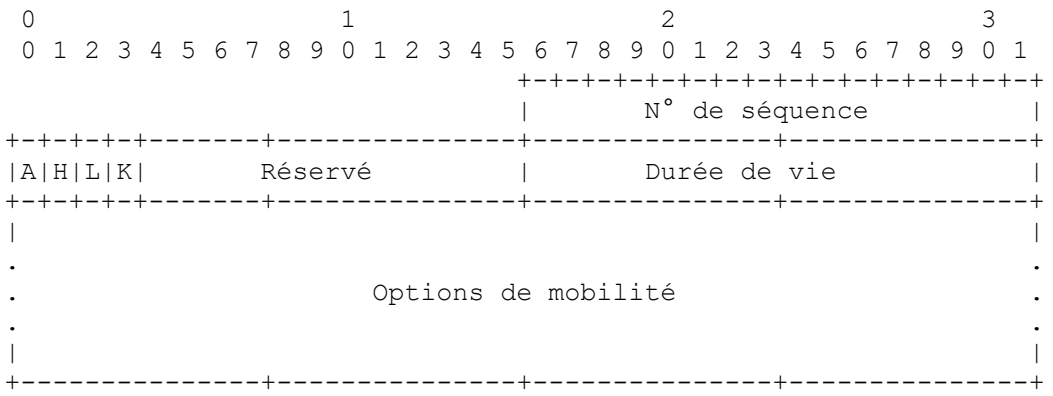


**Figure 8 : Message Mise à jour rapide de lien (FBU)**

Champs IP :
Adresse de source : la PCoA ou NCoA.
Adresse de destination : adresse IP du routeur d'accès précédent.
Fanion 'A' : DOIT être établi à un pour demander que le PAR envoie un message Accusé de réception de lien rapide.
Fanion 'H' : DOIT être établi à un. Voir la [RFC3775].
Fanion 'L' : voir la [RFC3775].

Fanion 'K' : voir la [RFC3775].
Réservé : ce champ n'est pas utilisé. DOIT être mis à zéro.
Numéro de séquence : voir la [RFC3775].
Durée de vie : durée demandée en secondes pendant laquelle l'envoyeur souhaite avoir un lien.

Options de mobilité : DOIT contenir une option CoA de remplacement réglée à la NCoA quand une FBU est envoyée de la liaison du PAR. DOIT contenir l'option Données d'autorisation de lien pour la FMIP (BADF, *Binding Authorization Data for the FMIP*) (voir au paragraphe 6.4.5). PEUT contenir l'option LLA d'en-tête de mobilité (voir au paragraphe 6.4.4).

Le MN envoie un message FBU après avoir reçu un message PrRtAdv. Si le MN bouge avant de recevoir un message PrRtAdv, il DEVRAIT envoyer une FBU au PAR après avoir configuré la NCoA sur le NAR en accord avec les protocoles de découverte de voisin et de configuration d'adresse IPv6. Quand le MN bouge sans avoir reçu de message PrRtAdv, il ne peut pas transmettre un message UNA lorsque il se rattache à la liaison du NAR.

L'adresse IP de source est la PCoA quand la FBU est envoyée à partir de la liaison du PAR, et l'adresse IP de source est la NCoA quand la FBU est envoyée de la liaison du NAR. Quand l'adresse IP de source est la PCoA, le MN DOIT inclure l'option CoA de remplacement réglée à la NCoA. Le PAR DOIT traiter la FBU même si l'adresse dans l'option CoA de remplacement est différente de celle de l'adresse IP de source, et s'assurer que l'adresse dans l'option CoA de remplacement est utilisée dans l'option Nouvelle CoA dans le message HI au NAR.

La FBU DOIT aussi inclure l'option Adresse de rattachement réglée à la PCoA. Un message de FBU DOIT être protégé afin que le PAR soit capable de déterminer que le message de FBU est envoyé par un MN qui possède légitimement la PCoA.

### 6.2.3 Accusé de réception de lien rapide (FBack)

Le format du message FBack est identique au message Accusé de réception de lien IPv6 mobile (BAck, *Binding Acknowledgment*). Cependant, les règles de traitement sont légèrement différentes. De plus, les fanions supplémentaires (au titre du champ Réservé ci-dessous) définis par d'autres protocoles en relation ne sont pas pertinents dans ce message, et DOIVENT être réglés à zéro.

Le message Accusé de réception de lien rapide a une valeur de type d'en-tête de mobilité de 9. Le message FBack est envoyé par le PAR pour accuser réception d'un message de mise à jour rapide de lien dans lequel le bit 'A' est établi. Si le PAR envoie un message HI au NAR après le traitement d'une FBU, le message FBack NE DEVRAIT PAS être envoyé au MN avant que le PAR reçoive un message HAck du NAR. Le PAR PEUT cependant envoyer le FBack immédiatement dans le mode réactif. L'accusé de réception de lien rapide PEUT aussi être envoyé au MN sur la vieille liaison.

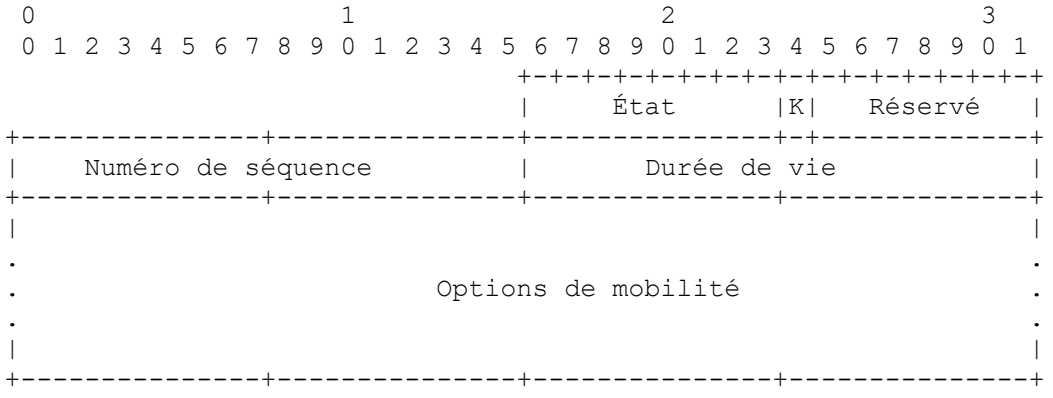


**Figure 9 : Message Accusé de réception de lien rapide (FBack)**

Champs IP :
Adresse de source : adresse IP du routeur d'accès précédent.
Adresse de destination : la NCoA, et facultativement, la PCoA.
État : entier non signé de 8 bits indiquant la disposition de la mise à jour rapide 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 d'état suivantes sont actuellement définies :
0 : mise à jour rapide de lien acceptée.

1 : mise à jour rapide de lien acceptée mais la NCoA est invalide. Utiliser la NCoA fournie dans la CoA de "remplacement"

Les valeurs du champ État 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 :
128 : raison non spécifiée
129 : administrativement interdit
130 : ressources insuffisantes
131 : longueur incorrecte d'identifiant d'interface

Fanion 'K' : voir la [RFC3775].

Réservé : champ non utilisé. DOIT être mis à zéro.

Numéro de séquence : copié du message de FBU pour que le MN l'utilise à faire correspondre cet accusé de réception avec une FBU en instance.

Durée de vie : durée de vie accordée en secondes pendant laquelle l'envoyeur de ce message va conserver un lien pour la redirection du trafic.

Options de mobilité : DOIT contenir une CoA de "remplacement" si État est 1. DOIT contenir l'option Données d'autorisation de lien pour FMIP (BADF). Voir le paragraphe 6.4.5.

### 6.3 Annonce de voisin non sollicitée (UNA)

C'est le même message que dans la [RFC4861] avec l'exigence que le bit 'O' soit toujours réglé à zéro. Comme c'est un message non sollicité, le bit 'S' est à zéro, et comme c'est envoyé par un MN, le bit 'R' est aussi zéro.

Si le NAR est mandataire pour la NCoA (par suite de l'échange HI et Hack) le traitement de l'UNA a des étapes supplémentaires (voir ci-dessous). Si le NAR n'est pas mandataire pour la NCoA (par exemple, l'échange HI et HAck n'a pas eu lieu) alors le traitement de l'UNA suit la procédure spécifiée dans la [RFC4861]. Les mises en œuvre PEUVENT retransmettre les UNA sous réserve de la spécification du paragraphe 7.2.6 de la [RFC4861] tout en notant que la valeur par défaut du temporisateur de retransmission est large pour les besoins du transfert.

L'adresse de source dans l'UNA DOIT être la NCoA. L'adresse de destination est normalement l'adresse de diffusion groupée Tous les nœuds ; cependant, certains déploiements peuvent ne pas préférer la transmission à une adresse de diffusion groupée. Dans ce cas, l'adresse de destination DEVRAIT être l'adresse IP du NAR.

L'adresse cible DOIT inclure la NCoA, et l'adresse de couche de liaison cible DOIT inclure la LLA du MN.

Le MN envoie un message UNA au NAR, aussitôt qu'il retrouve la connexité sur la nouvelle liaison. Les paquets arrivants ou mis en mémoire tampon peuvent être immédiatement transmis. Si le NAR est mandataire pour la NCoA, il crée une entrée d'antémémoire de voisins dans l'état STALE mais transmet les paquets quand il détermine une accessibilité bidirectionnelle en accord avec la procédure standard de découverte de voisin. Si il y a une entrée dans l'état INCOMPLET sans adresse de couche de liaison, le NAR la règle à STALE, en accord avec la procédure de la [RFC4861].

Le NAR PEUT souhaiter fournir au MN une adresse IP différente de celle du message UNA. Dans ce cas, le NAR DOIT supprimer l'entrée de mandataire pour la NCoA et envoyer une annonce de routeur avec une option NAACK contenant la nouvelle adresse IP.

La combinaison de la NCoA (présente dans l'adresse IP de source) et de l'adresse de couche de liaison (présente comme LLA cible) DEVRAIT être utilisée pour distinguer le MN des autres nœuds.

### 6.4 Nouvelles options

Toutes les options, à l'exception de l'autorisation de lien de données pour FMIPv6 (BADF) discutée au paragraphe 6.4.5, utilisent le format Type, Longueur, et Code d'option montré à la Figure 10.

Les valeurs de type sont définies à partir de l'espace d'options de découverte de voisin et de l'espace d'options d'en-tête de

mobilité. Le champ Longueur est en unités de 8 octets pour les options de découverte de voisin, et en unités d'octets pour les options d'en-tête de mobilité. Les codes d'option fournissent des informations supplémentaires pour chacune des options (voir les options individuelles ci-dessous).

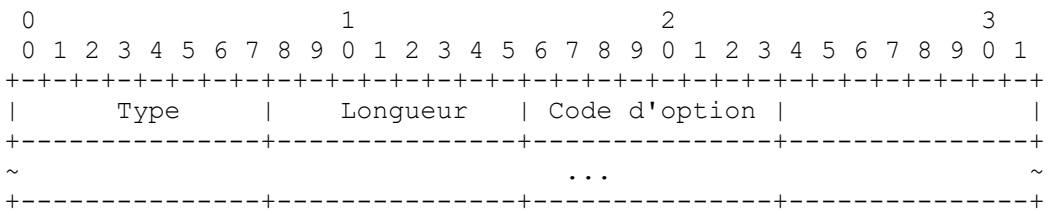


**Figure 10 : Format d'option**

### 6.4.1 Option Adresse/préfixe IP

Cette option est envoyée dans le message Annonce de routeur mandataire.

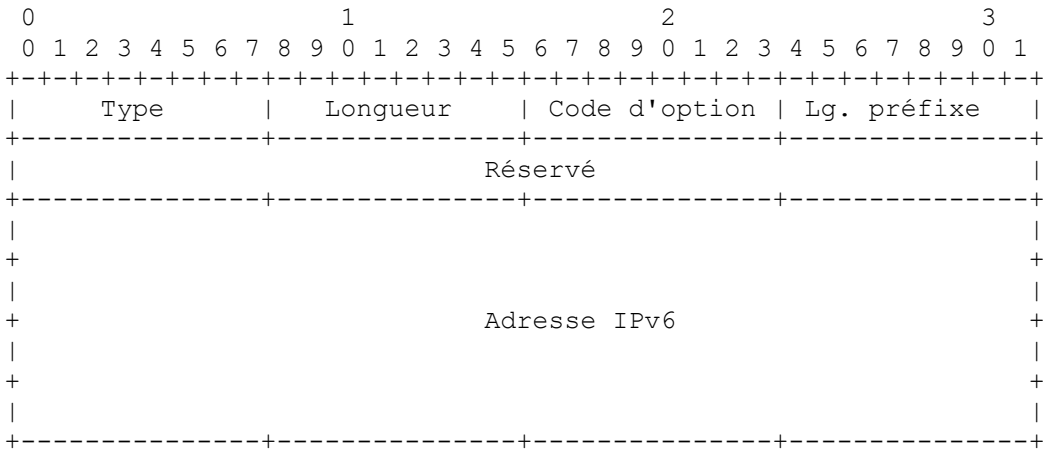


**Figure 11 : Option Adresse/préfixe IPv6**

Type : 17

Longueur : taille de cette option en unités de 8 octets incluant les champs de Type, Code d'option, et Longueur.

Code d'option :
1 : vieille adresse d'entretien
2 : nouvelle adresse d'entretien
3 : adresse IP du NAR
4 : préfixe du NAR, envoyé dans le PrRtAdv. Le champ Longueur de préfixe contient le nombre de bits en tête valides dans le préfixe. Les bits du préfixe après la longueur de préfixe sont réservés et DOIVENT être initialisés à zéro par l'envoyeur et ignorés par le receveurr.

Longueur de préfixe : entier non signé de 8 bits qui indique la longueur du préfixe de l'adresse IPv6. La gamme des valeurs va de 0 à 128.

Réservé : DOIT être réglé à zéro par l'envoyeur et DOIT être ignoré par le receveur.

Adresse IPv6 : adresse IP définie par le champ Code d'option.

### 6.4.2 Option Adresse/préfixe IP d'en-tête de mobilité

Cette option est envoyée dans les messages Initier le transfert et Accusé de réception de transfert. Cette option a une exigence d'alignement de 8n+4.

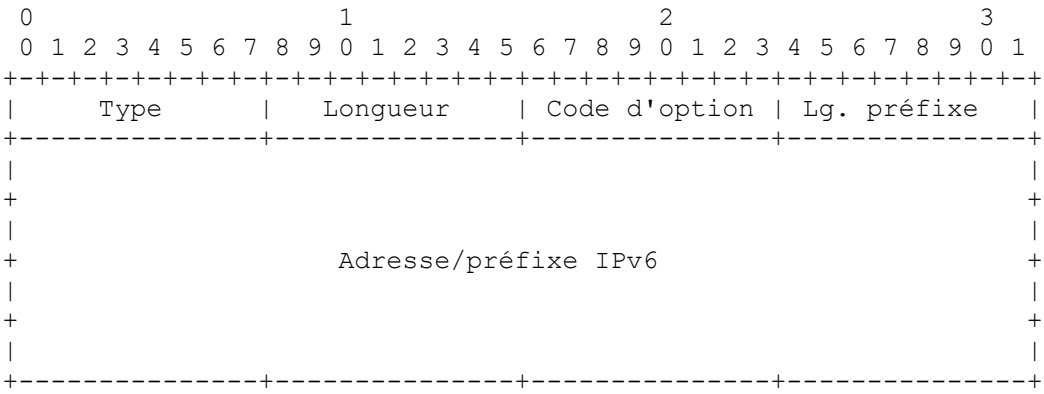


**Figure 12 : Option Adresse/préfixe d'en-tête de mobilité IPv6**

Type : 17

Longueur : taille de cette option en unités de 8 octets excluant les champs Type et Longueur.

Code d'option :
1 : vieille adresse d'entretien
2 : nouvelle adresse d'entretien
3 : adresse IP du NAR
4 : préfixe du NAR, envoyé dans le PrRtAdv. Le champ Longueur de préfixe contient le nombre de bits valides en tête dans le préfixe. Les bits dans le préfixe après la longueur de préfixe sont réservés et DOIVENT être initialisés à zéro par l'envoyeur et ignorés par le receveur.

Longueur de préfixe : entier non signé de 8 bits indiquant la longueur du préfixe d'adresse IPv6. Les valeurs vont de 0 à 128.

Adresse/préfixe IPv6 : adresse/préfixe IP défini par le champ Code d'option.

### 6.4.3 Option Adresse de couche de liaison (LLA)

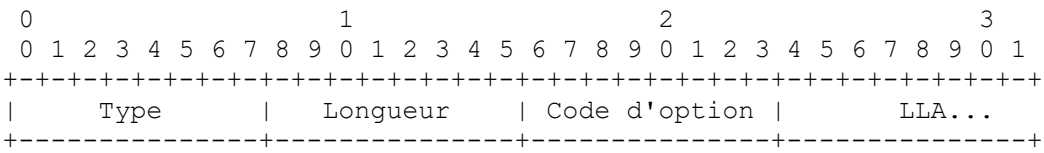


**Figure 13 : Option Adresse de couche de liaison**

Type : 19

Longueur : taille de cette option en unités de 8 octets incluant les champs Type, Code d'option, et Longueur.

Code d'option :
0 : caractère générique qui demande la résolution pour tous les points d'accès du voisinage
1 : adresse de couche de liaison du nouveau point d'accès
2 : adresse de couche de liaison du MN
3 : adresse de couche de liaison du NAR (c'est-à-dire, générateur mandataire)
4 : adresse de couche de liaison de la source du message RtSolPr ou PrRtAdv
5 : le point d'accès identifié par la LLA appartient à l'interface courante du routeur
6 : pas d'information de préfixe disponible pour le point d'accès identifié par la LLA
7 : pas de prise en charge du transfert rapide disponible pour le point d'accès identifié par la LLA

LLA : adresse de couche de liaison de longueur variable.

L'option LLA n'a pas de champ de longueur pour la LLA elle-même. Les mises en œuvre doivent consulter la couche de

liaison spécifique sur laquelle fonctionne le protocole afin de déterminer le contenu et la longueur de la LLA. Selon la taille de l'option LLA individuelle, le bourrage approprié DOIT être utilisé pour s'assurer que la taille de l'option entière est un multiple de 8 octets.

L'adresse de couche de liaison du nouveau point d'accès contient l'adresse de couche de liaison du point d'accès pour lequel le transfert va être tenté. Cela est utilisé dans le message Sollicitation de routeur pour annonce de mandataire.

L'option Adresse de couche de liaison du MN contient l'adresse de couche de liaison d'un MN. Elle est utilisée dans le message Initiier le transfert.

L'option Adresse de couche de liaison du NAR (c'est-à-dire, le générateur mandataire) contient l'adresse de couche de liaison du routeur d'accès auquel le message Sollicitation de routeur mandataire se réfère.

### 6.4.4 Option Adresse de couche de liaison d'en-tête de mobilité (MH-LLA)

Cette option est identique à l'option LLA, mais est portée dans les messages d'en-tête de mobilité, par exemple, la FBU. À l'avenir, d'autres messages d'en-tête de mobilité pourront aussi utiliser cette option. Le format de l'option est montré à la Figure 14. Il n'y a pas d'exigence d'alignement pour cette option.

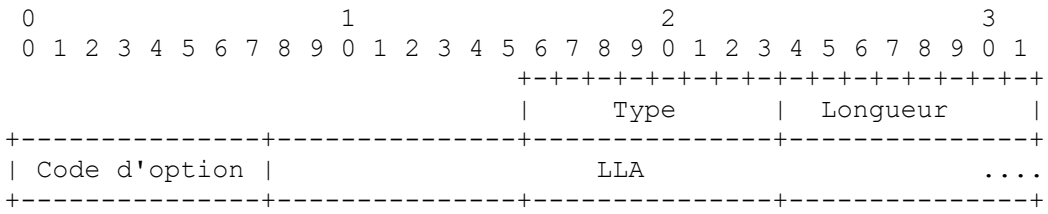


**Figure 14 : Option Adresse de couche de liaison d'en-tête de mobilité**

Type : 7

Longueur : taille de cette option en octets non inclus les champs Type et Longueur.

Code d'option : 2 : adresse de couche de liaison du MN.

LLA : adresse de couche de liaison de longueur variable.

### 6.4.5 Données d'autorisation de lien pour FMIPv6 (BADF)

Cette option DOIT être présente dans les messages FBU et FBack. L'association de sécurité entre le MN et le PAR est établie par un autre protocole [RFC5269]. Cette option spécifie comment calculer et vérifier un code d'authentification de message (MAC) en utilisant l'association de sécurité établie. Le format de cette option est montré à la Figure 15.

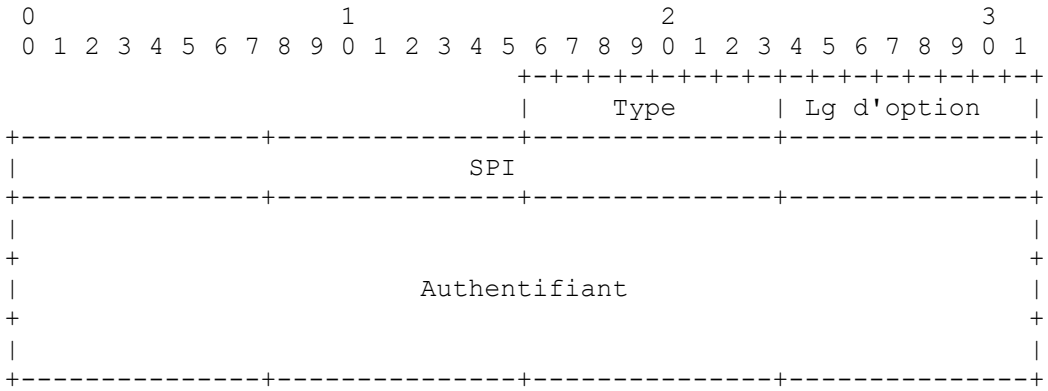


**Figure 15 : Option Données d'autorisation de lien pour FMIPv6 (BADF)**

Type : 21

Longueur d'option : longueur de l'authentifiant en octets

SPI *(Security Parameter Index)* indice de paramètre de sécurité. SPI = 0 est réservé pour l'authentifiant calculé en utilisant des clés de transfert fondées sur SEND.

Authentifiant : le même que dans la RFC 3775, avec "correspondant" remplacé par l'adresse IP du PAR, et la clé de gestion de lien (KBM, *Binding Management Key*) remplacé par la clé partagée entre le MN et le PAR.

Le calcul de MAC par défaut est fait en utilisant HMAC_SHA1 avec les 96 premiers bits utilisés pour le MAC. Comme il y a un champ Longueur d'option, les mises en œuvre peuvent utiliser d'autres algorithmes tels que HMAC_SHA256.

Cette option DOIT être la dernière option de mobilité présente.

### 6.4.6 Accusé de réception d'annonce de voisin (NAACK)

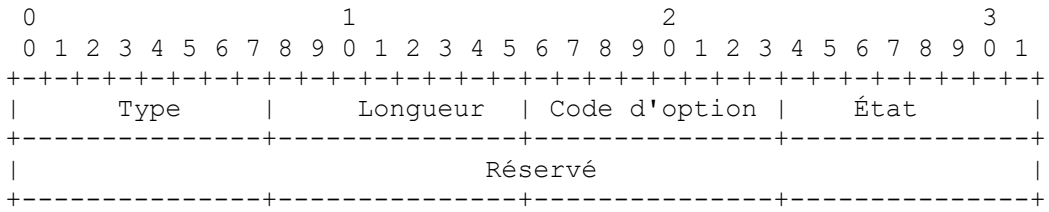


**Figure 16 : Option Accusé de réception d'annonce de voisin**

Type : 20

Longueur : entier non signé de 8 bits. Longueur de l'option, en unités de 8 octets. La longueur est 1 quand une nouvelle CoA n'est pas fournie. La longueur est 3 quand une nouvelle CoA est présente (suivant immédiatement le champ Réservé).

Code d'option : 0

État : entier non signé de 8 bits indiquant la disposition du message Annonce de voisin non sollicitée. Les valeurs d'état suivantes sont définies actuellement :
1 : NCoA invalide, effectuer une configuration d'adresse.
2 : NCoA invalide, utiliser la NCoA fournie. La NCoA fournie sous la forme d'une option Adresse IP DOIT être présente à la suite du champ Réservé.
3 : NCoA invalide, utiliser l'adresse IP du NAR comme NCoA dans la FBU.
4 : PCoA fournie, ne pas envoyer de FBU.
128 : adresse de couche de liaison non reconnue.

Réservé : DOIT être réglé à zéro par l'envoyeur et DOIT être ignoré par le receveur.

Le NAR répond à une UNA par une option NAACK pour notifier au MN d'utiliser une NCoA différente de celle qu'a utilisé le MN. Si le NAR propose une NCoA différente, l'annonce de routeur DOIT utiliser l'adresse IP de source dans le message UNA comme adresse de destination, et utiliser l'adresse de couche 2 présente dans l'UNA. Le MN DOIT utiliser la NCoA si elle est fournie avec l'option NAACK. Si le NAACK indique que l'adresse de couche de liaison n'est pas reconnue (par exemple, si le MN utilise une LLA valide sur la liaison du PAR mais que cette LLA n'est pas valide sur la liaison du NAR du fait d'une technologie d'accès différente) le MN NE DOIT PAS utiliser la NCoA ou la PCoA et DEVRAIT commencer immédiatement le processus d'acquisition d'une NCoA différente au NAR.
À l'avenir, de nouveaux types d'option pourront être définis.

## 7. Considérations relatives au protocole et à l'appareil

Le protocole spécifié ici, par principe, n'introduit pas de changement ou des changements minimes aux protocoles en rapport. Par exemple, aucun changement au protocole de base IPv6 mobile n'est nécessaire afin de mettre en œuvre le

présent protocole. De même, aucun changement n'est introduit au protocole d'auto configuration d'adresse IPv6 sans état [RFC4862] et à DHCP [RFC3315]. Le protocole spécifie une extension facultative à la découverte de voisin [RFC4861] dans laquelle un routeur d'accès peut envoyer une annonce de routeur en réponse au message UNA (voir au paragraphe 6.3). À part cette extension, la spécification ne modifie pas le comportement de découverte de voisin (incluant les procédures effectuées lors du rattachement au PAR et lors du rattachement au NAR).

Le protocole n'exige pas de changement d'un appareil intermédiaire de couche 2 entre un MN et son routeur d'accès qui prend en charge la présente spécification. Cela inclut les points d'accès sans fil, les commutateurs, les appareils de surveillance, et ainsi de suite.

## 8. Évolution et compatibilité par rapport à la RFC 4068

Le présent document a évolué depuis la [RFC4068]. Spécifiquement, une nouveau protocole d'établissement de clé de transfert (voir la [RFC5269]) a été défini pour permettre une association de sécurité entre un nœud mobile et son routeur d'accès. Cela permet la mise à jour sûre de l'acheminement des paquets durant un transfert. À l'avenir, de nouvelles spécifications pourront être définies pour établir de telles associations de sécurité selon le scénario de déploiement particulier.

Le protocole a été amélioré par les expériences de mise en œuvre [RFC4068], et par l'usage expérimental. Ces apports ont amélioré la spécification des champs de paramètres (comme la durée de vie, les codets, etc.) ainsi que l'inclusion de nouveaux champs de paramètres dans les messages existants. Au moment de la rédaction, il y a deux mises en œuvre publiquement disponibles, [fmipv6] et [tarzan], et plusieurs mises en œuvre propriétaires. Certaines expériences suggèrent que le protocole satisfait les exigences de délai et de perte de paquet quand il est utilisé de façon appropriée avec des protocoles d'accès radio particuliers. Par exemple, voir la [RFC5184] et [mip6-book]. Néanmoins, il est important de reconnaître que les performances de transfert sont une fonction des opérations de la couche IP, que spécifient le présent protocole, et de la technologie d'accès radio particulière, sur laquelle ce protocole s'appuie mais ne modifie pas.

Une mise en œuvre existante de la [RFC4068] a besoin d'une mise à jour afin de prendre en charge la présente spécification. Le principal ajout est l'établissement d'une association de sécurité entre un MN et son routeur d'accès (c'est-à-dire, entre MN et PAR). Une façon d'établir cette association de sécurité est spécifiée dans la [RFC5269]. Une mise en œuvre qui se conforme à la spécification de ce document va probablement fonctionner aussi avec la [RFC4068], excepté pour l'option Données d'autorisation de lien pour FMIPv6 (voir au paragraphe 6.4.5) qui ne peut être traitée que quand une association de sécurité est en place entre un nœud mobile et son routeur d'accès. La présente spécification déconseille le message Annonce de voisin rapide (FNA, *Fast Neighbor Advertisement*). Cependant, il est acceptable qu'un NAR traite ce message provenant d'un nœud mobile comme spécifié dans la [RFC4068].

## 9. Paramètres configurables

Les nœuds mobiles s'appuient sur les paramètres de configuration montrés dans le tableau ci-dessous. Chaque nœud mobile DOIT avoir un mécanisme de configuration pour ajuster les paramètres. Un tel mécanisme de configuration peut être local (comme une interface de ligne de commande) ou fondé sur la gestion centrale d'un certain nombre de nœuds mobiles.

| Nom de paramètre | Valeur par défaut | Définition |
|---|---|---|
| RTSOLPR_RETRIES | 3 | paragraphe 6.1.1 |
| MAX_RTSOLPR_RATE | 3 | paragraphe 6.1.1 |
| FBU_RETRIES | 3 | paragraphe 6.2.2 |
| PROXY_ND_LIFETIME | 1,5 seconde | paragraphe 6.2.1.2 |
| HI_RETRIES | 3 | paragraphe 6.2.1.1 |

## 10. Considérations sur la sécurité

Les vulnérabilités de la sécurité suivantes sont identifiées et les solutions suggérées sont mentionnées.

FBU non sûre : dans ce cas, des paquets destinés à une adresse pourraient être volés ou redirigés sur un nœud inattendu. Ce souci est le même que dans la relation entre un MN et l'agent de rattachement.

Donc, le PAR DOIT s'assurer que le paquet de FBU arrive d'un nœud qui possède légitimement la PCoA. Le routeur d'accès et ses hôtes peuvent utiliser tout mécanisme disponible pour établir une association de sécurité qui DOIT être utilisée pour sécuriser la FBU. La version actuelle de ce protocole s'appuie sur un protocole voisin [RFC5269] pour établir une telle association de sécurité. En utilisant la clé de transfert partagée de la [RFC5269], l'authentifiant dans l'option BADF (voir au paragraphe 6.4.5) DOIT être calculé, et l'option BADF incluse dans les messages FBU et FBack.

FBU sécurisée, redirection malveillante ou involontaire : dans ce cas, la FBU est sécurisée, mais la cible du lien se trouve être un nœud inattendu soit par une opération involontaire, soit dans une intention malveillante. Cette vulnérabilité peut conduire à un MN avec une authentique association de sécurité avec son routeur d'accès qui redirige le trafic à une adresse incorrecte.

Cependant, la cible de la redirection malveillante du trafic est limitée à une interface sur un routeur d'accès avec lequel le PAR a une association de sécurité. Le PAR DOIT vérifier que la NCoA à laquelle la PCoA est liée appartient réellement au préfixe du NAR. Pour faire cela, les échanges de messages HI et HAck sont à utiliser. Quand le NAR accepte la NCoA dans la HI (avec Code = 0) il agit comme mandataire de la NCoA afin que tous les paquets arrivants ne soient pas envoyés sur la liaison jusqu'à ce que le MN se rattache et s'annonce par la UNA. Donc, toute redirection par inadvertance ou malveillance à un hôte est évitée. Il est quand même possible de mettre la pagaille dans la mémoire tampon du NAR avec du trafic redirigé. Cependant, comme un état de transfert d'un NAR correspondant à une NCoA a une durée de vie finie (et courte) correspondant à un petit multiple de la latence de transfert anticipée, la portée de cette vulnérabilité est raisonnablement faible.

Envoi d'une FBU à partir d'une liaison du NAR : un nœud malveillant peut envoyer une FBU à partir de la liaison d'un NAR en fournissant l'adresse d'un nœud qui ne s'en doute pas comme NCoA. Cela est similaire à l'IP mobile de base où le MN peut fournir l'adresse IP d'un autre nœud comme sa CoA à son agent de rattachement ; ici, le PAR agit comme un "agent de rattachement temporaire" ayant une association de sécurité avec le nœud mobile et fournissant la prise en charge de la transmission pour le trafic de transfert. Comme dans IP mobile de base, cette mauvaise livraison est traçable pour le MN qui a une association de sécurité avec le routeur. Ainsi, il est possible d'isoler un tel MN si il continue de se conduire mal. De façon similaire, un MN qui a une association de sécurité avec le PAR peut fournir la LLA d'un autre noœud sur la liaison du NAR, qui peut causer la mauvaise livraison des paquets (destinés à la NCoA) à un nœud inattendu. Il est aussi possible dans ce cas de tracer le MN.

À part ce cas, les messages RtSolPr (paragraphe 6.1.1) et PrRtAdv (paragraphe 6.1.2) héritent des faiblesses du protocole de découverte de voisin [RFC4861]. Précisément, quand son routeur d'accès est compromis, un attaquant peut répondre au message RtSolPr du MN et fournir un routeur félon pour la résolution. Si le MN se rattachait à un tel routeur félon, sa communication pourrait être compromise. De même, un message PrRtAdv (voir au paragraphe 3.3) initié par le réseau provenant d'un attaquant pourrait causer un transfert du MN à un routeur félon. Lorsque ces faiblesses font problème, une solution comme la découverte de voisin sécurisée (SEND, *Secure Neighbor Discovery*) [RFC3971] DEVRAIT être envisagée.

Le protocole fournit la prise en charge de la mise en mémoire tampon des paquets durant un transfert de MN. Cela est fait en échangeant en toute sécurité les messages Initier le transfert (HI) et Accusé de réception de transfert (HAck) en réponse au message FBU provenant d'un MN. Il est possible qu'un MN échoue, par inadvertance ou de façon délibérée à entreprendre un transfert au NAR, qui fournit normalement la prise en charge de la mise en mémoire tampon. Cela peut causer un gaspillage de la mémoire du NAR contenant les paquets en mémoire tampon, et dans le pire des cas, pourrait créer des problèmes d'épuisement des ressources. Donc, les mises en œuvre doivent limiter la taille de la mémoire tampon par la configuration de la politique locale qui peut considérer des paramètres comme le délai moyen de transfert, la taille de paquets attendue, etc.

Les messages HI et HAck échangés entre PAR et NAR DOIVENT être protégés en utilisant une ou des associations de sécurité de bout en bout offrant la protection de l'intégrité et l'authentification de l'origine des données.

Le PAR et le NAR DOIVENT mettre en œuvre IPsec [RFC4301] pour la protection des messages HI et HAck. L'encapsulation de charge utile de sécurité IPsec (ESP, *Encapsulating Security Payload*) [RFC4303] en mode transport avec protection obligatoire de l'intégrité DEVRAIT être utilisé pour protéger les messages de signalisation. La protection de la confidentialité de ces messages n'est pas exigée.

Les associations de sécurité peuvent être créées en utilisant une configuration manuelle d'IPsec ou un protocole de négociation dynamique de clé comme la version 2 du protocole d'échange de clés Internet (IKEv2, *Internet Key Exchange Protocol version 2*) [RFC4306]. Si IKEv2 est utilisé, le PAR et le NAR peuvent utiliser tous les mécanismes d'authentification, comme spécifié dans la RFC 4306, pour l'authentification mutuelle. Cependant, pour assurer une

interopérabilité basique, les mises en œuvre DOIVENT prendre en charge les secrets partagés pour l'authentification mutuelle. Les paragraphes qui suivent décrivent les entrées de base de données d'autorisation d'homologue (PAD, *Peer Authorization Database*) et de base de données de politique de sécurité (SPD, *Security Policy Database*) spécifiées dans la [RFC4301] quand IKEv2 est utilisé pour établir les associations de sécurité IPsec requises.

### 10.1 Entrées de base de données d'autorisation d'homologue avec IKEv2

Ce paragraphe décrit les entrées de PAD sur le PAR et le NAR. Les entrées de PAD sont seulement des exemples de configurations. Noter que le PAD est un concept logique, et une mise en œuvre particulière de PAR ou de NAR peut l'appliquer de toute façon qui lui est propre. L'état du PAD peut aussi être distribué à travers diverses bases de données d'une manière spécifique de la mise en œuvre.

PAD de PAR :
- SI identité_distante = identité_nar_1 ALORS authentifier (secret/certificat/EAP partagé) et autoriser SA_FILLE pour l'adresse distante adresse_nar_1

PAD de NAR :
- SI identité_distante = identité_par_1 ALORS authentifier (secret/certificat/EAP partagé) et autoriser SA_FILLE pour l'adresse distante adresse_par_1

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

### 10.2 Entrées de base de données de politique de sécurité

Ce paragraphe décrit les entrées de politique de sécurité sur le PAR et le NAR requises pour protéger les messages HI et HAck. Les entrées de SPD sont seulement des exemples de configuration. Une mise en œuvre particulière de PAR ou de NAR pourrait configurer des entrées de SPD différentes pour autant qu'elles fournissent la sécurité requise.

Dans les exemples ci-dessous, l'identité du PAR est supposé être par_1, l'adresse du PAR est supposée être adresse_par_1, et l'adresse du NAR est supposée être adresse_nar_1.

SPD-S du PAR :
- SI adresse_locale = adresse_par_1 & adresse_distante = adresse_nar_1 & proto = MH & type_local_mh = HI & type_mh_distant = HAck ALORS utiliser Initier une SA ESP en mode transport en utilisant IDi = par_1 pour adresser adresse_nar_1

SPD-S du NAR :
- SI adresse_locale = adresse_nar_1 & adresse_distante = adresse_par_1 & proto = MH & type_local_mh = HAck & type_mh_distant = HI ALORS utiliser une SA ESP en mode transport.

## 11. Considérations relatives à l'IANA

Le présent document définit deux nouveaux messages d'en-tête de mobilité qui ont reçu une allocation de type dans le registre des types d'en-tête de mobilité :
14 message Initier le transfert (paragraphe 6.2.1.1)
15 message Accusé de réception de transfert (paragraphe 6.2.1.2)

Le présent document définit une nouvelle option de mobilité qui a reçu une allocation de type dans le registre des types d'options de mobilité :
1. Option Adresse/Préfixe IPv6 d'en-tête de mobilité (34), décrite au paragraphe 6.4.2

Le présent document définit un nouveau message ICMPv6, qui a été alloué dans le registre des types ICMPv6 :

154 messages FMIPv6

Le présent document crée un nouveau registre pour le champ "Sous type" dans le message ICMPv6 ci-dessus, appelé "Types de messages FMIPv6". L'IANA a alloué les valeurs suivantes :

| Sous-type | Description | Référence |
|---|---|---|
| 2 | RtSolPr | paragraphe 6.1.1 |
| 3 | PrRtAdv | paragraphe 6.1.2 \| |
| 4 | HI – déconseillé | paragraphe 6.2.1.1 \| |
| 5 | HAck – déconseillé | paragraphe 6.2.1.2 \| |

Les valeurs '0' et '1' sont réservées. La limite supérieure est 255. Une RFC est requise pour une nouvelle allocation de message. Les valeurs de sous type 4 et 5 sont déconseillées mais marquées comme indisponibles pour de futures allocations.

Le document définit une nouvelle option de mobilité qui a reçu une allocation de type dans le registre des types d'options de mobilité :

1. Option Données d'autorisation de lien pour FMIPv6 (BADF) (21), décrite au paragraphe 6.4.5

Le document définit les options suivantes de découverte de voisin [RFC4861] qui ont reçu une allocation de type de l'IANA :

| Type | Description | Référence |
|---|---|---|
| 17 | Option Adresse/Préfixe IP | paragraphe 6.4.1 |
| 19 | Option Adresse de couche de liaison | paragraphe 6.4.3 |
| 20 | Option Accusé de réception d'annonce de voisin | paragraphe 6.4.6 |

Le document définit les messages suivants d'en-tête de mobilité qui ont reçu une allocation de type dans le registre des types d'en-tête de mobilité :
1. Mise à jour rapide de lien (8), décrit au paragraphe 6.2.2
2. Accusé de réception de lien rapide (9), décrit au paragraphe 6.2.3

Le document définit l'option de mobilité suivante qui a reçu une allocation de type dans le registre des types d'options de mobilité :
1. Option Adresse de couche de liaison d'en-tête de mobilité (7), décrit au paragraphe 6.4.4

## 12. Remerciements

L'éditeur tient à remercier tous ceux qui ont fourni des réactions sur cette spécification, mais peut seulement en mentionner quelques uns ici : Vijay Devarapalli, Youn-Hee Han, Emil Ivov, Syam Madanapalli, Suvidh Mathur, Andre Martin, Javier Martin, Koshiro Mitsuya, Gabriel Montenegro, Takeshi Ogawa, Sun Peng, YC Peng, Alex Petrescu, Domagoj Premec, Subba Reddy, K. Raghav, Ranjit Wable, et Jonathan Wood. Behcet Sarikaya et Frank Xia sont remerciés pour leurs retours sur le fonctionnement dans les liaisons point à point. L'éditeur tient à remercier de sa contribution James Kempf qui améliore cette spécification. Vijay Devarapalli a fourni du texte pour la configuration de la sécurité entre routeurs d'accès à la Section 10. Merci à Jari Arkko pour sa relecture détaillée, qui a amélioré ce document. l'éditeur remercie aussi le président du groupe de travail MIPSHOP Gabriel Montenegro et les premiers présidents du groupe de travail IP MOBILE IBasavaraj Patil et Phil Roberts pour leur soutien à ce travail.

## 13. Références

### 13.1 Références normatives

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

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

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

RFC6275)

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

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

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

[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, RFC9131)

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

[RFC5268] R. Koodli, éd., "Transferts intercellulaires rapides pour IPv6 mobile", juin 2008. (*Remplace* RFC4068, *remplacée par* RFC5568) *(P.S.)*

[RFC5269] J. Kempf, R. Koodli, "Distribution d'une clé symétrique de transfert intercellulaire rapide IPv6 mobile (FMIPv6) avec la découverte de voisin sécurisée (SEND)", juin 2008. *(P.S.)*

### 13.2 Références pour information

[fmipv6] "fmipv6.org : Home Page", <http://fmipv6.org>.

[mip6-book] Koodli, R. and C. Perkins, "Mobile Inter-networking with IPv6", Chapter 22, John Wiley & Sons, Inc., 2007.

[RFC3290] Y. Bernet et autres, "Modèle informel de gestion pour routeurs Diffserv", mai 2002. *(Information)*

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

[RFC4068] R. Koodli, éd., "Transferts intercellulaires rapides pour IPv6 mobile", juillet 2005. (*Obsolète, voir* RFC5268) *(Exp.)*

[RFC5184] F. Teraoka et autres, "Abstractions de couche 2 unifiée pour transfert intercellulaire rapide piloté par la couche 3", mai 2008. *(Expérimentale)*

[RFC5213] S. Gundavelli et autres, "Mandataire IPv6 mobile", août 2008. *(P.S. ; MàJ par* RFC6543 *; MàJ par* RFC7864)

[RFC5555] H. Soliman, éd., "Prise en charge de IPv6 mobile pour hôtes et routeurs à double pile de protocoles", juin 2009. *(P. S.)*

[RFC5949] H. Yokota, K. Chowdhury, R. Koodli, B. Patil, F. Xia, "Transfert inter cellulaire rapide pour mandataire IPv6 mobile", septembre 2010. *(P.S.)*

[tarzan] "Nautilus6 - Tarzan", <http://software.nautilus6.org/TARZAN/>.

[x.s0057] 3GPP2, "E-UTRAN - eHRPD Connectivity et Interworking: Core Network Aspects", 3GPP2 X.S0057-0, avril 2009, <http://www.3gpp2.org/Public_html/Specs/X.S0057-0_v1.0_090406.pdf>.

## Appendice A. Contributeurs

Le présent document a son origine dans l'équipe de conception du transfert rapide dans le premier groupe de travail IP MOBILE. Les membres de cette équipe de conception sont, en ordre alphabétique : Gopal Dommety, Karim El-Malki, Mohammed Khalil, Charles Perkins, Hesham Soliman, George Tsirtsis, et Alper Yegin.

## Appendice B. Changements depuis la RFC 5268

Le présent document spécifie le format d'en-tête de mobilité pour les messages HI et HAck, et le format d'option d'en-tête de mobilité pour l'option Adresse/Préfixe IPv6. L'utilisation de ICMP pour les messages HI et HAck est déconseillée. Les développements suivants ont conduit le groupe de travail à adopter ces changements :

- Le protocole de mandataire IPv6 mobile [RFC5213] a été adopté pour le déploiement des réseaux mobiles de quatrième génération. Cela a établi l'en-tête de mobilité comme type par défaut pour la signalisation IP mobile critique.

- Le protocole IPv6 mobile [RFC3775] (en particulier, le protocole de double pile MIP6 ou DSMIP6 [RFC5555]) qui est aussi supposé être déployé dans les réseaux mobiles de quatrième génération, s'appuie de façon similaire sur l'en-tête de mobilité pour la signalisation IP mobile critique.

- Le protocole de transfert rapide spécifié dans le présent document est utilisé comme base du transfert rapide pour mandataire MIP6 [RFC5949], qui est adopté par les réseaux "HRPD amélioré" (CDMA) [x.s0057]. Donc, le protocole de transfert rapide, quand il est utilisé dans des déploiements qui utilisent PMIP6 ou MIP6, a besoin de prendre en charge l'en-tête de mobilité pour tous les messages critiques de signalisation de la mobilité. En même temps, l'utilisation de ICMP, principalement due au poids des traditions, ne va probablement pas faciliter la signalisation IP mobile critique sans un départ non trivial du déploiement de nouveaux protocoles de signalisation d'en-tête de mobilité.

Donc, il s'ensuit que la spécification de l'en-tête de mobilité pour les messages HI et HAck est nécessaire pour le déploiement du protocole à côté des protocoles PMIP6 et MIP6.

## Appendice C. Changements depuis la RFC 4068

Les changements et précisions majeurs sont les suivants :

- Une association de sécurité entre le MN et son routeur d'accès est spécifiée dans le document d'accompagnement [RFC5269].

- L'option Données d'autorisation de lien pour les transferts rapides (BADF) est spécifiée pour porter les paramètres de sécurité utilisés pour vérifier l'authenticité des messages FBU et FBack. La clé de transfert utilisée pour calculer l'authentifiant est spécifiée dans les documents d'accompagnement.

- La configuration de sécurité est spécifiée pour la signalisation inter routeurs d'accès (HI, HAck).

- Ajout d'un paragraphe sur la gestion de préfixe entre routeurs d'accès et illustration du fonctionnement du protocole sur des liaisons point à point.

- FNA, qui est un message d'en-tête de mobilité, est déconseillé. À sa place, le message Annonce de voisin non sollicitée (UNA, *Unsolicited Neighbor Advertisement*) provenant de la RFC 4861 est utilisé.

- Les options Adresse IPv6 et Préfixe IPv6 ont été combinées.

- Ajout de la description de l'exigence de DAD sur le NAR quand on détermine l'unicité de la NCoA à la Section 4, "Détails du protocole".

- Ajout d'une nouvelle valeur de code pour qu'un message HAck gratuit déclenche un message HI.

- Ajout du code d'option 5 dans le message PrRtAdv pour indiquer l'usage de la gestion de la mobilité localisée fondée

sur le réseau (NETLMM, *Network-based Localized Mobility Management*).

- Précisé l'usage du protocole quand DHCP est utilisé pour la formulation de la NCoA (paragraphes 6.1.2, 3.1, et 5.2). Ajout d'une nouvelle valeur de code (5) dans PrRtAdv (paragraphe 6.1.2).

- Précisé que les opérations de découverte de voisin IPv6 sont un DOIT à la Section 7, "Considérations relatives au protocole et aux appareils".

- Précisé que "PAR = HA temporaire" pour les FBU envoyées par le véritable MN à une CoA inattendue.

## Adresse de l'auteur

Rajeev Koodli (editor)
Starent Networks
USA
mél : rkoodli@starentnetworks.com