Équipe d'ingénierie de l'Internet (IETF)
**Request for Comments : 5944**
RFC rendue obsolète : 3344
Catégorie : Sur la voie de la normalisation
ISSN: 2070-1721

C. Perkins, éditeur, WiChorus Inc.
novembre 2010

Traduction Claude Brière de L'Isle

# Prise en charge de la mobilité IP pour IPv4, révisée

**Résumé**
Le présent document spécifie des améliorations au protocole qui permettent un acheminement transparent des datagrammes IP sur les nœuds mobiles dans l'Internet. Chaque nœud mobile est toujours identifié par son adresse de rattachement, sans considération de son point de rattachement réel dans l'Internet. Lorsque il est situé hors de son domaine de rattachement, un nœud mobile est aussi associé à une adresse d'entretien, qui donne des informations sur son point de rattachement actuel dans l'Internet. Le protocole assure l'enregistrement de l'adresse d'entretien auprès d'un agent de rattachement. L'agent de rattachement envoie des datagrammes destinés au nœud mobile à travers un tunnel à l'adresse d'entretien. Après l'arrivée au bout du tunnel, chaque datagramme est alors livré au nœud mobile.

**Statut de ce mémoire**
Ceci est un document de l'Internet sur la voie de la normalisation.
*(La présente traduction incorpore les errata 3116, 3428, 3438, 4133 et 4134.)*
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 paragraphe 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/rfc5944



## Table des matières

## 1. Introduction

IP version 4 suppose que l'adresse IP d'un nœud identifie de façon univoque le point de rattachement du nœud à l'Internet. Donc, un nœud doit être situé sur le réseau indiqué par son adresse IP afin de recevoir les datagrammes qui lui sont destinés ; autrement, les datagrammes destinés au nœud vont être indélivrables. Pour qu'un nœud change son point de rattachement sans perdre sa capacité de communiquer, un des deux mécanismes suivants doit normalement être employé :

o le nœud doit changer son adresse IP chaque fois qu'il change son point de rattachement, ou

- o les chemins spécifiques d'un hôte doivent être propagés à travers une grande partie du système d'acheminement de l'Internet.

Ces deux solutions sont souvent inacceptables. La première rend impossible à un nœud de conserver les connexions de couche transport et de couches supérieures quand le nœud change sa localisation. La seconde a d'évidents et sévères problèmes d'adaptation, en particulier quand on considère la croissance explosive des ventes de tablettes (mobiles) d'ordinateurs.

Un nouveau mécanisme, adaptable est nécessaire pour s'accommoder de la mobilité des nœuds au sein de l'Internet. Le présent document définit un tel mécanisme, qui permet aux nœuds de changer leur point de rattachement à l'Internet sans changer leur adresse IP.

Les changements entre cette spécification révisée pour IP mobile et les spécifications originales (voir [RFC2002], [RFC2003], [RFC2004], [RFC2005], [RFC2006], et [RFC3220]) sont détaillés dans l'Appendice F.

### 1.1 Exigences du protocole

Un nœud mobile doit être capable de communiquer avec les autres nœuds après avoir changé son point de rattachement de couche de liaison à l'Internet, et sans changer son adresse IP.

Un nœud mobile doit être capable de communiquer avec les autres nœuds qui ne mettent pas en œuvre ces fonctions de mobilité. Aucune amélioration du protocole n'est exigée des hôtes ou routeurs qui n'agissent pas comme une des nouvelles entités architecturales introduites au paragraphe 1.5.

Tous les messages utilisés pour mettre à jour un autre nœud quant à la localisation d'un nœud mobile doivent être authentifiés afin de protéger contre les attaques de redirection à distance.

### 1.2 Buts

La liaison par laquelle un nœud mobile est directement rattaché à l'Internet peut souvent être une liaison sans fil. Cette liaison peut donc avoir une bande passante substantiellement inférieure et un taux d'erreur plus fort que les réseaux filaires traditionnels. De plus, les nœuds mobiles sont probablement alimentés par une batterie, et minimiser la consommation d'énergie est important. Donc, le nombre de messages administratifs envoyés sur la liaison par laquelle un nœud mobile est directement rattaché à l'Internet devrait être minimisé, et la taille de ces messages devrait être aussi petite que raisonnablement possible.

### 1.3 Hypothèses

Les protocoles définis dans le présent document ne fixent pas de contraintes supplémentaires à l'allocation des adresses IP. C'est-à-dire qu'un nœud mobile peut recevoir une adresse IP allouée par l'organisation qui possède la machine.

Ce protocole suppose que les nœuds mobiles ne vont généralement pas changer leur point de rattachement à l'Internet plus fréquemment qu'une fois par seconde.

Ce protocole suppose que les datagrammes IP en envoi individuel sont acheminés sur la base de l'adresse de destination qui est dans l'en-tête du datagramme (et non, par exemple, par l'adresse de source).

### 1.4 Applicabilité

IP mobile est destiné à permettre aux nœuds de se déplacer d'un sous réseau IP à un autre. Il est tout aussi convenable à la mobilité à travers des supports homogènes qu'à la mobilité à travers des supports hétérogènes. C'est-à-dire que IP mobile facilite le mouvement des nœuds d'un segment Ethernet à un autre, aussi bien que d'un segment Ethernet à un LAN sans fil, pour autant que l'adresse IP du nœud mobile reste la même après un tel mouvement.

On peut voir IP mobile comme une solution au problème de la gestion de la "macro" mobilité. Il convient bien pour des applications de gestion de la mobilité plus "micro" -- par exemple, le transfert entre des émetteurs-récepteurs sans fil, dont chacun couvre seulement une très petite zone géographique. Tant que le mouvement du nœud ne se produit pas entre des points de rattachement sur des sous réseaux IP différents, les mécanismes de couche de liaison pour la mobilité (c'est-à-dire, le transfert de couche de liaison) peuvent offrir une convergence plus rapide et beaucoup moins de frais généraux que IP mobile.

### 1.5 Nouvelles entités architecturales

IP mobile introduit les nouvelles entités fonctionnelles suivantes :

Nœud mobile : hôte ou routeur qui change son point de rattachement d'un réseau ou sous réseau à un autre. Un nœud mobile peut changer sa localisation sans changer son adresse IP ; il peut continuer à communiquer avec d'autres nœuds de l'Internet à toute localisation en utilisant son adresse IP (constante) en supposant que la connexité de couche de liaison à un point de rattachement est disponible.

Agent de rattachement : un routeur sur le réseau de rattachement d'un nœud mobile qui tunnelle les datagrammes pour les livrer au nœud mobile quand il est loin de son rattachement, et conserve les informations sur la localisation actuelle pour le nœud mobile.

Agent étranger : un routeur sur le réseau visité d'un nœud mobile qui fournit des services d'acheminement au nœud mobile lorsque il est enregistré. L'agent étranger détunnelle et livre au nœud mobile les datagrammes qui ont été tunnelés par l'agent de rattachement du nœud mobile. Pour les datagrammes envoyés par un nœud mobile, l'agent étranger peut servir de routeur par défaut pour les nœuds mobiles enregistrés.

Un nœud mobile reçoit une adresse IP de long terme sur un réseau de rattachement. Cette adresse de rattachement est administrée de la même façon que l'est une adresse IP "permanente" à un hôte stationnaire. Quand il est hors de son réseau de rattachement, une "adresse d'entretien" est associée au nœud mobile et reflète le point de rattachement actuel du nœud mobile. Le nœud mobile utilise son adresse de rattachement comme adresse de source de tous les datagrammes IP qu'il envoie, sauf lorsque décrit autrement dans le présent document pour les datagrammes envoyés pour certaines fonctions de gestion de la mobilité (par exemple, comme au paragraphe 3.6.1.1).

### 1.6. Terminologie

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

De plus, le présent document utilise fréquemment les termes suivants :

Extension Activation d'autorisation : authentification qui rend un message (d'enregistrement) acceptable pour le receveur ultime du message d'enregistrement. Une extension Activation d'autorisation DOIT contenir un indice de paramètre de sécurité (SPI, *Security Parameter Index*). Dans le présent document, toutes les utilisations de l'extension Activation d'autorisation se réfèrent aux extensions d'authentification qui permettent au message Demande d'enregistrement d'être acceptable à l'agent de rattachement. En utilisant des structures de protocole supplémentaires spécifiées en dehors du présent document, il peut être possible au nœud mobile de fournir l'authentification de son enregistrement à l'agent de rattachement, au moyen d'une autre entité authentifiante au sein du réseau, qui est acceptable à l'agent de rattachement (par exemple, voir la [RFC2794]).

Annonce d'agent : message d'annonce construit en attachant une extension spéciale à un message d'annonce de routeur [RFC1256].

Authentification : processus de vérification (en utilisant des techniques cryptographiques, pour toutes les applications de la présente spécification) de l'identité du générateur d'un message.

Adresse d'entretien : point de terminaison d'un tunnel vers un nœud mobile, pour les datagrammes transmis au nœud mobile lorsque il est hors de son domaine. Le protocole peut utiliser deux types différents d'adresse d'entretien : une "adresse d'entretien d'agent étranger " est une adresse d'un agent étranger avec lequel le nœud mobile est enregistré, et une "adresse d'entretien colocalisée" est une adresse locale obtenue de l'extérieur que le nœud mobile a associé à une de ses propres interfaces réseau.

Nœud correspondant : homologue avec lequel un nœud mobile est en communication. Un nœud correspondant peut être mobile ou stationnaire.

Réseau étranger : tout réseau autre que le réseau de rattachement d'un nœud mobile.

ARP gratuit : paquet de protocole de résolution d'adresse (ARP, *Address Resolution Protocol*) envoyé par un nœud afin de causer spontanément la mise à jour d'une entrée par les autres nœuds dans leur antémémoire ARP [TCP/IP]. Voir au paragraphe 4.6.

Adresse de rattachement : adresse IP allouée pour une période longue à un nœud mobile. Elle reste inchangée sans considération de l'endroit où le nœud est rattaché à l'Internet.

Réseau de rattachement : réseau, éventuellement virtuel, qui a un préfixe de réseau qui correspond à celui de l'adresse de rattachement d'un nœud mobile. Noter que les mécanismes standard d'acheminement IP vont livrer les datagrammes destinés à l'adresse de rattachement d'un nœud mobile au réseau de rattachement du nœud mobile.

Liaison : facilité ou support sur lequel les nœuds peuvent communiquer à la couche de liaison. Une liaison sous-tend la couche réseau.

Adresse de couche de liaison : adresse utilisée pour identifier un point d'extrémité d'une communication sur une liaison physique. Normalement, l'adresse de couche de liaison est une adresse de contrôle d'accès au support (MAC, *Media Access Control*) d'une interface.

Agent de mobilité : agent de rattachement ou agent étranger.

Lien de mobilité : association d'une adresse de rattachement et d'une adresse d'entretien, avec la durée de vie restante de cette association.

Association de sécurité de mobilité : collection de contextes de sécurité, entre une paire de nœuds, qui peut être appliquée aux messages de protocole IP mobile échangés entre eux. Chaque contexte indique un algorithme et mode d'authentification (paragraphe 5.1), un secret (une clé partagée, ou une paire appropriée de clés publique/privée), et un style de protection contre la répétition en usage (paragraphe 5.7).

Nœud : hôte ou routeur.

Nom occasionnel : valeur choisie au hasard, différente des choix précédents, insérée dans un message pou protéger contre les répétitions.

Indice de paramètre de sécurité (SPI, *Security Parameter Index*) : indice qui identifie un contexte de sécurité entre une paire de nœuds, parmi les contextes disponibles dans l'association de sécurité de mobilité. Les valeurs de SPI de 0 à 255 sont réservées et NE DOIVENT PAS être utilisées dans une association de sécurité de mobilité.

Tunnel : chemin suivi par un datagramme pendant qu'il est encapsulé. Le modèle est que, pendant qu'il est encapsulé, un datagramme est acheminé à un agent de désencapsulement connaissable, qui désencapsule le datagramme et le livre ensuite correctement à sa destination ultime.

Réseau virtuel : réseau sans instanciation physique au delà d'un routeur (avec une interface réseau physique sur un autre réseau). Le routeur (par exemple, un agent de rattachement) annonce généralement l'accessibilité au réseau virtuel en utilisant les protocoles d'acheminement conventionnels.

Réseau visité : réseau autre que le réseau de rattachement d'un nœud mobile, auquel le nœud mobile est actuellement connecté.

Liste de visiteurs : liste des nœuds mobiles qui visitent un agent étranger.

### 1.7 Généralités sur le protocole

Les services de soutien suivants sont définis pour IP mobile :

Découverte d'agent : les agents de rattachement et les agents étrangers peuvent annoncer leur disponibilité sur chaque liaison pour laquelle ils fournissent le service. Un nœud mobile nouvellement arrivé peut envoyer une sollicitation sur la liaison pour apprendre si des agents possibles sont présents.

Enregistrement : quand le nœud mobile est hors de chez lui, il enregistre son adresse d'entretien auprès de son agent de rattachement. Selon sa méthode de rattachement, le nœud mobile va s'enregistrer soit directement auprès de son agent de rattachement, soit par un agent étranger qui transmet l'enregistrement à l'agent de rattachement.

Élimination en silence : la mise en œuvre élimine le datagramme sans autre traitement, et sans indiquer d'erreur à l'envoyeur. La mise en œuvre DEVRAIT fournir la capacité d'enregistrer l'erreur, incluant le contenu du datagramme éliminé, et DEVRAIT enregistrer l'événement dans un compteur statistique.

Les étapes suivantes fournissent une description générale du fonctionnement du protocole IP mobile :

- Les agents de mobilité (c'est-à-dire, agents étrangers et agents de rattachement) annoncent leur présence via des messages d'annonce d'agent (paragraphe 2). Un nœud mobile peut facultativement solliciter un message d'annonce d'agent de tous les agents de mobilité rattachés localement au moyen d'un message de sollicitation d'agent.

- Un nœud mobile reçoit ces annonces d'agent et détermine si il est sur son réseau de rattachement ou sur un réseau étranger.

- Quand le nœud mobile détecte qu'il est situé sur son réseau de rattachement, il fonctionne sans services de mobilité. Si il retourne à son réseau de rattachement après avoir été enregistré ailleurs, le nœud mobile se désenregistre de son agent de rattachement, par un échange de messages Demande d'enregistrement et Réponse d'enregistrement avec lui.

- Quand un nœud mobile détecte qu'il est passé sur un réseau étranger, il obtient une adresse d'entretien sur le réseau étranger. L'adresse d'entretien peut être déterminée à partir des annonces d'un agent étranger (l'adresse d'entretien d'un agent étranger) ou par des mécanismes d'allocation externes comme DHCP [RFC2131] (une adresse d'entretien co-localisée).

- Le nœud mobile qui fonctionne hors de son domaine enregistre alors sa nouvelle adresse d'entretien auprès de son agent de rattachement par l'échange d'un message Demande d'enregistrement et Réponse d'enregistrement avec l'agent de rattachement, éventuellement via un agent étranger (paragraphe 3).

- Les datagrammes envoyés à l'adresse de rattachement du nœud mobile sont interceptés par son agent de rattachement, tunnelés par l'agent de rattachement à l'adresse d'entretien du nœud mobile, reçus au point d'extrémité du tunnel (à l'agent étranger ou au nœud mobile lui-même) et finalement livrés au nœud mobile (paragraphe 4.2.3).

- Dans la direction inverse, les datagrammes envoyés par le nœud mobile sont généralement livrés à leur destination en utilisant les mécanismes d'acheminement IP standard, pas nécessairement en passant par l'agent de rattachement.

Lorsque il est hors de chez lui, IP mobile utilise le tunnelage de protocole pour cacher une adresse de rattachement du nœud mobile aux routeurs intermédiaires entre son réseau de rattachement et sa localisation actuelle. Le tunnel se termine à l'adresse d'entretien du nœud mobile. L'adresse d'entretien doit être une adresse à laquelle les datagrammes peuvent être livrés via l'acheminement IP conventionnel. À l'adresse d'entretien, le datagramme original est retiré du tunnel et livré au nœud mobile.

IP mobile fournit deux modes alternatifs pour l'acquisition d'une adresse d'entretien :

a. Une "adresse d'entretien d'agent étranger" est une adresse d'entretien fournie par un agent étranger par ses messages d'annonce d'agent. Dans ce cas, l'adresse d'entretien est une adresse IP de l'agent étranger. Dans ce mode, l'agent étranger est le point d'extrémité du tunnel et, à réception des datagrammes tunnelés, il les désencapsule et livre le datagramme interne au nœud mobile. Ce mode d'acquisition est préféré parce que il permet à de nombreux nœuds mobiles de partager la même adresse d'entretien et donc ne fait pas peser de demandes inutiles sur l'espace d'adresses déjà limité de IPv4.

b. Une "adresse d'entretien colocalisée" est une adresse d'entretien acquise par le nœud mobile comme adresse IP locale par des moyens externes, que le nœud mobile associe alors à une de ses propres interfaces réseau. L'adresse peut être acquise dynamiquement comme adresse temporaire par le nœud mobile, comme par DHCP [RFC2131], ou peut être possédée par le nœud mobile comme adresse de long terme pour sa seule utilisation quand il visite un réseau étranger. Les méthodes externes spécifiques d'acquisition d'une adresse IP locale à utiliser comme adresse d'entretien colocalisée sortent du domaine d'application du présent document. Quand il utilise une adresse d'entretien colocalisée, le nœud mobile sert de point d'extrémité de tunnel et il effectue lui-même la désencapsulation des datagrammes qui lui sont tunnelés.

Le mode qui utilise une adresse d'entretien colocalisée présente l'avantage de permettre à un nœud mobile de fonctionner sans agent étranger, par exemple, dans les réseaux qui n'ont pas encore déployé un agent étranger. Il fait cependant peser une charge supplémentaire sur l'espace d'adresses IPv4 parce que il exige un réservoir d'adresses au sein du réseau étranger qui soient disponibles pour les nœuds mobile visiteurs. Il est difficile de conserver efficacement des réservoirs d'adresses pour chaque sous réseau qui peut permettre des visites de nœuds mobiles.

Il est important de comprendre la distinction entre les fonctions d'adresse d'entretien et d'agent étranger. L'adresse d'entretien est simplement le point d'extrémité du tunnel. Elle peut bien sûr être une adresse d'un agent étranger (une adresse d'entretien d'agent étranger) mais elle peut aussi être une adresse acquise temporairement par le nœud mobile

(adresse d'entretien colocalisée). Par ailleurs, un agent étranger est un agent de mobilité qui fournit des services aux nœuds mobiles. Voir les détails aux paragraphes 3.7 et 4.2.2.

Un agent de rattachement DOIT être capable d'attirer et intercepter les datagrammes qui sont destinés à l'adresse de rattachement de tous ses nœuds mobiles enregistrés. En utilisant les mécanismes de mandataire et d'ARP gratuit décrits au paragraphe 4.6, cette exigence peut être satisfaite si l'agent de rattachement a une interface réseau sur la liaison indiquée par l'adresse de rattachement du nœud mobile. D'autres placements de l'agent de rattachement par rapport à la localisation de rattachement du nœud mobile PEUVENT aussi être possibles en utilisant d'autres mécanismes pour intercepter les datagrammes destinés à l'adresse de rattachement du nœud mobile. De tels placements sortent du domaine d'application du présent document.

De façon similaire, un nœud mobile et un agent étranger futur ou actuel DOIVENT être capables d'échanger des datagrammes sans s'appuyer sur les mécanismes d'acheminement IP standard ; c'est-à-dire, les mécanismes qui prennent les décisions de transmission sur la base du préfixe de réseau de l'adresse de destination dans l'en-tête IP. Cette exigence peut être satisfaite si l'agent étranger et le nœud mobile visiteur ont une interface sur la même liaison. Dans ce cas, le nœud mobile et l'agent étranger outrepassent simplement le mécanisme normal d'acheminement IP quand ils envoient l'un à l'autre des datagrammes, adressant les paquets de la couche de liaison sous-jacente à leurs adresses respectives de couche de liaison. D'autres placements de l'agent étranger par rapport au nœud mobile PEUVENT aussi être possibles en utilisant d'autres mécanismes pour échanger les datagrammes entre ces nœuds, mais de tels placements sortent du domaine d'application du présent document.

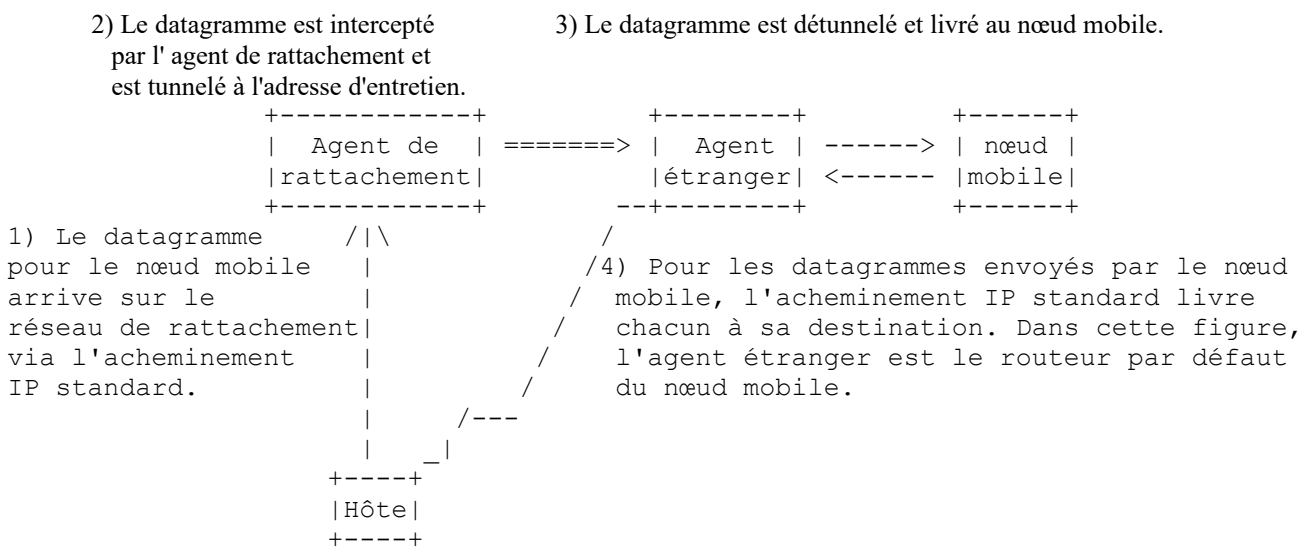



**Figure 1 : Fonctionnement de IPv4 mobile**

Si un nœud mobile utilise une adresse d'entretien colocalisée (comme décrit au point (b) ci-dessus) le nœud mobile DOIT être situé sur la liaison identifiée par le préfixe réseau de cette adresse d'entretien. Autrement, les datagrammes destinés à l'adresse d'entretien ne seraient pas livrables.

Par exemple, la Figure 1 illustre l'acheminement des datagrammes de et vers un nœud mobile hors de son domaine, une fois que le nœud mobile s'est enregistré auprès de son agent de rattachement. Dans la Figure 1, le nœud mobile utilise une adresse d'entretien d'agent étranger, et non une adresse d'entretien colocalisée.

### 1.8 Format de message et extensibilité du protocole

IP mobile définit un ensemble de nouveaux messages de commande, envoyés sur UDP [RFC0768] en utilisant le numéro d'accès bien connu 434. Les deux types de messages suivants sont définis dans le présent document :
1 : Demande d'enregistrement
3 : Réponse d'enregistrement

Les valeurs à jour de type de message pour les message de commandes IP mobile sont spécifiées dans la base de donnée en ligne de l'IANA [IANA].

De plus, pour la découverte d'agent, IP mobile utilise les messages existants Annonce de routeur et Sollicitation de routeur définis pour la découverte de routeur ICMP [RFC1256].

IP mobile définit un mécanisme général d'extension pour permettre que des informations facultatives soient portées par des messages de commande IP mobile ou par des messages de découverte de routeur ICMP. Certaines extensions ont été spécifiées comme étant codées dans le simple format Type-Longueur-Valeur décrit au paragraphe 1.9.

Les extensions permettent que des quantités d'informations variables soient portées dans chaque datagramme. La fin de la liste des extensions est indiquée par la longueur totale du datagramme IP.

Deux ensembles séparés d'espaces de numérotation, à partir desquels les valeurs de type d'extension sont allouées, sont utilisés dans IP mobile :

- Le premier ensemble consiste en les extensions qui peuvent apparaître dans les messages de commande IP mobile (ceux envoyés du et au numéro d'accès UDP 434). Dans le présent document, les types suivants sont définis pour les extensions qui apparaissent dans les messages de commande IP mobile :
  0 : bourrage d'un octet (codé sans champ Longueur ni Données)
  32 : authentification mobile-rattachement
  33 : authentification mobile-étranger
  34 : Authentification étranger-rattachement

- Le second ensemble consiste en les extensions qui peuvent apparaître dans les messages de découverte de routeur ICMP [RFC1256]. Dans le présent document, les types suivants sont définis pour les extensions qui apparaissent dans les messages ICMP de découverte de routeur :
  0 : bourrage d'un octet (codé sans champ Longueur ni Données)
  16 : annonce d'agent de mobilité
  19 : longueurs de préfixes

Chaque extension individuelle est décrite en détails dans un autre paragraphe du présent document. Les valeurs à jour de ces numéros de type d'extension sont spécifiées dans la base de données en ligne de l'IANA [IANA].

Du fait de la séparation (orthogonale) de ces ensembles, il est concevable que deux extensions qui seront définies ultérieurement puissent avoir des valeurs de type identiques, dans la mesure où une des extensions ne peut être utilisée que dans les messages de commande IP mobile et l'autre ne peut être utilisée que dans les messages ICMP de découverte de routeur.

Le champ Type dans la structure d'extension IP mobile peut prendre en charge jusqu'à 255 (sautables et non sautables) extensions identifiables de façon univoque. Quand une extension numérotée dans l'un ou l'autre de ces ensembles dans la gamme de 0 à 127 se rencontre mais n'est pas reconnue, le message contenant cette extension DOIT être éliminé en silence. Quand une extension numérotée dans la gamme de 128 à 255 se rencontre et n'est pas reconnue, cette extension particulière est ignorée, mais le reste de l'extension et les données du message DOIVENT quand même être traités. Le champ Longueur de l'extension est utilisé pour sauter le champ Données pour la recherche de la prochaine extension.

Sauf si une structure supplémentaire est utilisée pour les types d'extension, de nouveaux développements ou ajouts à IP mobile pourraient exiger une telle quantité de nouvelles extensions que l'espace disponible pour les types d'extension soit épuisé. Deux nouvelles structures d'extension sont proposées pour résoudre ce problème. Certains types d'extensions peuvent être agrégés, en utilisant des sous types pour identifier précisément l'extension, par exemple comme il a été fait avec les extensions génériques de clés d'authentification [RFC3957]. Dans de nombreux cas, cela peut réduire le taux d'allocation de nouvelles valeurs du champ Type.

Comme les nouvelles structures d'extension vont causer une utilisation efficace de l'espèce de type d'extensions, il est recommandé que les nouvelles extensions de IP mobile suivent un des deux nouveaux formats d"extension chaque fois qu'il y a une possibilité de grouper des extensions en rapport.

Les paragraphes qui suivent donnent des détails sur les trois structures distinctes pour les extensions IP mobile :
- Le format d'extension simple,
- Le format d'extension long,
- Le format d'extension court.

### 1.9 Format d'extension Type-Longueur-Valeur pour les extensions IP mobile

Le format Type-Longueur-Valeur illustré à la Figure 2 est utilisé pour les extensions qui sont spécifiées dans le présent document. Comme cette structure d'extension simple n'encourage pas à l'utilisation la plus efficace de l'espace de type d'extension, il est recommandé que les nouvelles extensions IP mobile suivent un des deux formats de nouvelle extension spécifié au paragraphe 1.10 ou 1.11 chaque fois qu'il y a une possibilité de grouper les extensions en rapport.

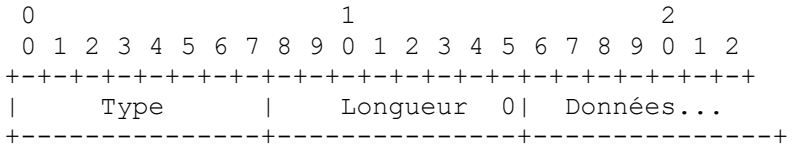



**Figure 2 : Format d'extension Type-Longueur-Valeur pour IPv4 mobile**

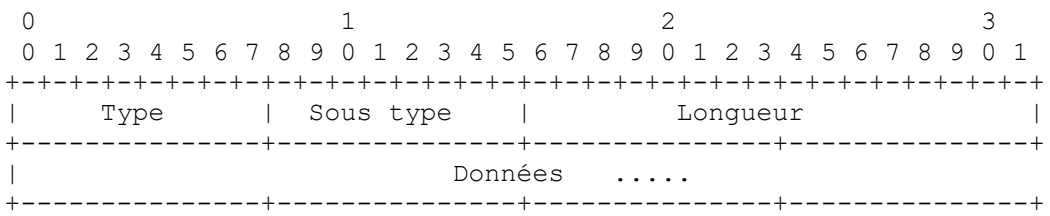
Type : Indique le type particulier de l'extension.

Longueur : Indique la longueur (en octets) du champ Données au sein de cette extension. La longueur N'inclut PAS les octets de Type et Longueur.

Données : données particulières associées à cette extension. Ce champ peut être long de zéro, un ou plusieurs octets. Le format et la longueur du champ Données sont déterminés par les champs Type et Longueur.

### 1.10 Format d'extension long

Ce format est applicable pour les extensions non sautables qui portent des informations de plus de 254 octets. Les extensions sautables ne peuvent jamais utiliser le format long, parce que le receveur n'est pas obligé d'inclure le code d'analyse et va probablement traiter les 8 bits qui suivent immédiatement le type comme champ Longueur.




Le format d'extension long exige que les champs suivants soient spécifiés dans les premiers champs de l'extension.

Type : c'est le type, qui décrit une collection d'extensions ayant un type de données commun.

Sous type : c'est un nombre unique donné à chaque membre dans le type agrégé.

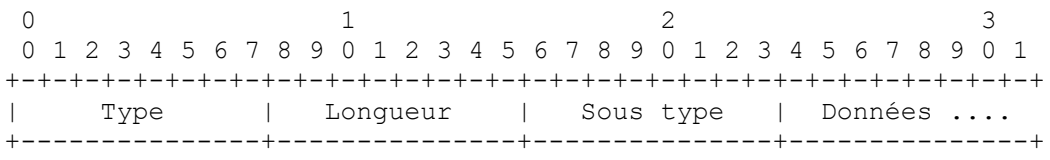
Longueur : indique la longueur (en octets) du champ Données au sein de cette extension. Il N'inclut PAS les octets de Type, Longueur, et Sous type.

Données : ce sont les données associées au sous type de cette extension. Cette spécification ne met aucune structure supplémentaire sur les données de sous type.

Comme le champ Longueur est de 16 bits, les données d'extension peuvent excéder 254 octets.

### 1.11 Format d'extension court

Ce format est compatible avec les extensions sautables définies au paragraphe 1.9. Il n'est pas applicable aux extensions qui exigent plus de 254 octets de données ; pour ces extensions, il faut utiliser le format décrit au paragraphe 1.10.




Le format d'extension court exige que les champs suivants soient spécifié comme premiers champs de l'extension :

Type : c'est le type, qui décrit une collection d'extensions qui ont un type de données commun.

Sous type : c'est un nombre unique donnée à chaque membre du type agrégé.

Longueur : entier non signé de 8 bits. Longueur de l'extension, en octets, excluant le type d'extension et le champ Longueur de l'extension. Ce champ DOIT être réglé à 1 plus la longueur totale du champ Données.

Données : ce sont les données associées à cette extension. La présente spécification ne met aucune structure supplémentaire sur les données de sous type.

## 2. Découverte d'agent

La découverte d'agent est la méthode par laquelle un nœud mobile détermine si il est actuellement connecté à son réseau de rattachement ou à un réseau étranger, et par laquelle un nœud mobile peut détecter quand il est passé d'un réseau à un autre. Lorsque il est connecté à un réseau étranger, les méthodes spécifiées dans cette section permettent aussi au nœud mobile de déterminer l'adresse d'entretien d'agent étranger offerte par chaque agent étranger sur ce réseau.

IP mobile étend la découverte de routeur ICMP [RFC1256] comme son principal mécanisme pour la découverte d'agent. Une annonce d'agent est formée par l'inclusion d'une extension Annonce d'agent de mobilité dans un message ICMP Annonce de routeur (paragraphe 2.1). Un message Sollicitation d'agent est identique à une sollicitation de routeur ICMP, sauf que sa durée de vie IP (TTL, *Time to Live*) DOIT être réglée à 1 (paragraphe 2.2). Cette section décrit les formats de messages et les procédures par lesquelles les nœuds mobiles, agents étrangers, et agents de rattachement coopèrent pour réaliser la découverte d'agent.

Une annonce d'agent et une sollicitation d'agent peuvent n'être pas nécessaires pour les couches de liaison qui fournissent déjà cette fonctionnalité. La méthode par laquelle les nœuds mobiles établissent les connexions de couche de liaison avec les futurs agents sort du domaine d'application du présent document (mais voir l'Appendice A). Les procédures décrites ci-dessous supposent qu'une telle connexité de couche de liaison a déjà été établie.

Aucune authentification n'est requise pour les messages d'annonce d'agent et de sollicitation d'agent. Ils PEUVENT être authentifiés en utilisant l'en-tête d'authentification IP [RFC4302], qui n'est pas en relation avec les messages décrits dans le présent document. Une spécification plus poussée de la façon dont les messages d'annonce et de sollicitation peuvent être authentifiés sort du domaine d'application du présent document.

### 2.1 Annonce d'agent

Les annonces d'agent sont transmises par un agent de mobilité pour annoncer ses services sur une liaison. Les nœuds mobiles utilisent ces annonces pour déterminer leur point de rattachement actuel à l'Internet. Une annonce d'agent est une annonce de routeur ICMP qui a été étendue pour porter aussi une extension d'annonce d'agent de mobilité (paragraphe 2.1.1) et, facultativement, une extension Longueurs de préfixes (paragraphe 2.1.2) une extension Bourrage d'un octet (paragraphe 2.1.3), ou d'autres extensions qui pourront être définies à l'avenir.

Dans un message d'annonce d'agent, les champs d'annonce de routeur ICMP du message doivent se conformer aux spécifications supplémentaires suivantes :

- Champs de couche de liaison

adresse de destination : l'adresse de destination de couche de liaison d'une annonce d'agent en envoi individuel DOIT être la même que l'adresse de source de couche de liaison de la sollicitation d'agent qui a provoqué l'annonce.

- Champs IP

TTL : le TTL pour toutes les annonces d'agent DOIT être réglé à 1.
Adresse de destination : comme spécifié pour la découverte de routeur ICMP [RFC1256], l'adresse de destination IP d'une annonce d'agent en diffusion groupée DOIT être soit l'adresse de diffusion groupée "Tous les systèmes sur cette liaison" (224.0.0.1) [RFC1112] soit l'adresse de "diffusion limitée" (255.255.255.255). L'adresse de diffusion dirigée sur le sous réseau de forme <préfixe>.<-1> ne peut pas être utilisée car les nœuds mobiles ne vont généralement pas connaître le préfixe du réseau étranger. Quand l'annonce d'agent est en envoi individuel pour un nœud mobile, l'adresse IP de rattachement du nœud mobile DEVRAIT être utilisée comme adresse de destination.

- Champs ICMP

Code : le champ Code de l'annonce d'agent est interprété comme suit :

0 L'agent de mobilité traite le trafic commun -- c'est-à-dire, il agit comme un routeur pour les datagrammes IP non nécessairement en rapport avec les nœuds mobiles.

16 L'agent de mobilité n'achemine pas le trafic commun. Cependant, tous les agents étrangers DOIVENT (au minimum) transmettre à un routeur par défaut tous les datagrammes reçus d'un nœud mobile enregistré (paragraphe 4.2.2).

Durée de vie : durée maximum pendant laquelle l'annonce est considérée valide en l'absence d'autres annonces.

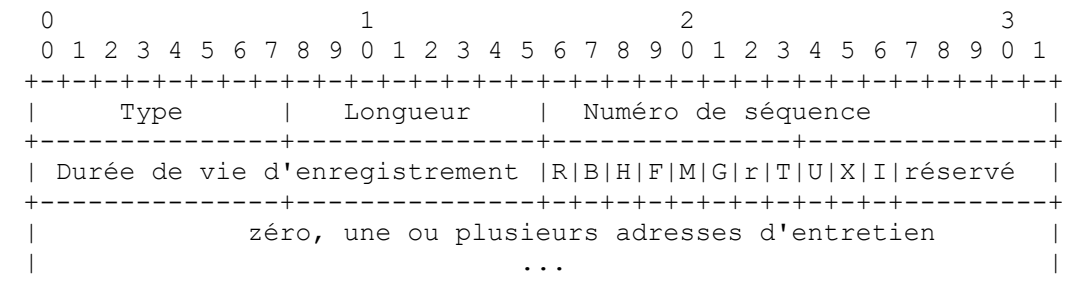
Adresses de routeur : Voir au paragraphe 2.3.1 la discussion des adresses qui peuvent apparaître dans cette portion de l'annonce d'agent.

Nombre d'adresses : nombre des adresses de routeur annoncées dans ce message. Noter que dans un message d'annonce d'agent, le nombre des adresses de routeur spécifiées dans la portion Annonce de routeur ICMP du message PEUT être réglé à 0. Voir les détails au paragraphe 2.3.1.

Si elles sont périodiques, l'intervalle nominal auquel les annonces d'agent sont envoyées DEVRAIT n'être pas supérieur à un tiers de la durée de vie de l'annonce donnée dans l'en-tête ICMP. Cet intervalle PEUT être plus court que 1/3 de la durée de vie annoncée. Cela permet à un nœud mobile de manquer trois annonces successives avant de supprimer l'agent de la liste des agents valides. Le temps réel de transmission pour chaque annonce DEVRAIT être légèrement aléatoire [RFC1256] afin d'éviter la synchronisation et les collisions qui en découlent avec d'autres annonces d'agent qui peuvent être envoyées par d'autres agents (ou avec d'autres annonces de routeur envoyées par d'autres routeurs). Noter que ce champ n'a pas de relation avec le champ "Durée de vie d'enregistrement" au sein de l'extension Annonce d'agent de mobilité définie ci-dessous.

### 2.1.1 Extension Annonce d'agent de mobilité

L'extension Annonce d'agent de mobilité suit les champs d'annonce de routeur ICMP. Elle est utilisée pour indiquer qu'un message ICMP Annonce de routeur est aussi une annonce d'agent qui est envoyée par un agent de mobilité. L'extension Annonce d'agent de mobilité est définie comme suit :




Type : 16

Longueur (6 + 4*N) où 6 compte pour le nombre d'octets dans les champs Numéro de séquence, Durée de vie d'enregistrement, les fanions, et les bits réservés, et N est le nombre d'adresses d'entretien annoncées.

Numéro de séquence : compte des messages d'annonce d'agent envoyés depuis l'initialisation de l'agent (paragraphe 2.3.2).

Durée de vie d'enregistrement : plus longue durée de vie (mesurée en secondes) que cet agent veut accepter dans toute demande d'enregistrement. Une valeur de 0xffff indique l'infini. Ce champ n'a pas de relation avec le champ "Durée de vie" au sein de la portion Annonce de routeur ICMP de l'annonce d'agent.

R : Enregistrement exigé. L'enregistrement auprès de cet agent étranger (ou un autre agent étranger sur cette liaison) est exigé même quand on utilise une adresse d'entretien colocalisée.

B : Occupé : l'agent étranger ne va pas accepter l'enregistrement de nœuds mobiles supplémentaires.

H : agent de rattachement. Cet agent offre des services comme agent de rattachement sur la liaison sur laquelle est envoyé ce message d'annonce d'agent.

F : agent étranger. Cet agent offre des services d'agent étranger sur la liaison sur laquelle ce message d'annonce d'agent est envoyé.

M : encapsulation minimale. Cet agent met en œuvre la réception de datagrammes tunnelés qui utilisent l'encapsulation minimale [RFC2004].

G : encapsulation d'acheminement générique (GRE, *Generic Routing Encapsulation*). Cet agent met en œuvre la réception de datagrammes tunnelés qui utilisent la GRE [RFC2784].

r : envoyé à zéro; ignoré à réception. NE DEVRAIT PAS être alloué pour un autre usage.

T : l'agent étranger prend en charge le tunnelage inverse comme spécifié dans la [RFC3024].

U : l'agent de mobilité prend en charge le tunnelage UDP comme spécifié dans la [RFC3519].

X : l'agent de mobilité prend en charge la révocation d'enregistrement comme spécifié dans la [RFC3543].

I : l'agent étranger prend en charge l'enregistrement régional comme spécifié dans la [RFC4857].

réservé : envoyé à zéro, ignoré à réception.

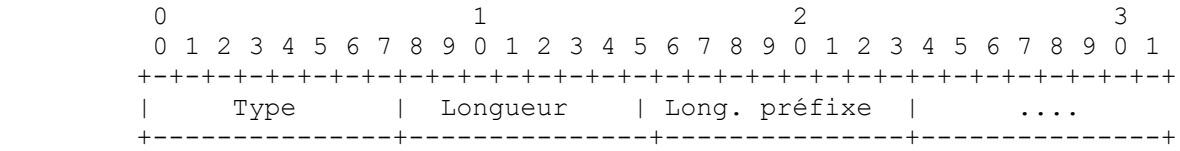
Adresses d'entretien : la ou les adresses d'entretien annoncées d'agent étranger fournies par cet agent étranger. Une annonce d'agent DOIT inclure au moins une adresse d'entretien si le bit "F" est établi. Le nombre d'adresses d'entretien présentes est déterminé par le champ Longueur dans l'extension.

Un agent de rattachement DOIT toujours être prêt à servir les nœuds mobiles pour lesquels il est l'agent de rattachement. Un agent étranger peut parfois être trop occupé pour servir des nœuds mobiles supplémentaires ; même ainsi, il doit continuer d'envoyer des annonces d'agent, afin que tous les nœuds mobiles déjà enregistrés auprès de lui sachent qu'il ne sont pas passés hors de portée de l'agent étranger et que l'agent étranger n'est pas défaillant. Un agent étranger peut indiquer en établissant le bit "B" dans ses annonces d'agent qu'il est "trop occupé" pour permettre l'enregistrement de nouveaux nœuds mobiles. Un message Annonce d'agent NE DOIT PAS avoir le bit "B" établi si le bit "F" n'est pas aussi établi. De plus, au moins un des bits "F" et "H" DOIT être établi dans tout message d'annonce d'agent envoyé.

Quand un agent étranger souhaite exiger l'enregistrement même des nœuds mobiles qui ont acquis une adresse d'entretien colocalisée, il établit le bit "R" à un. Comme ce bit ne s'applique qu'aux agents étrangers, un agent NE DOIT établir le bit "R" à un que si le le bit 'F' est aussi réglé à un.

### 2.1.2 Extension Longueurs de préfixe

L'extension Longueurs de préfixe PEUT suivre l'extension Annonce d'agent de mobilité. Elle est utilisée pour indiquer le nombre de bits de préfixe de réseau qui s'appliquent à chaque adresse de routeur de la liste de la portion Annonce de routeur ICMP de l'annonce d'agent. Noter que les longueurs de préfixe données NE S'APPLIQUENT PAS à la ou aux adresses d'entretien de la liste de l'extension Annonce d'agent de mobilité. L'extension Longueurs de préfixe est définie comme suit :




Type : 19 (extension Longueurs de préfixe)

Longueur : N, où N est la valeur (éventuellement zéro) du champ Nombre d'adresses dans la portion Annonce de routeur ICMP de l'annonce d'agent.

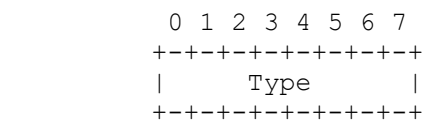
Longueurs de préfixe : nombre de bits de tête qui définissent le numéro de réseau de l'adresse de routeur correspondante sur la liste de la portion Annonce de routeur ICMP du message. La longueur de préfixe pour chaque adresse de routeur est codée comme un octet séparé, afin que les adresses de routeur figurent sur la liste de la portion Annonce de routeur ICMP du message.

Voir au paragraphe 2.4.2 des informations sur comment l'extension Longueurs de préfixe PEUT être utilisée par un nœud mobile lorsque il détermine si il s'est déplacé. Voir l'Appendice D pour les détails de mise en œuvre de l'utilisation de cette extension.

### 2.1.3 Extension Bourrage d'un octet

Certaines mises en œuvre de IP insistent pour bourrer les messages ICMP jusqu'à un nombre pair d'octets. Si la longueur ICMP d'une annonce d'agent est impaire, cette extension PEUT être incluse afin de rendre paire la longueur ICMP. Noter que cette extension N'EST PAS destinée à être une extension générale à inclure pour aligner sur le mot ou sur une certaine longueur les divers champs de l'annonce d'agent. Une annonce d'agent NE DEVRAIT PAS inclure plus d'une extension Bourrage d'un octet et si elle est présente, cette extension DEVRAIT être la dernière extension de l'annonce d'agent.

Noter que, à la différence des autres extensions utilisées dans IP mobile, l'extension Bourrage d'un octet est codée sur un seul octet, sans champ Longueur ni Données. L'extension Bourrage d'un octet est définie comme suit :




Type : 0 (extension Bourrage d'un octet)

## 2.2 Sollicitation d'agent

Une sollicitation d'agent est identique à une sollicitation de routeur ICMP avec la restriction que le champ TTL IP DOIT être réglé à 1.

## 2.3 Considérations d'agent étranger et d'agent de rattachement

Tout agent de mobilité qui ne peut pas être découvert par un protocole de couche de liaison DOIT envoyer des annonces d'agent. Un agent qui peut être découvert par un protocole de couche de liaison DEVRAIT aussi mettre en œuvre les annonces d'agent.

Cependant, les annonces n'ont pas besoin d'être envoyées, sauf quand la politique du site exige l'enregistrement auprès de l'agent (c'est-à-dire, quand le bit "R" est établi) ou comme réponse à une sollicitation d'agent spécifique. Tous les agents de mobilité DOIVENT traiter les paquets qui sont reçus adressés au groupe de diffusion groupée des agents mobiles, à l'adresse 224.0.0.11. Un nœud mobile PEUT envoyer une sollicitation d'agent au 224.0.0.11. Tous les agents de mobilité DEVRAIENT répondre aux sollicitations d'agents.

Les mêmes procédures, valeurs par défauts, et constantes sont utilisées dans les messages d'annonce d'agent et les messages de sollicitation d'agent comme spécifié pour la découverte de routeur ICMP [RFC1256], avec les exceptions que :

- o un agent de mobilité DOIT limiter le taux d'envoi des annonces d'agent en diffusion ou diffusion groupée ; le taux maximum DEVRAIT être choisi de telle sorte que les annonces ne consomment pas une quantité significative de la bande passante du réseau, ET
- o un agent de mobilité qui reçoit une sollicitation de routeur NE DOIT PAS exiger que l'adresse IP de source soit l'adresse d'un voisin (c'est-à-dire, une adresse qui correspond à une des propres adresses du routeur sur l'interface d'arrivée, sous le gabarit de sous réseau associé à cette adresse du routeur).
- o un agent de mobilité PEUT être configuré à n'envoyer des annonces d'agent qu'en réponse à un message de sollicitation d'agent.

Si le réseau de rattachement n'est pas un réseau virtuel, l'agent de rattachement pour tout nœud mobile DEVRAIT alors être situé sur la liaison identifiée par l'adresse de rattachement du nœud mobile, et les messages d'annonce d'agent envoyés par l'agent de rattachement sur cette liaison DOIVENT avoir le bit "'H" établi. De cette façon, les nœuds mobiles sur leur propre réseau de rattachement vont être capables de déterminer qu'ils sont bien chez eux. Tous les messages d'annonce d'agent envoyés par l'agent de rattachement sur une autre liaison à laquelle il peut être rattaché (si il est un agent de mobilité servant plus d'une liaison) NE DOIVENT PAS avoir le bit "H" établi sauf si l'agent de rattachement sert aussi comme agent de rattachement (pour d'autres nœuds mobiles) sur cette autre liaison. Un agent de mobilité PEUT utiliser des réglages différents pour chaque bit "R", "H", et "F" sur ses différentes interfaces réseau.

Si le réseau de rattachement est un réseau virtuel, le réseau de rattachement n'a pas de réalisation physique externe à l'agent de rattachement lui-même. Dans ce cas, il n'y a pas de liaison réseau physique sur laquelle envoyer les messages d'annonce d'agent annonçant l'agent de rattachement. Les nœuds mobiles pour lesquels c'est le réseau de rattachement sont toujours traités comme étant hors de chez eux.

Sur un réseau particulier, soit tous les agents de mobilité DOIVENT inclure l'extension Longueurs de préfixes, soit tous NE DOIVENT PAS inclure cette extension. De façon équivalente, il est interdit à certains agents sur un certain sous réseau

d'inclure l'extension mais pour d'autres de ne pas l'inclure. Autrement, un des algorithmes de détection de mouvement conçus pour les nœuds mobiles ne va pas fonctionner correctement (paragraphe 2.4.2).

### 2.3.1 Adresses de routeur annoncées

La portion annonce de routeur ICMP de l'annonce d'agent PEUT contenir une ou plusieurs adresses de routeur. Un agent DEVRAIT seulement mettre ses propres adresses, si il en est, dans l'annonce. Que sa propre adresse apparaisse ou non dans les adresses de routeur, un agent étranger DOIT acheminer les datagrammes qu'il reçoit des nœuds mobiles enregistrés (paragraphe 3.7).

### 2.3.2 Traitement des numéros de séquence et de leur retour à zéro

Le numéro de séquence dans les annonces d'agent va de 0 à 0xffff. Après l'amorçage, un agent DOIT utiliser le numéro 0 pour sa première annonce. Chaque annonce suivante DOIT utiliser le numéro de séquence supérieur de un, à l'exception du numéro de séquence 0xffff qui DOIT être suivi par le numéro de séquence 256. De cette façon, les nœuds mobiles peuvent distinguer une réduction du numéro de séquence qui se produit après un réamorçage d'une réduction qui résulte d'un retour à zéro du numéro de séquence après qu'il a atteint la valeur de 0xffff.

## 2.4 Considérations de nœud mobile

Chaque nœud mobile DOIT mettre en œuvre la sollicitation d'agent. Les sollicitations DEVRAIENT seulement être envoyées en l'absence d'annonces d'agent et quand une adresse d'entretien n'a pas été déterminée par un protocole de couche de liaison ou d'autres moyens. Le nœud mobile utilise les mêmes procédures, valeurs par défaut, et constantes pour la sollicitation d'agent que spécifié pour les messages ICMP de sollicitation de routeur [RFC1256], sauf que le nœud mobile PEUT solliciter plus souvent qu'une seule fois toutes les trois secondes, et qu'un nœud mobile qui n'est actuellement pas connecté à un agent étranger PEUT solliciter plus que MAX_SOLICITATIONS.

Le taux auquel un nœud mobile envoie des sollicitations DOIT être limité par le nœud mobile. Le nœud mobile PEUT envoyer trois sollicitations initiales au taux maximum d'une par seconde lorsque il cherche un agent. Après cela, le taux d'envoi des sollicitations DOIT être réduit afin de limiter les frais généraux sur la liaison locale. Les sollicitations suivantes DOIVENT être envoyées en utilisant un mécanisme de retard binaire exponentiel, doublant l'intervalle entre les sollicitations consécutives, jusqu'à l'intervalle maximum. L'intervalle maximum DEVRAIT être choisi de façon appropriée sur la base des caractéristiques du support sur lequel le nœud mobile sollicite. Cet intervalle maximum DEVRAIT être au moins d'une minute entre les sollicitations.

Lorsque il est encore en train de chercher un agent, le nœud mobile NE DOIT PAS augmenter son taux d'envoi de sollicitations sauf si il a reçu une indication positive de son déplacement sur une nouvelle liaison. Après s'être enregistré avec succès auprès d'un agent, le nœud mobile DEVRAIT aussi augmenter le taux auquel il envoie les sollicitations quand il recommence à chercher un nouvel agent auprès duquel s'enregistrer. Le taux augmenté de sollicitation PEUT revenir au taux maximum, mais il DOIT alors être limité de la manière décrite ci-dessus. Dans tous les cas, les intervalles recommandés de sollicitation sont des valeurs nominales. Les nœuds mobiles DOIVENT rendre aléatoires leurs temps de sollicitation autour de ces valeurs nominales comme spécifié pour la découverte de routeur ICMP [RFC1256].

Les nœuds mobiles DOIVENT traiter les annonces d'agent reçues. Un nœud mobile peut distinguer un message d'annonce d'agent des autres utilisations du message ICMP Annonce de routeur en examinant le nombre d'adresses annoncées et le champ Longueur IP totale. Quand la longueur IP totale indique que le message ICMP est plus long que nécessaire pour le nombre d'adresses annoncées, les données restantes sont interprétées comme une ou plusieurs extensions. La présence d'une extension Annonce d'agent de mobilité identifie l'annonce comme une annonce d'agent.

Si il y a plus d'une adresse annoncée, le nœud mobile DEVRAIT prendre la première adresse pour sa tentative initiale d'enregistrement. Si la tentative d'enregistrement échoue avec un code d'état qui indique le rejet par l'agent étranger, le nœud mobile PEUT réessayer la tentative avec chacune des adresses annoncées tour à tour.

Lorsque plusieurs méthodes de découverte d'agent sont utilisées, le nœud mobile DEVRAIT d'abord tenter l'enregistrement avec les agents qui incluent l'extension Annonce d'agent de mobilité dans leur annonce, de préférence à ceux découverts par d'autres moyens. Cette préférence maximise la probabilité que l'enregistrement soit reconnu, minimisant par là le nombre de tentatives d'enregistrement.

Un nœud mobile DOIT ignorer les bits réservés dans les annonces d'agent, plutôt que d'éliminer de telles annonces. De cette façon, de nouveaux bits pourront être définis à l'avenir, sans affecter la capacité des nœuds mobiles à utiliser les annonces même quand les nouveaux bits définis ne sont pas compris.

### 2.4.1 Enregistrement exigé

Quand le nœud mobile reçoit une annonce d'agent avec le bit "R" établi, le nœud mobile DEVRAIT s'enregistrer par l'agent étranger, même quand le nœud mobile pourrait être capable d'acquérir sa propre adresse d'entretien colocalisée. Cette caractéristique est destinée à permettre aux sites d'appliquer les politiques de visite (comme la comptabilité) qui exigent des échanges d'autorisation.

Si des bits anciennement réservés exigent une forme de surveillance/mise en application sur la liaison étrangère, les agents étrangers qui mettent en œuvre la nouvelle spécification pour les bits anciennement réservés peuvent établir le bit "R". Ceci a pour effet de forcer le nœud mobile à s'enregistrer à travers l'agent étranger, afin que l'agent étranger puisse alors surveiller/mettre en application la politique.

### 2.4.2 Détection de mouvement

Deux mécanismes principaux sont fournis pour que les nœuds mobiles détectent quand ils se sont déplacés d'un sous réseau à un autre. D'autres mécanismes PEUVENT aussi être utilisés. Quand le nœud mobile détecte qu'il a bougé, il DEVRAIT s'enregistrer (Section 3) avec une adresse d'entretien convenable sur le nouveau réseau étranger. Cependant, le nœud mobile NE DOIT PAS s'enregistrer plus fréquemment qu'une fois par seconde en moyenne, comme spécifié au paragraphe 3.6.3.

#### 2.4.2.1 Algorithme 1

La première méthode de détection de mouvement est fondée sur le champ Durée de vie au sein du corps principal de la portion Annonce de routeur ICMP de l'annonce d'agent. Un nœud mobile DEVRAIT enregistrer la durée de vie reçue dans toutes les annonces d'agent, jusqu'à ce que cette durée de vie arrive à expiration. Si le nœud mobile échoue a recevoir une autre annonce du même agent pendant la durée de vie spécifiée, il DEVRAIT supposer qu'il a perdu le contact avec cet agent. Si le nœud mobile a précédemment reçu une annonce d'agent d'un autre agent pour lequel le champ Durée de vie n'est pas encore expiré, le nœud mobile PEUT immédiatement tenter de s'enregistrer avec cet autre agent. Autrement, le nœud mobile DEVRAIT tenter de découvrir un nouvel agent auprès duquel s'enregistrer.

#### 2.4.2.2 Algorithme 2

La seconde méthode utilise les préfixes de réseau. L'extension Longueurs de préfixe PEUT être utilisée dans certains cas par un nœud mobile pour déterminer si une nouvelle annonce d'agent a été reçue ou non sur le même sous réseau que l'adresse d'entretien actuelle du nœud mobile. Si les préfixes diffèrent, le nœud mobile PEUT supposer qu'il a bougé. Si un nœud mobile utilise actuellement l'adresse d'entretien d'un agent étranger, le nœud mobile NE DEVRAIT PAS utiliser cette méthode de détection de mouvement à moins que l'agent actuel et le nouvel agent incluent tous deux l'extension Longueurs de préfixe dans leurs annonces d'agent respectives ; si cette extension manque dans l'une des annonces ou les deux, cette méthode de détection de mouvement NE DEVRAIT PAS être utilisée. De même, si un nœud mobile utilise une adresse d'entretien colocalisée, il NE DEVRAIT PAS utiliser cette méthode de détection de mouvement sauf si le nouvel agent inclut l'extension Longueurs de préfixe dans son annonce et si le nœud mobile connaît le préfixe de réseau de son adresse d'entretien colocalisée actuelle. À l'expiration de son enregistrement actuel, si cette méthode indique que le nœud mobile a bougé, plutôt que de se réenregistrer avec son adresse d'entretien actuelle, un nœud mobile PEUT choisir de s'enregistrer plutôt avec l'agent étranger qui envoie la nouvelle annonce avec le préfixe de réseau différent. L'annonce d'agent sur laquelle se fonde le nouvel enregistrement NE DOIT PAS avoir expiré selon son champ Durée de vie.

### 2.4.3 Retour au domaine de rattachement

Un nœud mobile peut détecter qu'il est retourné à son réseau de rattachement quand il reçoit une annonce d'agent de son propre agent de rattachement. Si il en est ainsi, il DEVRAIT se désenregistrer de son agent de rattachement (Section 3). Avant de tenter de se désenregistrer, le nœud mobile DEVRAIT configurer son tableau d'acheminement de façon appropriée pour son réseau de rattachement (paragraphe 4.2.1). De plus, si le réseau de rattachement utilise l'ARP [RFC0826], le nœud mobile DOIT suivre les procédures décrites au paragraphe 4.6 concernant l'ARP, l'ARP mandataire, et l'ARP gratuit.

### 2.4.4 Traitement des numéros de séquence et de leur retour à zéro

Si un nœud mobile détecte deux valeurs successives de numéro de séquence dans les annonces d'agent provenant de l'agent étranger auprès duquel il est enregistré, dont le second est inférieur au premier et dans la gamme de 0 à 255, le nœud mobile DEVRAIT s'enregistrer à nouveau. Si la seconde valeur est inférieure à la première mais est supérieure ou égale à 256, le nœud mobile DEVRAIT supposer que le numéro de séquence est revenu à zéro après être passé par sa valeur maximum (0xffff) et que le réenregistrement n'est pas nécessaire (paragraphe 2.3).

# 3. Enregistrement

L'enregistrement IP mobile fournit un mécanisme souple pour que les nœuds mobiles communiquent leurs informations d'accessibilité actuelles à leur agent de rattachement. C'est la méthode par laquelle les nœuds mobiles :
- o demandent des services de transmission quand ils visitent un réseau étranger,
- o informent leur agent de rattachement de leur adresse d'entretien actuelle,
- o renouvellent un enregistrement qui va arriver à expiration, et/ou
- o se désenregistrent quand ils retournent chez eux.

Les messages d'enregistrement échangent des informations entre un nœud mobile, (facultativement) un agent étranger, et l'agent de rattachement. L'enregistrement crée ou modifie un lien de mobilité chez l'agent de rattachement, associant l'adresse de rattachement du nœud mobile à son adresse d'entretien pour la durée de vie spécifiée.

Plusieurs autres capacités (facultatives) sont disponibles par la procédure d'enregistrement, qui permettent à un nœud mobile de :
- o découvrir son adresse de rattachement, si le nœud mobile n'est pas configuré avec cette information,
- o maintenir plusieurs enregistrements simultanés, afin qu'une copie de chaque datagramme soit tunnelée à chaque adresse d'entretien active,
- o désenregistrer des adresses d'entretien spécifiques tout en conservant d'autres liens de mobilité, et
- o découvrir l'adresse d'un agent de rattachement si le nœud mobile n'est pas configuré avec cette information.

## 3.1 Généralités sur l'enregistrement

IP mobile définit deux procédures d'enregistrement différentes, une via un agent étranger qui relaie l'enregistrement à l'agent de rattachement du nœud mobile, et une directement avec l'agent de rattachement du nœud mobile. Les règles suivantes déterminent laquelle de ces deux procédures d'enregistrement utiliser dans toute circonstance particulière :

- o Si un nœud mobile enregistre une adresse d'entretien d'agent étranger, le nœud mobile DOIT s'enregistrer via cet agent étranger.

- o Si un nœud mobile utilise une adresse d'entretien colocalisée, et reçoit une annonce d'agent d'un agent étranger sur la liaison sur laquelle il utilise cette adresse d'entretien, le nœud mobile DEVRAIT s'enregistrer via cet agent étranger (ou via un autre agent étranger sur cette liaison) si le bit "R" est établi dans le message d'annonce d'agent reçu.

- o Si autrement un nœud mobile utilise une adresse d'entretien colocalisée, le nœud mobile DOIT s'enregistrer directement auprès de son agent de rattachement.

- o Si un nœud mobile est retourné à son réseau de rattachement et s'enregistre (se désenregistre) auprès de son agent de rattachement, le nœud mobile DOIT s'enregistrer directement auprès de son agent de rattachement.

Les deux procédures d'enregistrement impliquent l'échange de messages Demande d'enregistrement et Réponse d'enregistrement (paragraphe 3.3 et paragraphe 3.4). Quand l'enregistrement est via un agent étranger, la procédure d'enregistrement exige les quatre messages suivants :
a. Le nœud mobile envoie une demande d'enregistrement au futur agent étranger pour commencer le processus d'enregistrement.
b. L'agent étranger traite la demande d'enregistrement et la relaie à l'agent de rattachement.
c. L'agent de rattachement envoie une réponse d'enregistrement à l'agent étranger pour accorder ou refuser la demande.
d. L'agent étranger traite la réponse d'enregistrement et la relaie ensuite au nœud mobile pour l'informer de la disposition de sa demande.

Quand le nœud mobile s'enregistre directement auprès de son agent de rattachement, la procédure d'enregistrement exige seulement les deux messages suivants :
a. Le nœud mobile envoie une demande d'enregistrement à l'agent de rattachement.
b. L'agent de rattachement envoie une réponse d'enregistrement au nœud mobile, accordant ou refusant la demande.

Les messages d'enregistrement définis aux paragraphes 3.3 et 3.4 utilisent le protocole de datagramme d'utilisateur (UDP, *User Datagram Protocol*) [RFC0768]. Une somme de contrôle UDP non zéro DEVRAIT être incluse dans l'en-tête, et DOIT être vérifiée par le receveur. Une somme de contrôle UDP de zéro DEVRAIT être acceptée par le receveur. Le comportement du nœud mobile et de l'agent de rattachement à l'égard de leur acceptation mutuelle de paquets avec des

sommes de contrôle UDP de zéro DEVRAIT être définie au titre de l'association de sécurité de mobilité qui existe entre eux.

### 3.2 Authentification

Chaque nœud mobile, agent étranger, et agent de rattachement DOIT être capable de prendre en charge une association de sécurité de mobilité pour les entités mobiles, indexée par leur SPI et leur adresse IP. Dans le cas du nœud mobile, ce doit être son adresse de rattachement. Voir au paragraphe 5.1 les exigences pour la prise en charge des algorithmes d'authentification. Les messages d'enregistrement entre un nœud mobile et son agent de rattachement DOIVENT être authentifiés avec une extension d'activation d'autorisation, par exemple, l'extension Authentification mobile-rattachement (paragraphe 3.5.2). Cette extension DOIT être la première extension d'authentification ; d'autres extensions spécifiques de l'agent étranger PEUVENT être ajoutées au message après que le nœud mobile a calculé l'authentification.

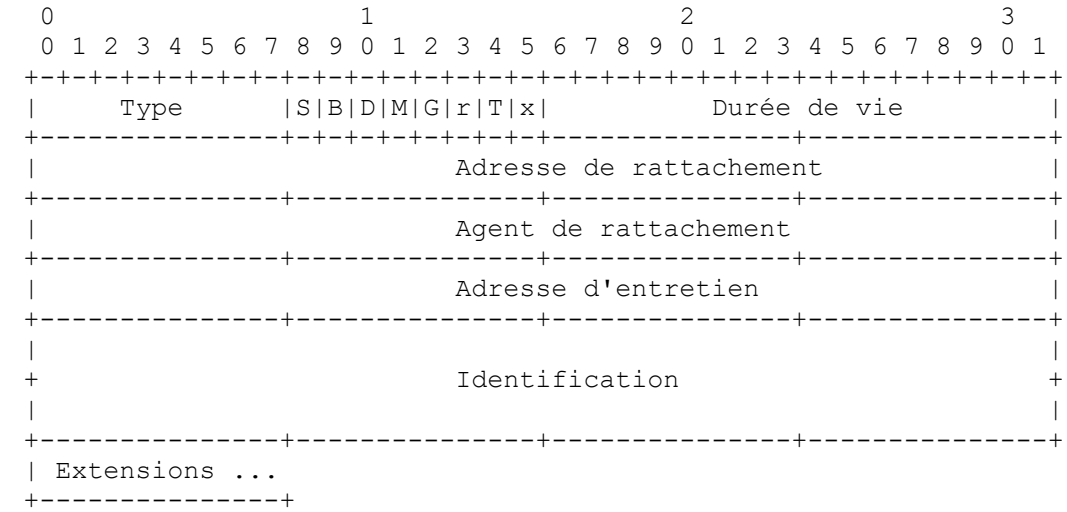
### 3.3 Demande d'enregistrement

Un nœud mobile s'enregistre auprès de son agent de rattachement en utilisant un message Demande d'enregistrement afin que son agent de rattachement puisse créer ou modifier un lien de mobilité pour ce nœud mobile (par exemple, avec une nouvelle durée de vie). La demande peut être relayée à l'agent de rattachement par l'agent étranger à travers lequel le nœud mobile s'est enregistré, ou elle peut être envoyée directement à l'agent de rattachement dans le cas où le nœud mobile s'est enregistré à une adresse d'entretien colocalisée.

Champs IP :
Adresse de source : normalement l'adresse de l'interface par laquelle le message est envoyé.
Adresse de destination : normalement celle de l'agent étranger ou de l'agent de rattachement. Voir les détails aux paragraphes 3.6.1.1 et 3.7.2.2.

Champs UDP :
Accès de source : variable
Accès de destination : 434

L'en-tête UDP est suivi par les champs IP mobile montrés ci-dessous :




Type : 1 (Demande d'enregistrement)

S : liens simultanés. Si le bit "S" est établi, le nœud mobile demande que l'agent de rattachement conserve ses liens de mobilité antérieurs, comme décrit au paragraphe 3.6.1.2.

B : datagrammes en diffusion. Si le bit "B" est établi, le nœud mobile demande que l'agent de rattachement lui tunnelle tous les datagrammes en diffusion qu'il reçoit sur le réseau de rattachement, comme décrit au paragraphe 4.3.

D : Désencapsulation par le nœud mobile. Si le bit "D" est établi, le nœud mobile va lui-même désencapsuler les datagrammes qui sont envoyés à l'adresse d'entretien. C'est-à-dire que le nœud mobile utilise une adresse d'entretien colocalisée.

M : encapsulation minimale. Si le bit "M" est établi, le nœud mobile demande que son agent de rattachement utilise l'encapsulation minimale [RFC2004] pour les datagrammes tunnelés au nœud mobile.

G : encapsulation GRE. Si le bit "G" est établi, le nœud mobile demande que son agent de rattachement utilise l'encapsulation GRE [RFC2784] pour les datagrammes tunnelés au nœud mobile.

r : envoyé à zéro; ignoré à réception. NE DEVRAIT être alloué pour aucune autre utilisation.

T : tunnelage inverse demandé; voir la [RFC3024].

x : envoyé à zéro; ignoré à réception.

Durée de vie : nombre de secondes restantes avant que l'enregistrement soit considéré comme expiré. Une valeur de zéro indique une demande de désenregistrement. Une valeur de 0xffff indique l'infini.

Adresse de rattachement : adresse IP du nœud mobile.

Agent de rattachement : adresse IP de l'agent de rattachement du nœud mobile.

Adresse d'entretien : adresse IP de la fin du tunnel.

Identification : nombre de 64 bits, construit par le nœud mobile, utilisé pour confronter les demandes d'enregistrement aux réponses d'enregistrement, et pour protéger contre les attaques en répétition des messages d'enregistrement. Voir les paragraphes 5.4 et 5.7.

Extensions : la portion fixe de la demande d'enregistrement est suivie par une ou plusieurs des extensions dont la liste figure au paragraphe 3.5. Une extension de capacité d'autorisation DOIT être incluse dans toues les demandes d'enregistrement. Voir aux paragraphes 3.6.1.3 et 3.7.2.2 des informations sur l'ordre relatif dans lequel les différentes extensions, lorsque présentes, DOIVENT être placées dans un message Demande d'enregistrement.

### 3.4 Réponse d'enregistrement

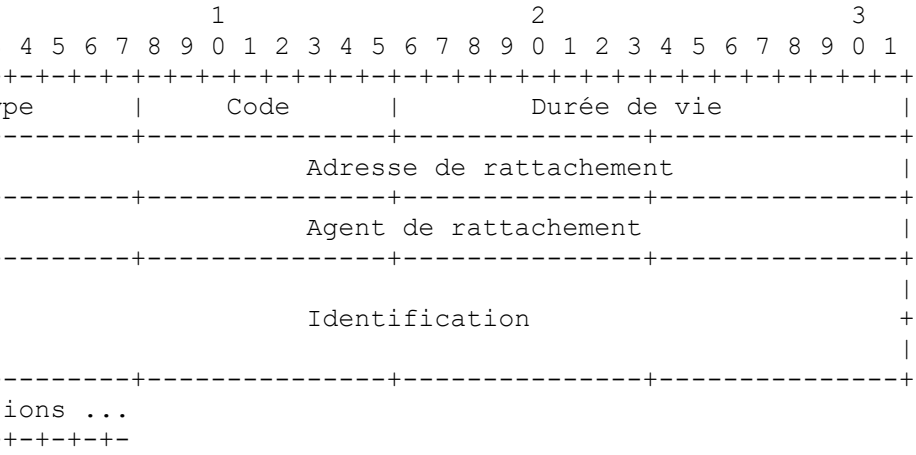
Un agent de mobilité retourne normalement un message de réponse d'enregistrement à un nœud mobile qui a envoyé un message Demande d'enregistrement. Si le nœud mobile demande le service à partir d'un agent étranger, cet agent étranger va normalement recevoir la réponse de l'agent de rattachement et ensuite la relayer au nœud mobile. Les messages de réponse contiennent les codes nécessaires pour informer le nœud mobile sur l'état de sa demande, ainsi que la durée de vie accordée par l'agent de rattachement, qui PEUT être plus petite que dans la demande originale.

L'agent étranger NE DOIT PAS augmenter la durée de vie choisie par le nœud mobile dans la demande d'enregistrement, car la durée de vie est couverte par une extension d'authentification qui active l'autorisation par l'agent de rattachement. Une telle extension contient des données d'authentification qui ne peuvent pas être correctement (re)calculées par l'agent étranger. L'agent de rattachement NE DOIT PAS augmenter la durée de vie choisie par le nœud mobile dans la demande d'enregistrement, car le faire pourrait l'augmenter au delà de la durée de vie maximum d'enregistrement permise par l'agent étranger. Si la durée de vie reçue dans la réponse d'enregistrement est supérieure à celle de la demande d'enregistrement, la durée de vie de la demande DOIT être utilisée. Quand la durée de vie reçue dans la réponse d'enregistrement est inférieure à celle de la demande d'enregistrement, la durée de vie de la réponse DOIT être utilisée.

Champs IP :
Adresse de source : normalement copiée de l'adresse de destination de la demande d'enregistrement à laquelle répond l'agent. Voir les détails complets aux paragraphes 3.7.2.3 et 3.8.3.2.
Adresse de destination : copiée de l'adresse de source de la demande d'enregistrement à laquelle répond l'agent.

Champs UDP :
Accès de source : copiée de l'accès UDP de destination de la demande d'enregistrement correspondante.
Accès de destination : copiée de l'accès de source de la demande d'enregistrement correspondante (paragraphe 3.7.1).

L'en-tête UDP est suivi par les champs IP mobile montrés ci-dessous :




Type : 3 (réponse d'enregistrement)

Code : valeur qui indique le résultat de la demande d'enregistrement. Voir ci-dessous la liste des valeurs de code actuellement définies.

Durée de vie : Si le champ Code indique que l'enregistrement a été accepté, le champ Durée de vie est réglé au nombre de secondes restantes avant que l'enregistrement soit considéré expiré. Une valeur de zéro indique que le nœud mobile n'a pas été désenregistré. Une valeur de 0xffff indique l'infini. Si le champ Code indique que l'enregistrement a été refusé, le contenu du champ Durée de vie est inspécifié et DOIT être ignoré à réception.

Adresse de rattachement : adresse IP du nœud mobile.

Agent de rattachement : adresse IP de l'agent de rattachement du nœud mobile.

Identification : nombre de 64 bits utilisé pour confronter les demandes et réponses d'enregistrement, et pour protéger contre les attaques en répétition des messages d'enregistrement. La valeur se fonde sur le champ Identification du message de demande d'enregistrement provenant du nœud mobile, et sur le style de protection contre la répétition utilisé dans le contexte de sécurité entre le nœud mobile et son agent de rattachement (défini par l'association de sécurité mobile entre eux, et la valeur de SPI dans l'extension d'activation d'autorisation). Voir aux paragraphes 5.4 et 5.7.

Extensions : la portion fixe de la réponse d'enregistrement est suivie par une ou plusieurs des extensions mentionnées au paragraphe 3.5. Une extension d'activation d'autorisation DOIT être incluse dans toutes les réponses d'enregistrement retournées par l'agent de rattachement. Voir aux paragraphes 3.7.2.2 et 3.8.3.3 les règles sur le placement des extensions dans les messages de réponse.

Les valeurs suivantes sont définies pour l'usage du champ Code.

Enregistrement réussi :
0 : enregistrement accepté
1 : enregistrement accepté, mais liens de mobilité simultanés non acceptés

Enregistrement refusé par l'agent étranger :
64 : raison non spécifiée
65 : administrativement interdit
66 : ressources insuffisantes
67 : échec de l'authentification du nœud mobile
68 : échec de l'authentification de l'agent de rattachement
69 : durée de vie demandée trop longue
70 : demande mal formée
71 : réponse mal formée
72 : encapsulation demandée indisponible
73 : réservé et indisponible
77 : adresse d'entretien invalide
78 : enregistrement arrivé à expiration
80 : réseau de rattachement injoignable (erreur ICMP reçue)
81 : hôte de l'agent de rattachement injoignable (erreur ICMP reçue)

82 : accès de l'agent de rattachement injoignable (erreur ICMP reçue)
88 : agent de rattachement injoignable (autre erreur ICMP reçue)
116 : adresse d'agent de rattachement invalide

Enregistrement refusé par l'agent de rattachement :
128 : raison non spécifiée
129 : administrativement interdit
130 : ressources insuffisantes
131 : échec de l'authentification du nœud mobile
132 : échec de l'authentification de l'agent étranger
133 : discordance d'identification d'enregistrement
134 : demande mal formée
135 : trop de liens de mobilité simultanés
136 : adresse d'agent de rattachement inconnue
Les valeurs à jour du champ Code sont spécifiées dans la base de données en ligne de l'IANA [IANA].

## 3.5 Extensions d'enregistrement

### 3.5.1 Calcul des valeurs d'extension d'authentification

La valeur d'authentifiant calculée pour chaque extension d'authentification DOIT protéger les champs suivants du message d'enregistrement :
- o la charge utile UDP (c'est-à-dire, les données de la demande d'enregistrement ou de la réponse d'enregistrement),
- o toutes les extensions antérieures dans leur totalité, et
- o le type, la longueur, et le SPI de cette extension.

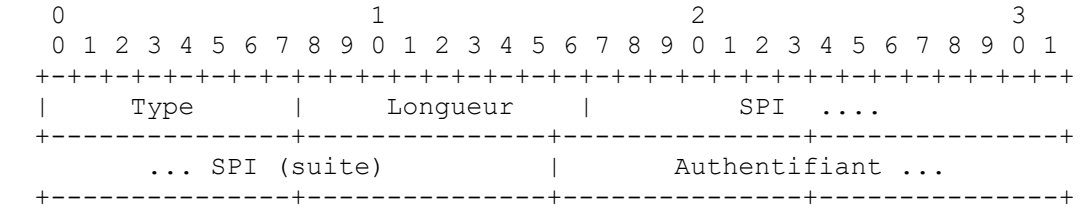
L'algorithme d'authentification par défaut utilise HMAC-MD5 [RFC2104] pour calculer un "résumé de message" de 128 bits du message d'enregistrement. Les données sur lesquelles le HMAC est calculé sont définies comme :
- o la charge utile UDP (c'est-à-dire, les données de la demande d'enregistrement ou de la réponse d'enregistrement),
- o toutes les extensions antérieures dans leur totalité, et
- o le type, la longueur, et le SPI de cette extension.

Noter que le champ Authentifiant lui-même et l'en-tête UDP NE sont PAS inclus dans le calcul de la valeur de l'authentifiant par défaut. Voir au paragraphe 5.1 des informations sur les exigences de prise en charge des codes d'authentification, qui sont à utiliser avec les diverses extensions d'authentification.

L'indice de paramètre de sécurité (SPI, *Security Parameter Index*) au sein de toute extension d'authentification définit le contexte de sécurité qui est utilisé pour calculer la valeur d'authentifiant et qui DOIT être utilisée par le receveur pour vérifier cette valeur. En particulier, le SPI choisit l'algorithme et le mode d'authentification (paragraphe 5.1) et le secret (une clé partagée, ou une paire appropriée de clés publique/privée) utilisé pour calculer l'authentifiant. Afin d'assurer l'interopérabilité entre les différentes mises en œuvre du protocole IP, une mise en œuvre DOIT être capable d'associer toute valeur de SPI à tout algorithme et mode d'authentification qu'elle met en œuvre. De plus, toutes les mises en œuvre de IP mobile DOIVENT mettre en œuvre l'algorithme d'authentification par défaut (HMAC-MD5) spécifié ci-dessus.

### 3.5.2 Extension d'authentification mobile-rattachement

Au moins une extension d'activation d'autorisation DOIT être présente dans toutes les demandes d'enregistrement, et aussi dans toutes les réponses d'enregistrement générées par l'agent de rattachement. L'extension d'authentification mobile-rattachement est toujours une extension d'activation d'autorisation pour les messages d'enregistrement spécifiés dans le présent document. Cette exigence est destinée à éliminer les problèmes [TCPIP] qui résultent de la propagation incontrôlée de redirections à distance dans l'Internet. La localisation de l'extension d'activation d'autorisation marque la fin des données à authentifier par l'agent d'autorisation qui interprète cette extension d'activation d'autorisation.




Type : 32

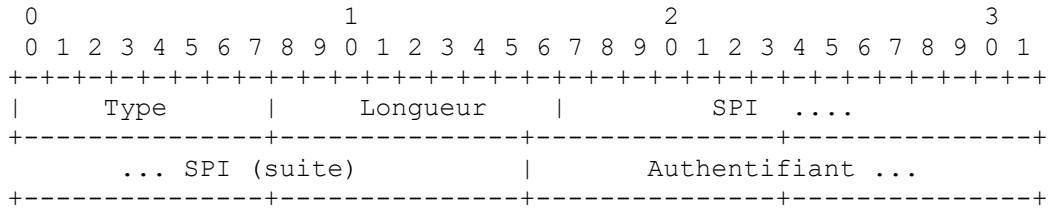
Longueur : 4 plus le nombre d'octets de l'authentifiant.

SPI : 4 octets. Identifiant opaque (voir au paragraphe 1.6).

Authentifiant : longueur variable (voir au paragraphe 3.5.1).

### 3.5.3 Extension d'authentification mobile-étranger

Cette extension PEUT être incluse dans les demandes et réponses d'enregistrement dans les cas où une association de sécurité mobile existe entre le nœud mobile et l'agent étranger. Voir au paragraphe 5.1 des informations sur la prise en charge des exigences pour les codes d'authentification de message.




Type : 33

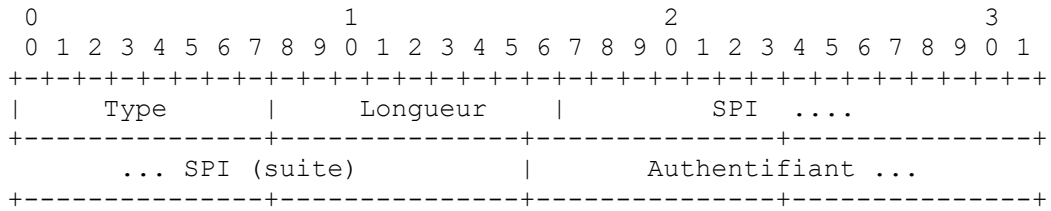
Longueur : 4 plus le nombre d'octets de l'authentifiant.

SPI : 4 octets. Identifiant opaque (voir au paragraphe 1.6).

Authentifiant : longueur variable (voir au paragraphe 3.5.1).

### 3.5.4 Extension d'authentification étranger-rattachement

Cette extension PEUT être incluse dans les demandes et réponses d'enregistrement dans les cas où une association de sécurité mobile existe entre l'agent étranger et l'agent de rattachement, pour autant que la demande d'enregistrement n'est pas un désenregistrement (c'est-à-dire, que le nœud mobile a demandé une durée de vie non zéro et que l'adresse de rattachement est différente de l'adresse d'entretien). L'extension d'authentification étranger-rattachement NE DOIT PAS être appliquée aux messages de désenregistrement. Voir au paragraphe 5.1 les informations sur les exigences de prise en charge des codes d'authentification de message.




Type : 34

Longueur : 4 plus le nombre d'octets de l'authentifiant.

SPI : 4 octets. Identifiant opaque (voir au paragraphe 1.6).

Authentifiant : longueur variable (voir au paragraphe 3.5.1).

Afin d'effectuer l'authentification, l'agent de rattachement et l'agent étranger sont configurés avec une association de sécurité mobile qui est indexée par le SPI (dans l'extension d'authentification étranger-rattachement ajoutée) et l'adresse de source IP de la demande d'enregistrement. Quand l'extension est utilisée avec un message de réponse d'enregistrement, l'adresse de l'agent étranger DOIT être utilisée comme adresse IP de destination dans l'en-tête IP.

Quand cette extension est appliquée à un message Demande d'enregistrement, l'association de sécurité mobile pour vérifier que les données d'authentification sont correctes est choisie par l'agent de rattachement sur la base de la valeur du champ

Adresse IP de source de la demande d'enregistrement et le SPI de l'extension d'authentification. L'adresse IP de source sera la même que celle du champ Adresse d'entretien de la demande d'enregistrement (voir au paragraphe 3.7.2.2).

Quand cette extension est appliquée à un message de réponse d'enregistrement, l'association de sécurité mobile pour vérifier que les données d'authentification sont correctes est choisie par l'agent étranger sur la base de la valeur du champ Adresse d'agent de rattachement de la réponse d'enregistrement.

Si l'adresse d'entretien dans la demande d'enregistrement n'est pas dans l'annonce d'agent, l'agent étranger NE DOIT alors PAS ajouter l'extension Authentification étranger-rattachement quand il relaie le message à l'agent de rattachement. De plus, pour un message de désenregistrement (c'est-à-dire, Durée de vie = 0) l'agent étranger NE DOIT PAS ajouter l'extension Authentification étranger-rattachement quand il relaie le message à l'agent de rattachement. Par conséquent, quand l'agent de rattachement (HA) reçoit une demande de désenregistrement qui ne contient pas une extension Authentification étranger-rattachement, il NE DOIT PAS pour cette raison éliminer la demande au titre du traitement de l'association de sécurité.

### 3.6 Considérations de nœud mobile

Un nœud mobile DOIT être configuré (de façon statique ou dynamique) avec un gabarit de réseau et une association de sécurité mobile pour chacun de ses agents de rattachement. De plus, un nœud mobile PEUT être configuré avec son adresse de rattachement, et l'adresse IP d'un ou plusieurs de ses agents de rattachement ; autrement, le nœud mobile PEUT découvrir un agent de rattachement en utilisant les procédures décrites au paragraphe 3.6.1.2.

Si le nœud mobile n'est pas configuré avec une adresse de rattachement, il PEUT utiliser l'extension Identifiant d'accès réseau (NAI, *Network Access Identifier*) de nœud mobile [RFC2794] pour s'identifier, et régler le champ Adresse de rattachement de la demande d'enregistrement à 0.0.0.0. Dans ce cas, le nœud mobile DOIT être capable d'allouer son adresse de rattachement après avoir extrait ces informations de la réponse d'enregistrement provenant de l'agent de rattachement.

Pour chaque enregistrement en cours, le nœud mobile maintient les informations suivantes :
- o l'adresse de couche de liaison de l'agent étranger auquel a été envoyée la demande d'enregistrement, si applicable,
- o l'adresse IP de destination de la demande d'enregistrement,
- o l'adresse d'entretien utilisée dans l'enregistrement,
- o la valeur d'identification envoyée dans l'enregistrement,
- o la durée de vie demandée à l'origine, et
- o la durée de vie restante de l'enregistrement en cours.

Un nœud mobile DEVRAIT initier un enregistrement chaque fois qu'il détecte un changement de sa connexité au réseau. Voir au paragraphe 2.4.2 les méthodes par lesquelles les nœuds mobiles PEUVENT faire une telle détermination. Quand il est hors de chez lui, la demande d'enregistrement du nœud mobile permet à son agent de rattachement de créer ou modifier pour lui un lien de mobilité. Quand il est chez lui, la demande d'enregistrement (ou désenregistrement) du nœud mobile permet à son agent de rattachement de supprimer tous les liens de mobilité précédents pour lui. Un nœud mobile fonctionne sans le soutien de fonctions de mobilité quand il est chez lui.

Il y a d'autres conditions dans lesquelles le nœud mobile DEVRAIT se (ré)enregistrer auprès de son agent étranger, comme quand le nœud mobile détecte que l'agent étranger a réamorcé (comme spécifié au paragraphe 2.4.4) et quand la durée de vie de l'enregistrement actuel est proche de l'expiration.

En l'absence d'indications à la couche de liaison de changement du point de rattachement, les annonces d'agent provenant de nouveaux agents NE DEVRAIENT PAS causer la tentative par le nœud mobile d'un nouvel enregistrement, si son enregistrement actuel n'a pas expiré et si il reçoit aussi des annonces d'agent de l'agent étranger auprès duquel il est actuellement enregistré. En l'absence d'indications de couche de liaison, un nœud mobile NE DOIT PAS tenter de s'enregistrer plus d'une fois par seconde.

Un nœud mobile PEUT s'enregistrer auprès d'un agent différent quand les protocoles de couche transport indiquent des retransmissions excessives. Un nœud mobile NE DOIT PAS considérer la réception d'une redirection ICMP provenant d'un agent étranger qui lui fournit actuellement le service comme une raison pour s'enregistrer auprès d'un nouvel agent étranger. En respectant ces contraintes, le nœud mobile PEUT se réenregistrer à tout moment.

L'Appendice C montre des exemples de la façon dont les champs dans les messages d'enregistrement vont être réglés dans certains scénarios typiques d'enregistrement.

### 3.6.1 Envoi des demandes d'enregistrement

Les paragraphes qui suivent spécifient les détails des valeurs que le nœud mobile DOIT fournir dans les champs des messages de demande d'enregistrement.

#### 3.6.1.1 Champs IP

On donne ici les règles spécifiques selon lesquelles les nœuds mobiles prennent des valeurs pour les champs d'en-tête IP d'une demande d'enregistrement.

Adresse IP de source :

- Quand il s'enregistre sur un réseau étranger avec une adresse d'entretien colocalisée, l'adresse IP de source DOIT être l'adresse d'entretien.
- Autrement, si le nœud mobile n'a pas une adresse de rattachement, l'adresse IP de source DOIT être 0.0.0.0.
- Dans toutes les autres circonstances, l'adresse IP de source DOIT être l'adresse de rattachement du nœud mobile.

Adresse IP de destination :

- Quand le nœud mobile a découvert l'agent auprès duquel il s'enregistre, par un moyen quelconque (par exemple, la couche de liaison) qui ne fournit pas l'adresse IP de l'agent (l'adresse IP de l'agent n'est pas connue du nœud mobile) alors l'adresse de diffusion groupée "Tous agents de mobilité" (224.0.0.11) DOIT être utilisée. Dans ce cas, le nœud mobile DOIT utiliser l'adresse d'envoi individuel de couche de liaison de l'agent afin de livrer le datagramme à l'agent correct.
- Quand il s'enregistre auprès d'un agent étranger, l'adresse de l'agent telle qu'apprise de l'adresse IP de source de l'annonce d'agent correspondante DOIT être utilisée. Ce PEUT être une adresse qui n'apparaît pas comme une adresse d'entretien annoncée dans l'annonce d'agent. De plus, quand il transmet ce message de demande d'enregistrement, le nœud mobile DOIT utiliser une adresse de destination de couche de liaison copiée de l'adresse de source de couche de liaison du message d'annonce d'agent dans laquelle il a appris l'adresse IP de cet agent étranger.
- Quand le nœud mobile s'enregistre directement auprès de son agent de rattachement et connaît l'adresse IP (d'envoi individuel) de son agent de rattachement, l'adresse de destination DOIT être réglée à cette adresse.
- Si le nœud mobile s'enregistre directement auprès de son agent de rattachement, mais ne connaît pas l'adresse IP de son agent de rattachement, le nœud mobile peut utiliser la résolution dynamique d'adresse d'agent de rattachement pour déterminer automatiquement l'adresse IP de son agent de rattachement (paragraphe 3.6.1.2). Dans ce cas, l'adresse de destination IP est réglée à l'adresse de diffusion dirigée sur le sous réseau du réseau de rattachement du nœud mobile. Cette adresse NE DOIT PAS être utilisée comme adresse de destination IP si le nœud mobile s'enregistre via un agent étranger, bien qu'elle PUISSE être utilisée comme adresse de l'agent de rattachement dans le corps de la demande d'enregistrement quand il s'enregistre via un agent étranger.

Durée de vie IP :

- Le champ TTL IP DOIT être réglé à 1 si l'adresse de destination IP est réglée à l'adresse de diffusion groupée "Tous agents de mobilité" comme décrit ci-dessus. Autrement, une valeur convenable devrait être choisie conformément à la pratique IP standard [RFC0791].

#### 3.6.1.2 Champs de la demande d'enregistrement

On donne ici les règles spécifiques selon lesquelles les nœuds mobiles prennent les valeurs pour les champs dans la portion fixe d'une demande d'enregistrement.

Un nœud mobile PEUT établir le bit "S" afin de demander que l'agent de rattachement conserve un ou des liens de mobilité antérieurs. Autrement, l'agent de rattachement supprime tous les liens antérieurs et les remplace par le nouveau lien spécifié dans la demande d'enregistrement. Plusieurs liens de mobilité simultanés vont probablement être utiles quand un nœud mobile qui utilise au moins une interface réseau sans fil passe au sein d'une gamme de transmission sans fil de plus d'un agent étranger. IP permet explicitement la duplication des datagrammes. Quand l'agent de rattachement permet des liens simultanés, il va tunneler une copie séparée de chaque datagramme arrivant à chaque adresse d'entretien, et le nœud mobile va recevoir plusieurs copies des datagrammes qui lui sont destinés.

Le nœud mobile DEVRAIT établir le bit "D" si il s'enregistre avec une adresse d'entretien colocalisée. Autrement, le bit "D" NE DOIT PAS être établi.

Un nœud mobile PEUT établir le bit "B" pour demander à son agent de rattachement de lui transmettre une copie des datagrammes en diffusion reçus par son agent de rattachement provenant du réseau de rattachement. La méthode utilisée par l'agent de rattachement pour transmettre les datagrammes en diffusion dépend du type d'adresse d'entretien enregistrée par le nœud mobile, comme déterminé par le bit "D" dans la demande d'enregistrement du nœud mobile :

- o Si le bit "D" est établi, le nœud mobile a alors indiqué qu'il va désencapsuler lui-même tous les datagrammes tunnelés à cette adresse d'entretien (le nœud mobile utilise une adresse d'entretien colocalisée). Dans ce cas, pour transmettre un tel datagramme reçu en diffusion au nœud mobile, l'agent de rattachement DOIT le tunneler à cette adresse d'entretien. Le nœud mobile détunnelle le datagramme reçu de la même façon que tout autre datagramme qui lui est directement tunnelé.
- o Si le bit "D" N'EST PAS établi, alors le nœud mobile a indiqué qu'il utilise une adresse d'entretien d'agent étranger, et que l'agent étranger va donc désencapsuler les datagrammes arrivants avant de les transmettre au nœud mobile. Dans ce cas, pour transmettre un tel datagramme reçu en diffusion au nœud mobile, l'agent de rattachement DOIT d'abord encapsuler le datagramme en diffusion dans un datagramme en envoi individuel adressé à l'adresse de rattachement du nœud mobile, et DOIT ensuite tunneler le datagramme résultant à l'adresse d'entretien du nœud mobile.

Quand il est désencapsulé par l'agent étranger, le datagramme interne va donc être un datagramme IP en envoi individuel adressé au nœud mobile, identifiant à l'agent étranger la destination prévue du datagramme en diffusion encapsulé, et va être livré au nœud mobile de la même façon que tout datagramme tunnelé qui arrive pour le nœud mobile. L'agent étranger NE DOIT PAS désencapsuler le datagramme en diffusion encapsulé et NE DOIT PAS utiliser une diffusion de réseau local pour le transmettre au nœud mobile. Le nœud mobile DOIT donc désencapsuler lui-même le datagramme en diffusion encapsulé, et NE DOIT donc dans ce cas PAS établir le bit "B" dans sa demande d'enregistrement, sauf si il est capable de désencapsuler les datagrammes.

Le nœud mobile PEUT demander d'autres formes d'encapsulation en établissant le bit "M" et/ou le bit "G", mais seulement si le nœud mobile désencapsule ses propres datagrammes (le nœud mobile utilise une adresse d'entretien colocalisée) ou si son agent étranger a indiqué qu'il prend en charge ces formes d'encapsulation en établissant les bits correspondants dans l'extension Annonce d'agent de mobilité d'une annonce d'agent reçue par le nœud mobile. Autrement, le nœud mobile NE DOIT PAS établir ces bits.

Le champ Durée de vie est choisi comme suit :

- o Si le nœud mobile s'enregistre auprès d'un agent étranger, la durée de vie NE DEVRAIT PAS excéder la valeur du champ Durée de vie d'enregistrement du message d'annonce d'agent reçu de l'agent étranger. Quand la méthode par laquelle l'adresse d'entretien est apprise n'inclut pas de durée de vie, la durée de vie par défaut d'annonce de routeur ICMP (1800 secondes) PEUT être utilisée.
- o Le nœud mobile PEUT demander à un agent de rattachement de supprimer un lien de mobilité particulier, en envoyant une demande d'enregistrement avec l'adresse d'entretien pour ce lien, avec le champ Durée de vie réglé à zéro (paragraphe 3.8.2).
- o De même, une durée de vie de zéro est utilisée quand le nœud mobile désenregistre toutes les adresses d'entretien, comme lorsque il retourne chez lui.

Le champ Adresse de rattachement DOIT être réglé à l'adresse de rattachement du nœud mobile, si cette information est connue. Autrement, le champ Adresse de rattachement DOIT être réglé tout à zéro.

Le champ Agent de rattachement DOIT être réglé à l'adresse de l'agent de rattachement du nœud mobile, si le nœud mobile connaît cette adresse. Autrement, le nœud mobile PEUT utiliser la résolution dynamique d'adresse d'agent de rattachement pour apprendre l'adresse de son agent de rattachement. Dans ce cas, le nœud mobile DOIT régler le champ Agent de rattachement à l'adresse de diffusion dirigée sur le sous réseau du réseau de rattachement du nœud mobile. Chaque agent de rattachement qui reçoit une telle demande d'enregistrement avec une adresse de destination de diffusion DOIT rejeter l'enregistrement du nœud mobile et DEVRAIT retourner une réponse d'enregistrement de rejet indiquant son adresse IP d'envoi individuel pour que le nœud mobile l'utilise dans une future tentative d'enregistrement.

Le champ Adresse d'entretien DOIT être réglé à la valeur de l'adresse d'entretien particulière que le nœud mobile souhaite enregistrer/désenregistrer. Dans le cas particulier où un nœud mobile souhaite désenregistrer toutes les adresses d'entretien, il DOIT régler ce champ à son adresse de rattachement.

Le nœud mobile choisit le champ Identification en accord avec le style de protection contre la répétition qu'il utilise avec son agent de rattachement. Ceci fait partie de l'association de sécurité mobile que le nœud mobile partage avec son agent de rattachement. Voir au paragraphe 5.7 la méthode par laquelle le nœud mobile calcule le champ Identification.

#### 3.6.1.3 Extensions

On décrit ici l'ordre de toutes les extensions obligatoires et facultatives qu'un nœud mobile ajoute à une demande d'enregistrement. Cet ordre est EXIGÉ :

a. l'en-tête IP, suivi par l'en-tête UDP, suivi par la portion de longueur fixe de la demande d'enregistrement, suivie par
b. si il en est, toutes les extensions non d'authentification dont l'utilisation par l'agent de rattachement ou autre agent d'autorisation (qui peut ou non être aussi utile à l'agent étranger) est prévue, suivies par
c. toutes les extensions d'activation d'autorisation (voir au paragraphe 1.6), suivies par

d. si il en est, toutes les extensions non d'authentification utilisées seulement par l'agent étranger, suivies par
e. l'extension d'authentification mobile-étranger, si présente.

Noter que les éléments (a) et (c) DOIVENT apparaître dans chaque demande d'enregistrement envoyée par le nœud mobile. Les éléments (b), (d), et (e) sont facultatifs. Cependant, l'élément (e) DOIT être inclus quand le nœud mobile et l'agent étranger partagent une association de sécurité mobile.

### 3.6.2 Réception des réponses d'enregistrement

Les réponses d'enregistrement vont être reçues par le nœud mobile en réponse à ses demandes d'enregistrement. Les réponses d'enregistrement rentrent généralement dans une de ces trois catégories :

- l'enregistrement a été accepté,
- l'enregistrement a été refusé par l'agent étranger, ou
- l'enregistrement a été refusé par l'agent de rattachement.

Les paragraphes qui suivent décrivent le traitement de la réponse d'enregistrement par un nœud mobile dans chacune de ces trois catégories.

#### 3.6.2.1 Vérifications de validité

Les réponses d'enregistrement dont la somme de contrôle UDP non zéro est invalide DOIVENT être éliminées en silence.

De plus, les 32 bits de moindre poids du champ Identification dans la réponse d'enregistrement DOIVENT être comparés aux 32 bits de moindre poids du champ Identification de la plus récente demande d'enregistrement envoyée à l'agent qui répond. Si ils ne correspondent pas, la réponse DOIT être éliminée en silence.

Aussi, la présence dans la réponse d'enregistrement d'une extension d'activation d'autorisation DOIT être vérifiée. Pour tout message de réponse d'enregistrement contenant un code d'état qui indique l'état de l'agent de rattachement, le nœud mobile DOIT vérifier la présence d'une extension d'activation d'autorisation, agissant en accord avec le champ Code dans la réponse. Les règles sont les suivantes :

a. Si le nœud mobile et l'agent étranger partagent une association de sécurité mobile, exactement une extension d'authentification mobile-étranger DOIT être présente dans la réponse d'enregistrement, et le nœud mobile DOIT vérifier la valeur de l'authentifiant dans l'extension. Si aucune extension d'authentification mobile-étranger n'est trouvée, ou si plus d'une extension d'authentification mobile-étranger est trouvée, ou si l'authentifiant est invalide, le nœud mobile DOIT éliminer en silence la réponse et DEVRAIT enregistrer l'événement comme exception de sécurité.

b. Si le champ Code indique que le service est refusé par l'agent de rattachement, ou si le champ Code indique que l'enregistrement a été accepté par l'agent de rattachement, exactement une extension Authentification mobile-rattachement DOIT être présente dans la réponse d'enregistrement, et le nœud mobile DOIT vérifier la valeur de l'authentifiant dans l'extension. Si la réponse d'enregistrement a été générée par l'agent de rattachement mais qu'aucune extension Authentification mobile-rattachement n'est trouvée, ou si plus d'une extension Authentification mobile-rattachement est trouvée, ou si l'authentifiant est invalide, le nœud mobile DOIT éliminer en silence la réponse et DEVRAIT enregistrer l'événement comme exception de sécurité.

Si le champ Code indique un échec de l'authentification, chez l'agent étranger ou chez l'agent de rattachement, il est alors possible que tous les authentifiants de la réponse d'enregistrement soient aussi erronés. Cela peut arriver, par exemple, si le secret partagé entre le nœud mobile et l'agent de rattachement a été configuré de façon erronée. Le nœud mobile DEVRAIT enregistrer de telles erreurs comme des exceptions de sécurité.

#### 3.6.2.2 Demande d'enregistrement acceptée

Si le champ Code indique que la demande a été acceptée, le nœud mobile DEVRAIT configurer son tableau d'acheminement de façon appropriée pour son point de rattachement actuel (paragraphe 4.2.1).

Si le nœud mobile retourne à son réseau de rattachement et que ce réseau est un de ceux qui mettent en œuvre ARP, le nœud mobile DOIT suivre les procédures décrites au paragraphe 4.6 à l'égard de ARP, du mandataire ARP, et de ARP gratuit.

Si le nœud mobile s'est enregistré sur un réseau étranger, il DEVRAIT se réenregistrer avant l'expiration de la durée de vie de son enregistrement. Comme décrit au paragraphe 3.6, pour chaque demande d'enregistrement en instance, le nœud mobile DOIT conserver la durée de vie restante de cet enregistrement en instance, ainsi que la durée de vie originale

provenant de la demande d'enregistrement. Quand le nœud mobile reçoit une réponse d'enregistrement valide, le nœud mobile DOIT diminuer sa vue de la durée de vie restante de l'enregistrement de la quantité dont l'agent de rattachement a diminué la durée de vie demandée originellement. Cette procédure est équivalente à celle du nœud mobile qui lance un temporisateur pour la durée de vie accordée au moment où il envoie la demande d'enregistrement, même si la durée de vie accordée n'est pas connue du nœud mobile tant que la réponse d'enregistrement n'est pas reçue. Comme la demande d'enregistrement est certainement envoyée avant que l'agent de rattachement commence la temporisation de la durée de vie de l'enregistrement (aussi fondée sur la durée de vie accordée) cette procédure assure que le nœud mobile va se réenregistrer avant que l'agent de rattachement arrive à expiration et supprime l'enregistrement, en dépit de délais de transmission éventuellement non négligeables pour la demande et la réponse originales d'enregistrement qui ont lancé la temporisation de la durée de vie au nœud mobile et chez son agent de rattachement.

#### 3.6.2.3 Demande d'enregistrement refusée

Si le champ Code indique que le service est refusé, le nœud mobile DEVRAIT enregistrer l'erreur. Dans certains cas, le nœud mobile peut être capable de "réparer" l'erreur. Cela inclut :

Code 69 : (refusé par l'agent étranger, durée de vie demandée trop longue). Dans ce cas, le champ Durée de vie dans la réponse d'enregistrement va contenir la valeur maximum de durée de vie que l'agent étranger veut accepter dans toute demande d'enregistrement. Le nœud mobile PEUT tenter de s'enregistrer auprès du même agent, en utilisant une durée de vie dans la demande d'enregistrement qui DOIT être inférieure ou égale à la valeur spécifiée dans la réponse.

Code 133 : (refusé par l'agent de rattachement, discordance d'identification d'enregistrement). Dans ce cas, le champ Identification dans la réponse d'enregistrement va contenir une valeur qui permet au nœud mobile de se synchroniser avec l'agent de rattachement, sur la base du style de protection activée contre la répétition (paragraphe 5.7). Le nœud mobile DOIT ajuster les paramètres qu'il utilise pour calculer le champ Identification sur la base des informations dans la réponse d'enregistrement, avant de produire toute demande d'enregistrement future

Code 136 : (refusé par l'agent de rattachement, adresse d'agent de rattachement inconnue). Ce code est retourné par un agent de rattachement quand le nœud mobile effectue une résolution dynamique d'adresse d'agent de rattachement comme décrit aux paragraphes 3.6.1.1 et 3.6.1.2. Dans ce cas, le champ Agent de rattachement dans la réponse va contenir l'adresse IP d'envoi individuel de l'agent de rattachement qui retourne la réponse. Le nœud mobile PEUT alors tenter de s'enregistrer auprès de cet agent de rattachement dans de futures demandes d'enregistrement. De plus, le nœud mobile DEVRAIT ajuster les paramètres qu'il utilise pour calculer le champ Identification sur la base du champ correspondant dans la réponse d'enregistrement, avant de produire de futures demandes d'enregistrement.

### 3.6.3 Retransmission d'enregistrement

Quand aucune réponse d'enregistrement n'a été reçue dans un délai raisonnable, une autre demande d'enregistrement PEUT être transmise. Quand des horodatages sont utilisés, une nouvelle identification d'enregistrement est choisie pour chaque retransmission ; donc, elle compte comme un nouvel enregistrement. Quand des noms occasionnels sont utilisés, la demande sans réponse est retransmise inchangée ; donc, la retransmission ne compte pas comme un nouvel enregistrement (paragraphe 5.7). De cette façon, une retransmission ne va pas exiger que l'agent de rattachement se resynchronise avec le nœud mobile en produisant un autre nom occasionnel dans le cas où la demande d'enregistrement originale (plutôt que sa réponse d'enregistrement) a été perdue par le réseau.

Le délai maximum jusqu'à ce qu'une nouvelle demande d'enregistrement soit envoyée NE DEVRAIT PAS être supérieur à la durée de vie demandée de la demande d'enregistrement. La valeur minimum DEVRAIT être assez grande pour tenir compte de la taille des messages, deux fois le délai aller-retour pour la transmission à l'agent de rattachement, et au moins un délai supplémentaire de 100 millisecondes pour permettre le traitement des messages avant de répondre. Le délai d'aller-retour pour la transmission à l'agent de rattachement sera au moins aussi long que le temps nécessaire pour transmettre les messages à la vitesse de la liaison du point de rattachement actuel du nœud mobile. Certains circuits ajoutent encore 200 millisecondes de délai de satellite au délai total d'aller-retour à l'agent de rattachement. Le délai minimum entre les demandes d'enregistrement NE DOIT PAS être inférieur à 1 seconde. Chaque période successive de temporisation de retransmission DEVRAIT être au moins de deux fois la période précédente, pour autant que ceci soit inférieur au maximum spécifié ci-dessus.

## 3.7 Considérations d'agent étranger

L'agent étranger joue un rôle essentiellement passif dans l'enregistrement IP mobile. Il relaye les demandes d'enregistrement entre les nœuds mobiles et les agents de rattachement, et, quand il fournit l'adresse d'entretien, désencapsule les datagrammes pour livraison au nœud mobile. Il DEVRAIT aussi envoyer périodiquement des messages

d'annonce d'agent pour annoncer sa présence comme décrit au paragraphe 2.3, si il n'est pas détectable par les moyens de la couche de liaison.

Un agent étranger NE DOIT PAS transmettre une demande d'enregistrement, sauf si la demande est relayée à partir d'un nœud mobile à cet agent de rattachement du nœud mobile. Un agent étranger NE DOIT PAS transmettre une réponse d'enregistrement sauf quand il relaye une réponse d'enregistrement reçue d'un agent de rattachement du nœud mobile, ou quand il répond à une demande d'enregistrement reçue d'un nœud mobile dans le cas où l'agent étranger refuse le service au nœud mobile. En particulier, un agent étranger NE DOIT PAS générer une demande ou réponse d'enregistrement parce que la durée de vie d'enregistrement du nœud mobile a expiré. Un agent étranger NE DOIT PAS non plus générer un message Demande d'enregistrement qui demande le désenregistrement d'un nœud mobile ; cependant, il DOIT relayer les demandes d'enregistrement/désenregistrement bien formées générées par un nœud mobile.

### 3.7.1 Tableaux de configuration et d'enregistrement

Chaque agent étranger DOIT être configuré avec une adresse d'entretien. De plus, pour chaque enregistrement en instance ou en cours, l'agent étranger DOIT conserver une entrée de la liste des visiteurs contenant les informations suivantes, obtenues de la demande d'enregistrement du nœud mobile :

- o l'adresse de source de couche de liaison du nœud mobile,
- o l'adresse IP de source (l'adresse de rattachement du nœud mobile) ou son adresse d'entretien colocalisée (voir la description du bit "R" au paragraphe 2.1.1)
- o l'adresse de destination IP (comme spécifié au paragraphe 3.6.1.1)
- o l'accès de source UDP,
- o l'adresse de l'agent de rattachement,
- o le champ Identification,
- o la durée de vie d'enregistrement demandée, et
- o la durée de vie restante de l'enregistrement en instance ou en cours.

Si il y a une extension NAI dans le message Demande d'enregistrement (souvent, par exemple, quand l'adresse de rattachement du nœud mobile est zéro) l'agent étranger DOIT alors suivre les procédures spécifiées dans la [RFC2794]. En particulier, si l'agent étranger ne peut pas gérer les enregistrements en instance de demande d'enregistrement avec une telle adresse de rattachement de zéro pour le nœud mobile, l'agent étranger DOIT retourner une réponse d'enregistrement avec le code indiquant NONZERO_HOMEADDR_REQD (voir la [RFC2794]).

L'agent étranger PEUT configurer un maximum d'enregistrements en instance qu'il veut conserver (normalement 5). Les enregistrements supplémentaires DEVRAIENT alors être rejetés par l'agent étranger avec le code 66. L'agent étranger PEUT supprimer toute demande d'enregistrement en instance après qu'elle est restée en instance pendant plus de 7 secondes ; dans ce cas, l'agent étranger DEVRAIT rejeter la demande avec le code 78 (fin de temporisation d'enregistrement).

Comme avec tout nœud sur l'Internet, un agent étranger PEUT aussi partager des associations de sécurité de mobilité avec tous autres nœuds. Quand il relaye une demande d'enregistrement d'un nœud mobile à son agent de rattachement, si l'agent étranger partage une association de sécurité mobile avec l'agent de rattachement, il DOIT ajouter une extension Authentification étranger-rattachement à la demande. Dans ce cas, quand la réponse d'enregistrement a une durée de vie non à zéro, l'agent étranger DOIT vérifier l'extension Authentification étranger-rattachement exigée dans la réponse d'enregistrement provenant de l'agent de rattachement (paragraphes 3.3 et 3.4). De même, quand il reçoit une demande d'enregistrement provenant d'un nœud mobile, si l'agent étranger partage une association de sécurité mobile avec le nœud mobile, il DOIT vérifier l'extension d'authentification mobile-étranger exigée dans la demande et DOIT ajouter une extension d'authentification mobile-étranger à la réponse d'enregistrement au nœud mobile.

### 3.7.2 Réception des demandes d'enregistrement

Si l'agent étranger accepte une demande d'enregistrement d'un nœud mobile, il vérifie que l'adresse d'agent de rattachement indiquée n'appartient pas à une interface réseau de l'agent étranger. Sinon, l'agent étranger DOIT alors relayer la demande à l'agent de rattachement indiqué. Autrement, si l'agent étranger refuse la demande, il DOIT envoyer une réponse d'enregistrement au nœud mobile avec un code de refus approprié, sauf dans les cas où l'agent étranger serait obligé d'envoyer plus d'un tel refus par seconde au même nœud mobile. Les paragraphes qui suivent décrivent ce comportement plus en détail.

Si l'agent étranger a configuré une de ses interfaces réseau avec l'adresse IP spécifiée par le nœud mobile comme son adresse d'agent de rattachement, l'agent étranger NE DOIT PAS transmettre à nouveau la demande. Si l'agent étranger sert le nœud mobile comme agent de rattachement, l'agent étranger suit les procédures spécifiées au paragraphe 3.8.2. Autrement, si l'agent étranger ne sert pas le nœud mobile comme agent de rattachement, l'agent étranger rejette la demande d'enregistrement avec le code 116 (Adresse d'agent de rattachement invalide).

Si un agent étranger reçoit une demande d'enregistrement d'un nœud mobile qui est dans sa liste des visiteurs, l'entrée existante de la liste des visiteurs pour le nœud mobile NE DEVRAIT PAS être supprimée ou modifiée jusqu'à de que l'agent étranger reçoive une réponse d'enregistrement valide de la part de l'agent de rattachement avec un code indiquant le succès. L'agent étranger DOIT enregistrer la nouvelle demande en instance comme une partie séparée de l'entrée existante de liste des visiteurs pour le nœud mobile. Si la demande d'enregistrement demande le désenregistrement, l'entrée existante de liste des visiteurs pour le nœud mobile NE DEVRAIT PAS être supprimée jusqu'à ce que l'agent étranger ait reçu une réponse d'enregistrement réussi. Si la réponse d'enregistrement indique que la demande (d'enregistrement ou de désenregistrement) a été refusée par l'agent de rattachement, l'entrée existante de liste de visiteurs pour le nœud mobile NE DOIT PAS être modifiée par suite de la réception de la réponse d'enregistrement.

#### 3.7.2.1 Vérifications de validité

Les demandes d'enregistrement avec une somme de contrôle UDP invalide non zéro DOIVENT être éliminées en silence. Les demandes avec des bits non à zéro dans les champs réservés reçus DOIVENT être rejetées avec le code 70 (Demande mal formée). Les demandes avec le bit "D" réglé à 0, une durée de vie non à zéro, et qui spécifient une adresse d'entretien non offerte par l'agent étranger, DOIVENT être rejetées avec le code 77 (Adresse d'entretien invalide).

Aussi, l'authentification dans la demande d'enregistrement DOIT être vérifiée. Si l'agent étranger et le nœud mobile partagent une association de sécurité mobile, exactement une extension d'authentification mobile-étranger DOIT être présente dans la demande d'enregistrement, et l'agent étranger DOIT vérifier la valeur de l'authentifiant dans l'extension. Si aucune extension d'authentification mobile-étranger n'est trouvée, ou si plus d'une extension d'authentification mobile-étranger est trouvée, ou si l'authentifiant est invalide, l'agent étranger DOIT éliminer en silence la demande et DEVRAIT enregistrer l'événement comme exception de sécurité. L'agent étranger DEVRAIT aussi envoyer une réponse d'enregistrement au nœud mobile avec le code 67.

#### 3.7.2.2 Transmission d'une demande valide à l'agent de rattachement

Si l'agent étranger accepte la demande d'enregistrement du nœud mobile, il DOIT relayer la demande à l'agent de rattachement du nœud mobile comme spécifié dans le champ Agent de rattachement de la demande d'enregistrement. L'agent étranger NE DOIT PAS modifier de champs commençant par la portion fixe de la demande d'enregistrement jusque et y compris l'extension Authentification mobile-rattachement ou autre extension d'authentification fournie par le nœud mobile comme extension d'activation d'autorisation pour l'agent de rattachement. Autrement, un échec d'authentification va très probablement se produire chez l'agent de rattachement. De plus, l'agent étranger procède comme suit :

- o il DOIT traiter et supprimer toute extension qui ne précède pas une extension d'activation d'autorisation,
- o il PEUT ajouter une de ses propres extensions non d'authentification pertinente pour l'agent de rattachement, si applicable, et,
- o si l'agent étranger partage une association de sécurité mobile avec l'agent de rattachement, et si la demande a une durée de vie $\neq 0$, il DOIT alors ajouter l'extension Authentification étranger-rattachement.

Les champs spécifiques au sein de l'en-tête IP et de l'en-tête UDP de la demande d'enregistrement relayée DOIVENT être réglés comme suit :

Adresse IP de source : l'adresse d'entretien offerte par l'agent étranger pour le nœud mobile qui envoie la demande d'enregistrement.
Adresse de destination IP : copiée du champ Agent de rattachement dans la demande d'enregistrement.
Accès de source UDP : variable.
Accès de destination UDP : 434

Après la transmission d'une demande d'enregistrement valide à l'agent de rattachement, l'agent étranger DOIT lancer le temporisateur de durée de vie restante de l'enregistrement en instance sur la base de la durée de vie dans la demande d'enregistrement. Si cette durée de vie indiquée expire avant de recevoir une réponse d'enregistrement valide, l'agent étranger DOIT supprimer son entrée de liste des visiteurs pour cet enregistrement en instance.

#### 3.7.2.3 Refus des demandes invalides

Si l'agent étranger refuse la demande d'enregistrement du nœud mobile pour une raison quelconque, il DEVRAIT envoyer au nœud mobile une réponse d'enregistrement avec un code de refus approprié. Dans ce cas, les champs Adresse de rattachement, Agent de rattachement, et Identification dans la réponse d'enregistrement sont copiés des champs correspondants de la demande d'enregistrement.

Si le champ Réservé n'est pas zéro, l'agent étranger DOIT refuser la demande et DEVRAIT retourner une réponse d'enregistrement avec le code d'état 70 au nœud mobile. Si la demande est refusée parce que la durée de vie demandée est

trop longue, l'agent étranger règle la durée de vie dans la demande à la valeur maximum de durée de vie qu'il veut accepter dans une demande d'enregistrement, et règle de champ Code à 69. Autrement, la durée de vie DEVRAIT être copiée du champ Durée de vie de la demande.

Les champs spécifiques dans l'en-tête IP et l'en-tête UDP de la réponse d'enregistrement DOIVENT être réglés comme suit :

Adresse IP de source : copiée de l'adresse IP de destination de la demande d'enregistrement, sauf si l'adresse "Tous agents de diffusion groupée" était utilisée. Dans ce cas, l'adresse de l'agent étranger (sur l'interface d'où le message sera envoyé) DOIT être utilisée.

Adresse de destination IP : si la réponse d'enregistrement est générée par l'agent étranger afin de rejeter la demande d'enregistrement d'un nœud mobile, et si la demande d'enregistrement contient une adresse de rattachement qui n'est pas 0.0.0.0, alors l'adresse IP de destination est copiée du champ Adresse de rattachement de la demande d'enregistrement. Autrement, si la réponse d'enregistrement est reçue de l'agent de rattachement, et contient une adresse de rattachement qui n'est pas 0.0.0.0, alors l'adresse de destination IP est copiée du champ Adresse de rattachement de la réponse d'enregistrement. Autrement, l'adresse de destination IP de la réponse d'enregistrement est réglée à 255.255.255.255.

Accès de source UDP : 434

Accès de destination UDP : copiée de l'accès de source UDP de la demande d'enregistrement.

### 3.7.3 Réception des réponses d'enregistrement

L'agent étranger met à jour sa liste des visiteurs quand il reçoit une réponse d'enregistrement valide d'un agent de rattachement. il relaye alors la réponse d'enregistrement au nœud mobile. Le paragraphe qui suit décrit ce comportement plus en détail.

Si lorsque il relaye une demande d'enregistrement à un agent de rattachement, l'agent étranger reçoit un message d'erreur ICMP au lieu d'une réponse d'enregistrement, l'agent étranger DEVRAIT alors envoyer au nœud mobile une réponse d'enregistrement avec un code d'échec approprié "Agent de rattachement injoignable" (dans la gamme de 80-95, inclus). Voir au paragraphe 3.7.2.3 les détails de la construction de la réponse d'enregistrement.

#### 3.7.3.1 Vérifications de validité

Les réponses d'enregistrement avec une somme de contrôle UDP invalide non à zéro DOIVENT être éliminées en silence.

Quand un agent étranger reçoit un message de réponse d'enregistrement, il DOIT chercher dans sa liste des visiteurs une demande d'enregistrement en instance avec la même adresse de rattachement de nœud mobile qu'indiquée dans la réponse. Si il y a plusieurs entrées avec la même adresse de rattachement, et si la réponse d'enregistrement a l'extension NAI de nœud mobile [RFC2794], l'agent étranger DOIT utiliser le NAI pour distinguer les demandes d'enregistrement en instance avec la même adresse de rattachement. Si aucune demande en instance correspondante n'est trouvée, et si la réponse d'enregistrement ne correspond à aucune demande d'enregistrement en instance avec une adresse de rattachement de nœud mobile de zéro (voir au paragraphe 3.7.1) l'agent étranger DOIT éliminer en silence la réponse. L'agent étranger DOIT aussi éliminer en silence la réponse si les 32 bits de moindre poids du champ Identification de la réponse ne correspondent pas à ceux de la demande.

Aussi, l'authentification dans la réponse d'enregistrement DOIT être vérifiée. Si l'agent étranger et l'agent de rattachement partagent une association de sécurité mobile, exactement une extension Authentification étranger-rattachement DOIT être présente dans la réponse d'enregistrement, et l'agent étranger DOIT vérifier la valeur de l'authentifiant dans l'extension. Si aucune extension Authentification étranger-rattachement n'est trouvée, ou si plus d'une extension Authentification étranger-rattachement est trouvée, ou si l'authentifiant est invalide, l'agent étranger DOIT éliminer en silence la réponse et DEVRAIT enregistrer l'événement comme exception de sécurité. L'agent étranger DOIT aussi rejeter l'enregistrement du nœud mobile et DEVRAIT envoyer une réponse d'enregistrement au nœud mobile avec le code 68.

#### 3.7.3.2 Transmission des réponses au nœud mobile

Une réponse d'enregistrement qui satisfait les vérifications de validité du paragraphe 3.7.3.1 est relayée au nœud mobile. L'agent étranger DOIT aussi mettre à jour son entrée de liste des visiteurs pour le nœud mobile pour refléter le résultat de la demande d'enregistrement, comme indiqué par le champ Code dans la réponse. Si le code indique que l'agent de rattachement a accepté l'enregistrement et si le champ Durée de vie n'est pas zéro, l'agent étranger DEVRAIT régler la durée de vie dans l'entrée de liste des visiteurs au minimum des deux valeurs suivantes :

- la valeur spécifiée dans le champ Durée de vie de la réponse d'enregistrement, et
- la propre valeur maximum de l'agent étranger pour la durée de vie d'enregistrement admissible.

Si le code indique plutôt que le champ Durée de vie est zéro, l'agent étranger DOIT supprimer son entrée de liste des visiteurs pour le nœud mobile. Finalement, si le code indique que l'enregistrement a été refusé par l'agent de rattachement, l'agent étranger DOIT supprimer son entrée de liste d'enregistrements en instance, mais pas son entrée de liste des visiteurs, pour le nœud mobile.

L'agent étranger NE DOIT modifier aucun des champs commençant par la portion fixe de la réponse d'enregistrement jusque et y compris l'extension Authentification mobile-rattachement. Autrement, un échec d'authentification va très probablement se produire au nœud mobile. De plus, l'agent étranger DEVRAIT effectuer les procédures supplémentaires suivantes :

- Il DOIT traiter et supprimer toute extension non couverte par une extension d'activation d'autorisation,
- Il PEUT ajouter ses propres extension non d'authentification qui fournissent des informations au nœud mobile, si applicable, et,
- il DOIT ajouter l'extension d'authentification mobile-étranger, si l'agent étranger partage une association de sécurité mobile avec le nœud mobile.

Dans les en-têtes IP et l'en-tête UDP, les champs spécifiques de la réponse d'enregistrement relayée sont réglés selon les mêmes règles que spécifié au paragraphe 3.7.2.3.

Après la transmission d'une réponse d'enregistrement valide au nœud mobile, l'agent étranger DOIT mettre à jour son entrée de liste des visiteurs pour cet enregistrement comme suit. Si la réponse d'enregistrement indique que l'enregistrement a été accepté par l'agent de rattachement, l'agent étranger règle son temporisateur de durée de vie d'enregistrement à la durée de vie accordée dans la réponse d'enregistrement ; à la différence du réglage de la durée de vie d'enregistrement du nœud mobile, comme décrit au paragraphe 3.6.2.2, l'agent étranger considère que cette durée de vie commence quand il transmet le message de réponse d'enregistrement, s'assurant que l'agent étranger ne va pas faire expirer l'enregistrement avant le nœud mobile. Par ailleurs, si la réponse d'enregistrement indique que l'enregistrement a été rejeté par l'agent de rattachement, l'agent étranger supprime son entrée de liste des visiteurs pour cette tentative d'enregistrement.

## 3.8 Considérations d'agent de rattachement

Les agents de rattachement jouent un rôle réactif dans le processus d'enregistrement. L'agent de rattachement reçoit les demandes d'enregistrement du nœud mobile (peut-être relayées par un agent étranger) met à jour son enregistrement des liens de mobilité pour ce nœud mobile, et produit une réponse d'enregistrement convenable en réponse à chacune.

Un agent de rattachement NE DOIT PAS transmettre une réponse d'enregistrement sauf quand il répond à une demande d'enregistrement reçue d'un nœud mobile. En particulier, l'agent de rattachement NE DOIT PAS générer une réponse d'enregistrement pour indiquer que la durée de vie a expiré.

### 3.8.1 Tableaux de configuration et d'enregistrement

Chaque agent de rattachement DOIT être configuré avec une adresse IP et la taille de préfixe pour le réseau de rattachement. L'agent de rattachement DOIT être configuré avec l'association de sécurité mobile de chaque nœud mobile autorisé qu'il dessert comme agent de rattachement.

Quand l'agent de rattachement accepte une demande d'enregistrement valide d'un nœud mobile qu'il dessert comme agent de rattachement, l'agent de rattachement DOIT créer ou modifier l'entrée pour ce nœud mobile dans sa liste des liens de mobilité contenant :

- l'adresse de rattachement du nœud mobile,
- l'adresse d'entretien du nœud mobile,
- le champ Identification provenant de la réponse d'enregistrement,
- la durée de vie restante de l'enregistrement.

L'agent de rattachement PEUT facultativement offrir la capacité d'associer dynamiquement une adresse de rattachement à un nœud mobile à réception d'une demande d'enregistrement de ce nœud mobile. La méthode par laquelle est allouée une adresse de rattachement au nœud mobile sort du domaine d'application du présent document, mais voir la [RFC2794]. Après que l'agent de rattachement a fait l'association de l'adresse de rattachement au nœud mobile, l'agent de rattachement DOIT mettre cette adresse de rattachement dans le champ Adresse de rattachement de la réponse d'enregistrement.

L'agent de rattachement PEUT aussi maintenir des associations de sécurité de mobilité avec divers agents étrangers. Quand il reçoit une demande d'enregistrement d'un agent étranger, si l'agent de rattachement partage une association de sécurité

mobile avec l'agent étranger, l'agent de rattachement DOIT vérifier l'authentifiant dans l'extension Authentification étranger-rattachement exigée dans le message, sur la base de cette association de sécurité mobile, sauf si le champ Durée de vie égale 0. Quand il traite une demande d'enregistrement avec Durée de vie = 0, le HA PEUT sauter la vérification de la présence et validité d'une extension Authentification étranger-rattachement. De même, quand il envoie une réponse d'enregistrement à un agent étranger, si l'agent de rattachement partage une association de sécurité mobile avec l'agent étranger, l'agent de rattachement DOIT inclure une extension Authentification étranger-rattachement dans le message, sur la base de cette association de sécurité mobile.

### 3.8.2 Réception des demandes d'enregistrement

Si l'agent de rattachement accepte une demande d'enregistrement entrante, il DOIT mettre à jour son enregistrement des liens de mobilité du nœud mobile et DEVRAIT envoyer une réponse d'enregistrement avec un code convenable. Autrement (l'agent de rattachement a refusé la demande) il DEVRAIT dans la plupart des cas envoyer une réponse d'enregistrement avec un code approprié spécifiant la raison du refus de la demande. Les paragraphes qui suivent décrivent ce comportement plus en détail. Si l'agent de rattachement ne prend pas en charge les diffusions (voir au paragraphe 4.3) il DOIT ignorer le bit "B" (plutôt que de rejeter la demande d'enregistrement).

#### 3.8.2.1 Vérifications de validité

Les demandes d'enregistrement avec une somme de contrôle UDP invalide, non zéro, DOIVENT être éliminées en silence par l'agent de rattachement.

L'authentification dans la demande d'enregistrement DOIT être vérifiée. Cela implique les opérations suivantes :

a L'agent de rattachement DOIT vérifier la présence d'au moins une extension d'activation d'autorisation, et s'assurer que toutes les authentifications indiquées sont effectuées. Au moins une extension d'activation d'autorisation DOIT être présente dans la demande d'enregistrement, et l'agent de rattachement DOIT soit vérifier la valeur de l'authentifiant dans l'extension, soit vérifier que la valeur de l'authentifiant a été vérifiée par un autre agent avec lequel il a une association de sécurité.
Si l'agent de rattachement reçoit une demande d'enregistrement provenant d'un nœud mobile avec lequel il n'a aucune association de sécurité, l'agent de rattachement DOIT éliminer en silence la demande d'enregistrement.
Si l'agent de rattachement reçoit une demande d'enregistrement sans aucune extension d'activation d'autorisation, l'agent de rattachement DOIT éliminer en silence la demande d'enregistrement.
Si l'authentifiant est invalide, l'agent de rattachement DOIT rejeter l'enregistrement du nœud mobile. Les autres actions à entreprendre dans ce cas dépendent de si la demande a une extension d'authentification étranger-rattachement valide (comme suit) :
   * Si il y a une extension d'authentification étranger-rattachement valide, l'agent de rattachement DOIT envoyer une réponse d'enregistrement avec le code 131.
   * Autrement, si il n'y a pas d'association de sécurité étranger-rattachement, l'agent de rattachement PEUT envoyer une réponse d'enregistrement avec le code 131. Si l'agent de rattachement envoie une réponse d'enregistrement, elle DOIT contenir une extension Authentification mobile-rattachement valide. En construisant la réponse, l'agent de rattachement DEVRAIT choisir une association de sécurité qui existe probablement dans le nœud mobile ; par exemple, ce peut être une association de sécurité plus ancienne ou une qui a une plus longue durée de vie que celle que le nœud mobile a tenté d'utiliser dans sa demande. Les déploiements devraient, quand ils mettent à jour les associations de sécurité, s'assurer qu'il y a au moins une association de sécurité commune entre le nœud mobile et l'agent de rattachement. Dans tous les cas d'échec d'authentifiant, l'agent de rattachement DOIT alors éliminer la demande sans autre traitement et DEVRAIT enregistrer l'erreur comme une exception de sécurité.

b. L'agent de rattachement DOIT vérifier que le champ Identification d'enregistrement est correct en utilisant le contexte choisi par le SPI dans l'extension d'activation d'autorisation que l'agent de rattachement a utilisé pour authentifier la demande d'enregistrement du nœud mobile. Voir au paragraphe 5.7 une description de la façon dont ceci est effectué. Si c'est incorrect, l'agent de rattachement DOIT rejeter la demande et DEVRAIT envoyer une réponse d'enregistrement au nœud mobile avec le code 133, incluant un champ Identification calculé en accord avec les règles spécifiées au paragraphe 5.7. L'agent de rattachement DOIT ne pas poursuivre le traitement d'une telle demande, mais DEVRAIT enregistrer l'erreur comme exception de sécurité.

c. Si l'agent de rattachement partage une association de sécurité mobile avec l'agent étranger, et si c'est une demande d'enregistrement (elle a une durée de vie non zéro) l'agent de rattachement DOIT vérifier la présence d'une extension Authentification étranger-rattachement valide. Exactement une extension Authentification étranger-rattachement DOIT être présente dans la Demande d'enregistrement dans ce cas, et l'agent de rattachement DOIT vérifier la valeur de l'authentifiant dans l'extension. Si aucune extension Authentification étranger-rattachement n'est trouvée, ou si plus d'une extension Authentification étranger-rattachement est trouvée, ou si l'authentifiant est invalide, l'agent de

rattachement DOIT rejeter l'enregistrement du nœud mobile et DEVRAIT envoyer une réponse d'enregistrement au nœud mobile avec le code 132. L'agent de rattachement DOIT alors éliminer la demande et DEVRAIT enregistrer l'erreur comme exception de sécurité.

d. Si l'agent de rattachement et l'agent étranger ne partagent pas d'association de sécurité mobile, et si l'enregistrement contient une extension Authentification étranger-rattachement, l'agent de rattachement DOIT éliminer la demande et DEVRAIT enregistrer l'erreur comme exception de sécurité.

En plus de vérifier l'authentification dans la demande d'enregistrement, les agents de rattachement DOIVENT refuser les demandes d'enregistrement envoyées à l'adresse de diffusion dirigée sur le sous réseau du réseau de rattachement (par opposition à l'envoi individuel à l'agent de rattachement). L'agent de rattachement DOIT éliminer la demande et DEVRAIT retourner une réponse d'enregistrement avec un code de 136. Dans ce cas, la réponse d'enregistrement va contenir l'adresse d'envoi individuel de l'agent de rattachement, de sorte que le nœud mobile pourra produire à nouveau la demande d'enregistrement avec l'adresse correcte d'agent de rattachement.

Noter que certains routeurs changent l'adresse de destination IP d'un datagramme d'une adresse de diffusion dirigée sur le sous réseau en 255.255.255.255 avant de l'injecter dans le sous réseau de destination. Dans ce cas, les agents de rattachement qui tentent de prendre des demandes dynamiques de découverte d'agent de rattachement en liant explicitement une prise à l'adresse de diffusion dirigée sur le sous réseau ne vont pas voir de tels paquets. Les mises en œuvre d'agent de rattachement devraient être prêtes à avoir aussi bien l'adresse de diffusion dirigée sur le sous réseau et 255.255.255.255 si elles souhaitent prendre en charge la découverte dynamique d'agent de rattachement.

#### 3.8.2.2 Acceptation d'une demande valide

Si la demande d'enregistrement satisfait les vérifications de validité du paragraphe 3.8.2.1, et si l'agent de rattachement est capable de s'accommoder de la demande, l'agent de rattachement DOIT mettre à jour sa liste de liens de mobilité pour le nœud mobile demandeur et DOIT retourner une réponse d'enregistrement au nœud mobile. Dans ce cas, le code dans la réponse d'enregistrement va être soit 0 si l'agent de rattachement prend en charge des liens simultanés de mobilité, soit 1 si il ne le fait pas. Voir au paragraphe 3.8.3 les détails de la construction du message de réponse d'enregistrement.

L'agent de rattachement met à jour, sur la base des champs de la demande d'enregistrement, ses enregistrements de liens de mobilité du nœud mobile comme suit :

- Si la durée de vie est zéro et si l'adresse d'entretien est égale à l'adresse de rattachement du nœud mobile, l'agent de rattachement supprime toutes les entrées de la liste de liens de mobilité pour le nœud mobile demandeur. C'est comme si un nœud mobile demandait que son agent de rattachement cesse de fournir des services de mobilité.
- Si la durée de vie est zéro et si l'adresse d'entretien n'est pas égale à l'adresse de rattachement du nœud mobile, l'agent de rattachement supprime seulement l'entrée contenant l'adresse d'entretien spécifiée de la liste des liens de mobilité pour le nœud mobile demandeur. Toutes les autres entrées actives contenant d'autres adresses d'entretien vont rester actives.
- Si la durée de vie n'est pas zéro, l'agent de rattachement ajoute une entrée contenant l'adresse d'entretien demandée à la liste de liens de mobilité pour le nœud mobile. Si le bit "S" est établi et si l'agent de rattachement prend en charge les liens de mobilité simultanés, les précédentes entrées de mobilité sont conservées. Autrement, l'agent de rattachement retire toutes les précédentes entrées de la liste des liens de mobilité pour le nœud mobile.

Dans tous les cas, l'agent de rattachement DOIT envoyer une réponse d'enregistrement à la source de la demande d'enregistrement, qui peut bien sûr être un agent étranger différent de celui dont l'adresse d'entretien est en train d'être (dés)enregistrée. Si l'agent de rattachement partage une association de sécurité mobile avec l'agent étranger dont l'adresse d'entretien est en train d'être désenregistrée, et si cet agent étranger est différent de celui qui a relayé la demande d'enregistrement, l'agent de rattachement PEUT de plus envoyer une réponse d'enregistrement à l'agent étranger dont l'adresse d'entretien est en train d'être désenregistrée. L'agent de rattachement NE DOIT PAS envoyer une telle réponse si il ne partage pas une association de sécurité mobile avec l'agent étranger. Si aucune réponse n'est envoyé, la liste de visiteurs de l'agent étranger va arriver naturellement à expiration quand la durée de vie originale expirera.

Quand un agent étranger relaye un message de désenregistrement contenant une adresse d'entretien qu'il ne possède pas, il NE DOIT PAS ajouter d'extension Authentification étranger-rattachement à ce désenregistrement. Voir au paragraphe 3.5.4 plus de détails.

L'agent de rattachement NE DOIT PAS augmenter la durée de vie au delà de ce qui est spécifié par le nœud mobile dans la demande d'enregistrement. Cependant, ce n'est pas une erreur pour le nœud mobile de demander une durée de vie plus longue que ce que l'agent de rattachement veut accepter. Dans ce cas, l'agent de rattachement réduit simplement la durée de vie à une valeur permise et retourne cette valeur dans la réponse d'enregistrement. La valeur de durée de vie dans la réponse d'enregistrement informe le nœud mobile de la durée de vie accordée pour l'enregistrement, indiquant quand il DEVRAIT

se réenregistrer afin de conserver le service. Après l'expiration de cette durée de vie d'enregistrement, l'agent de rattachement DOIT supprimer son entrée pour cet enregistrement dans sa liste de liens de mobilité.

Si la demande d'enregistrement duplique une demande d'enregistrement actuellement acceptée, la nouvelle durée de vie NE DOIT PAS s'étendre au delà de la durée de vie originellement accordée. Une demande d'enregistrement est un dupliqué si les champs Adresse de rattachement, Adresse d'entretien, et Identification sont égaux à ceux d'un enregistrement actuellement accepté.

De plus, si le réseau de rattachement met en œuvre ARP [RFC0826], et si la demande d'enregistrement demande à l'agent de rattachement de créer un lien de mobilité pour un nœud mobile qui n'avait antérieurement pas de lien (le nœud mobile était précédemment supposé être chez lui) alors l'agent de rattachement DOIT suivre les procédures décrites au paragraphe 4.6 à l'égard de ARP, mandataire ARP, et ARP gratuit. Si le nœud mobile a déjà un lien de mobilité antérieur, l'agent de rattachement DOIT continuer de suivre les règles pour les mandataires ARP décrites au paragraphe 4.6.

#### 3.8.2.3 Refus d'une demande invalide

Si la demande d'enregistrement ne satisfait pas toutes les vérifications de validité du paragraphe 3.8.2.1, ou si l'agent de rattachement est incapable de s'accommoder de la demande, l'agent de rattachement DEVRAIT retourner une réponse d'enregistrement au nœud mobile avec un code qui indique la raison de l'erreur. Si un agent étranger a été impliqué dans le relais de la demande, cela permet à l'agent étranger de supprimer son entrée de liste des visiteurs en instance. Aussi, cela informe le nœud mobile de la raison de l'erreur de sorte qu'il peut tenter de réparer l'erreur et produire une autre demande.

On trouvera dans cette section une liste des raisons pour lesquelles un agent de rattachement peut rejeter une demande, et la valeur de code qu'il devrait utiliser dans chaque cas. Voir au paragraphe 3.8.3 les détails de la construction du message de réponse d'enregistrement.

De nombreuses raisons de rejet d'un enregistrement sont de nature administrative. Par exemple, un agent de rattachement peut limiter le nombre d'enregistrements simultanés pour un nœud mobile, en rejetant tout enregistrement qui causerait le dépassement de cette limite, et en retournant une réponse d'enregistrement avec le code 135. De même, un agent de rattachement peut refuser d'accorder le service aux nœuds mobiles qui sont entrés dans des zones de service non autorisées en retournant une réponse d'enregistrement avec le code 129.

Les demandes qui ont des bits non à zéro dans les champs réservés DOIVENT être rejetées avec le code 134 (demande mal formée).

### 3.8.3 Envoi des réponses d'enregistrement

Si l'agent de rattachement accepte une demande d'enregistrement, il DOIT alors mettre à jour son enregistrement du ou des liens de mobilité du nœud mobile et DEVRAIT envoyer une réponse d'enregistrement avec un code convenable. Autrement (l'agent de rattachement a refusé la demande) il DEVRAIT dans la plupart des cas envoyer une réponse d'enregistrement avec un code approprié spécifiant la raison du refus de la demande. Les paragraphes qui suivent donnent des détails supplémentaires sur les valeurs que l'agent de rattachement DOIT fournir dans les champs des messages de réponse d'enregistrement.

#### 3.8.3.1 Champs IP/UDP

Ce paragraphe donne les règles spécifiques de choix par les agents de rattachement des valeurs des champs d'en-tête IP et UDP d'une réponse d'enregistrement.

Adresse IP de source : copiée de l'adresse de destination IP de la demande d'enregistrement, sauf si une adresse de diffusion ou de diffusion groupée a été utilisée. Si l'adresse de destination IP de la demande d'enregistrement était une adresse de diffusion ou de diffusion groupée, l'adresse IP de source de la réponse d'enregistrement DOIT être réglée à l'adresse IP (en envoi individuel) de l'agent de rattachement.

Adresse IP de destination : copiée de l'adresse IP de source de la demande d'enregistrement.

Accès UDP de source : copié de l'accès UDP de destination de la demande d'enregistrement.

Accès UDP de destination : copié de l'accès UDP de source de la demande d'enregistrement.

Lors de l'envoi d'une réponse d'enregistrement en réponse à une demande d'enregistrement qui demandait le désenregistrement du nœud mobile (la durée de vie est zéro et l'adresse d'entretien est égale à l'adresse de rattachement du

nœud mobile) et dans laquelle l'adresse IP de source était aussi réglée à l'adresse de rattachement du nœud mobile (c'est la méthode normale utilisée par un nœud mobile pour se désenregistrer quand il retourne à son réseau de rattachement) l'adresse de destination IP dans la réponse d'enregistrement va être réglée à l'adresse de rattachement du nœud mobile, telle que copiée de l'adresse IP de source de la demande.

Dans ce cas, quand il transmet la réponse d'enregistrement, l'agent de rattachement DOIT transmettre la réponse directement sur le réseau de rattachement comme si le nœud mobile était chez lui, outrepassant toute entrée de liste de lien de mobilité qui pourrait encore exister chez l'agent de rattachement pour le nœud mobile de destination. En particulier, pour un nœud mobile qui retourne chez lui après avoir été enregistré avec une adresse d'entretien, si la nouvelle demande d'enregistrement du nœud mobile n'est pas acceptée par l'agent de rattachement, l'entrée de liste de liens de mobilité pour le nœud mobile va encore indiquer que les datagrammes adressés au nœud mobile devraient être tunnelés à l'adresse d'entretien enregistrée du nœud mobile ; lors de l'envoi de la réponse d'enregistrement indiquant le rejet de cette demande, cette entrée existante de la liste des liens DOIT être ignorée, et l'agent de rattachement DOIT transmettre cette réponse comme si le nœud mobile était chez lui.

#### 3.8.3.2 Champs de réponse d'enregistrement

Ce paragraphe donne les règles spécifiques selon lesquelles les agents de rattachement prennent les valeur des champs de la portion fixe d'une réponse d'enregistrement.

Le champ Code de la réponse d'enregistrement est choisi en accord avec les règles spécifiées dans les paragraphes précédents. Lors d'une réponse à un enregistrement accepté, un agent de rattachement DEVRAIT répondre avec le code 1 si il ne prend pas en charge les enregistrements simultanés.

Le champ Durée de vie DOIT être copié du champ correspondant de la demande d'enregistrement, sauf si la valeur demandée est supérieure à la durée maximum pendant laquelle l'agent de rattachement veut fournir le service demandé. Dans ce cas, la durée de vie DOIT être réglée à la durée pendant laquelle le service va réellement être fourni par l'agent de rattachement. Cette durée de vie réduite DEVRAIT être la durée de vie maximum permise par l'agent de rattachement (pour ce nœud mobile et cette adresse d'entretien).

Si le champ Adresse de rattachement de la demande d'enregistrement est non zéro, il DOIT être copié dans le champ Adresse de rattachement du message de réponse d'enregistrement. Si l'agent de rattachement ne peut pas prendre en charge l'adresse d'envoi individuel non zéro spécifiée dans le champ Adresse de rattachement de la demande d'enregistrement, l'agent de rattachement DOIT alors rejeter la demande d'enregistrement avec un code de 129.

Autrement, si le champ Adresse de rattachement de la demande d'enregistrement est zéro comme spécifié au paragraphe 3.6, l'agent de rattachement DEVRAIT s'arranger pour choisir une adresse de rattachement pour le nœud mobile, et insérer l'adresse choisie dans le champ Adresse de rattachement du message de réponse d'enregistrement. Voir dans la [RFC2794] d'autres détails pertinents dans le cas où les nœuds mobiles s'identifient en utilisant un NAI au lieu de leur adresse IP de rattachement.

Si le champ Agent de rattachement dans la demande d'enregistrement contient une adresse d'envoi individuel de cet agent de rattachement, ce champ DOIT alors être copié dans le champ Agent de rattachement de la réponse d'enregistrement. Autrement, l'agent de rattachement DOIT régler le champ Agent de rattachement dans la réponse d'enregistrement à son adresse d'envoi individuel. Dans ce dernier cas, l'agent de rattachement DOIT rejeter l'enregistrement avec un code convenable (par exemple, le code 136) pour empêcher le nœud mobile d'être éventuellement simultanément enregistré auprès de deux agents de rattachement ou plus.

#### 3.8.3.3 Extensions

Ce paragraphe décrit l'ordre de toutes les extensions IP mobile exigées et facultatives qu'un agent de rattachement ajoute à une réponse d'enregistrement. L'ordre suivant DOIT être respecté :

a. l'en-tête IP, suivi par l'en-tête UDP, suivi par la portion de longueur fixe de la réponse d'enregistrement,
b. si il en est de présentes, toute extension non d'authentification utilisée par le nœud mobile (qui peut ou non aussi être utilisée par l'agent étranger),
c. l'extension Authentification mobile-rattachement,
d. si il en est de présente, toute extension non d'authentification utilisée seulement par l'agent étranger, et
e l'extension Authentification étranger-rattachement, si elle est présente.

Noter que les éléments (a) et (c) DOIVENT apparaître dans chaque réponse d'enregistrement envoyée par l'agent de rattachement. Les éléments (b), (d), et (e) sont facultatifs. Cependant, l'élément (e) DOIT être inclus quand l'agent de rattachement et l'agent étranger partagent une association de sécurité mobile.

# 4. Considérations d'acheminement

Cette section décrit comment les nœuds mobiles, les agents de rattachement, et (éventuellement) les agents étrangers coopèrent pour acheminer les datagrammes depuis/vers les nœuds mobiles qui sont connectés à un réseau étranger. Le nœud mobile informe son agent de rattachement de sa localisation actuelle en utilisant la procédure d'enregistrement décrite à la Section 3. Voir la vue d'ensemble du protocole au paragraphe 1.7 pour les localisations relatives de l'adresse de rattachement du nœud mobile par rapport à son agent de rattachement, et du nœud mobile lui-même par rapport à tout agent étranger auprès duquel il pourrait tenter de s'enregistrer.

## 4.1 Types d'encapsulation

Les agents de rattachement et les agents étrangers DOIVENT prendre en charge le tunnelage des datagrammes en utilisant l'encapsulation IP dans IP [RFC2003]. Tout nœud mobile qui utilise une adresse d'entretien colocalisée DOIT prendre en charge la réception des datagrammes tunnelés en utilisant l'encapsulation IP dans IP. L'encapsulation minimale [RFC2004] et l'encapsulation GRE [RFC2784] sont des méthodes d'encapsulation de remplacement qui PEUVENT être prises en charge par les agents de mobilité et les nœuds mobiles. L'utilisation de ces formes d'encapsulation de remplacement, quand elles sont demandées par le nœud mobile, sont à la discrétion de l'agent de rattachement.

## 4.2 Acheminement de datagramme en envoi individuel

### 4.2.1 Considérations de nœud mobile

Quand il est connecté à son réseau de rattachement, un nœud mobile fonctionne sans le support des services de mobilité. C'est-à-dire qu'il opère de la même façon que tout autre hôte ou routeur (fixe). La méthode par laquelle un nœud mobile choisit un routeur par défaut quand il est connecté à son réseau de rattachement, ou quand il est hors de chez lui et utilise une adresse d'entretien colocalisée, sort du domaine d'application du présent document. Une annonce de routeur ICMP [RFC1256] est une de ces méthodes.

Quand il s'enregistre sur un réseau étranger, le nœud mobile choisit un routeur par défaut selon les règles suivantes :

- Si le nœud mobile est enregistré en utilisant une adresse d'entretien d'agent étranger, il PEUT utiliser son agent étranger comme routeur de premier bond. L'adresse MAC de l'agent étranger peut être apprise du message d'annonce d'agent de l'agent étranger. Autrement, le nœud mobile DOIT choisir son routeur par défaut parmi les adresses de routeur annoncées dans la portion annonce de routeur ICMP de ce message d'annonce d'agent.
- Si le nœud mobile est enregistré directement auprès de son agent de rattachement en utilisant une adresse d'entretien colocalisée, le nœud mobile DEVRAIT alors choisir son routeur par défaut parmi ceux annoncés dans tout message ICMP d'annonce de routeur qu'il reçoit pour laquelle son adresse d'entretien obtenue de l'extérieur et l'adresse du routeur correspondent par le préfixe de réseau. Si l'adresse d'entretien obtenue de l'extérieur du nœud mobile correspond à l'adresse IP de source de l'annonce d'agent sous le préfixe de réseau, le nœud mobile PEUT aussi considérer l'adresse IP de source comme un autre choix possible pour l'adresse IP d'un routeur par défaut. Le préfixe de réseau PEUT être obtenu de l'extension Longueurs de préfixe dans l'annonce de routeur, si elle est présente. Le préfixe PEUT aussi être obtenu par d'autres mécanismes qui sortent du domaine d'application du présent document.

Lorsque ils sont éloignés de leur réseau de rattachement, les nœuds mobiles NE DOIVENT PAS diffuser de paquets ARP pour trouver l'adresse MAC d'un autre nœud Internet. Donc, la liste (éventuellement vide) des adresses de routeur provenant de la portion annonce de routeur ICMP du message n’est pas utile pour choisir un routeur par défaut, sauf si le nœud mobile a des moyens, qui n'impliquent pas de diffusion ARP et non spécifiés dans le présent document, pour obtenir l'adresse MAC d'un des routeurs de la liste. De même, en l'absence de mécanismes non spécifiés pour obtenir les adresses MAC sur les réseaux étrangers, le nœud mobile DOIT ignorer les redirections sur d'autres routeurs sur les réseaux étrangers.

### 4.2.2 Considérations d'agent étranger

À réception d'un datagramme encapsulé envoyé à son adresse d'entretien annoncée, un agent étranger DOIT comparer l'adresse de destination interne aux entrées de sa liste des visiteurs. Quand la destination ne correspond pas à l'adresse d'un nœud mobile de la liste des visiteurs actuelle, l'agent étranger NE DOIT PAS transmettre le datagramme sans modification de l'en-tête IP original, parce que autrement il résultera probablement une boucle d'acheminement. Le datagramme DEVRAIT être éliminé en silence. Le message ICMP "Destination injoignable" NE DOIT PAS être envoyé quand un agent étranger est incapable de transmettre un datagramme entrant tunnelé. Autrement, l'agent étranger transmet le datagramme désencapsulé au nœud mobile.

L'agent étranger NE DOIT PAS annoncer aux autres routeurs de son domaine d'acheminement, ni à aucun autre nœud mobile, la présence d'un routeur mobile (paragraphe 4.5) ou nœud mobile dans sa liste des visiteurs.

L'agent étranger DOIT acheminer les datagrammes qu'il reçoit des nœuds mobiles enregistrés. Au minimum, cela signifie que l'agent étranger doit vérifier la somme de contrôle de l'en-tête IP, décrémenter le TTL IP, recalculer la somme de contrôle d'en-tête IP, et transmettre de tels datagrammes à un routeur par défaut.

Un agent étranger NE DOIT PAS utiliser ARP en diffusion pour l'adresse MAC d'un nœud mobile sur un réseau étranger. Il peut obtenir l'adresse MAC en copiant les informations d'une sollicitation d'agent ou d'une demande d'enregistrement transmise d'un nœud mobile. L'antémémoire ARP d'un agent étranger pour l'adresse IP du nœud mobile NE DOIT PAS être laissée arriver à expiration avant que n'arrive à expiration l'entrée de liste des visiteurs du nœud mobile, sauf si l'agent étranger a un autre moyen que ARP en diffusion pour rafraîchir l'adresse MAC associée à l'adresse IP du nœud mobile.

Chaque agent étranger DEVRAIT prendre en charge les caractéristiques obligatoires pour le tunnelage inverse [RFC3024].

### 4.2.3 Considérations d'agent de rattachement

L'agent de rattachement DOIT être capable d'intercepter tous les datagrammes sur le réseau de rattachement qui sont adressés au nœud mobile lorsque celui-ci est enregistré hors de chez lui. ARP mandataire et ARP gratuit PEUVENT être utilisés pour permettre cette interception, comme spécifié au paragraphe 4.6.

L'agent de rattachement doit examiner l'adresse de destination IP de tout datagramme arrivant pour voir si elle est égale à l'adresse de rattachement d'un des nœuds mobiles enregistrés hors de chez eux. Si il en est ainsi, l'agent de rattachement tunnelle le datagramme à la ou aux adresses d'entretien actuellement enregistrées du nœud mobile. Si l'agent de rattachement prend en charge la capacité facultative de plusieurs liens de mobilité simultanés, il tunnelle une copie à chaque adresse d'entretien de la liste des liens de mobilité du nœud mobile. Si le nœud mobile n'a pas de lien actuel de mobilité, l'agent de rattachement NE DOIT PAS tenter d'intercepter les datagrammes destinés au nœud mobile, et donc ne va en général pas recevoir de tels datagrammes. Cependant, si l'agent de rattachement est aussi un routeur qui traite le trafic IP courant, il est possible qu'il reçoive de tels datagrammes à transmettre sur le réseau de rattachement. Dans ce cas, l'agent de rattachement DOIT supposer que le nœud mobile est chez lui et simplement transmettre le datagramme directement sur le réseau de rattachement.

Pour les agents de rattachement multi rattachements, l'adresse de source dans l'en-tête IP externe du datagramme encapsulé DOIT être l'adresse envoyée au nœud mobile dans le champ Agent de rattachement de la réponse d'enregistrement. C'est-à-dire que l'agent de rattachement ne peut pas utiliser l'adresse d'une autre interface réseau comme adresse de source.

Voir au paragraphe 4.1 les méthodes d'encapsulation qui peuvent être utilisées pour le tunnelage. Les nœuds qui mettent en œuvre le tunnelage DEVRAIENT aussi mettre en œuvre le mécanisme de "tunnel à état conditionnel" [RFC2003], qui permet que les messages d'erreur ICMP retournés du tunnel soient correctement reflétés aux envoyeurs d'origine des datagrammes tunnelés.

Les agents de rattachement DOIVENT désencapsuler les paquets adressés à eux mêmes, envoyés par un nœud mobile pour les besoins de la conservation de la confidentialité de la localisation, comme décrit au paragraphe 5.5. Ce dispositif est aussi requis pour la prise en charge du tunnelage inverse [RFC3024].

Si la durée de vie pour un certain lien de mobilité expire avant que l'agent de rattachement ait reçu une autre demande d'enregistrement valide pour ce nœud mobile, ce lien est alors supprimé de la liste des liens de mobilité. L'agent de rattachement NE DOIT PAS envoyer de message de réponse d'enregistrement simplement parce que le lien du nœud mobile est arrivé à expiration. L'entrée dans la liste des visiteurs de l'agent étranger actuel du nœud mobile va arriver naturellement à expiration, probablement au même moment que le lien chez l'agent de rattachement. Quand la durée de vie d'un lien de mobilité expire, l'agent de rattachement DOIT supprimer le lien, mais il DOIT conserver tous les autres liens de mobilité simultanés (non expirés) qu'il détient pour ce nœud mobile.

Quand il reçoit un datagramme, intercepté pour un de ses nœuds mobiles enregistrés hors de chez eux, l'agent de rattachement DOIT examiner le datagramme pour vérifier si il est déjà encapsulé. Si il l'est, des règles particulières s'appliquent à la transmission de ce datagramme au nœud mobile :

- Si l'adresse de destination interne (encapsulée) est la même que l'adresse de destination externe (le nœud mobile) alors l'agent de rattachement DOIT aussi examiner l'adresse de source externe du datagramme encapsulé (l'adresse de source du tunnel). Si cette adresse de source externe est la même que l'adresse d'entretien actuelle du nœud mobile, l'agent de rattachement DOIT éliminer en silence ce datagramme afin d'empêcher une probable boucle d'acheminement. Si, l'adresse de source externe N'EST PAS la même que l'adresse d'entretien actuelle du nœud mobile, l'agent de rattachement DEVRAIT alors transmettre le datagramme au nœud mobile. Afin de transmettre le datagramme dans ce

cas, l'agent de rattachement PEUT simplement altérer l'adresse de destination externe en l'adresse d'entretien, plutôt que de réencapsuler le datagramme.

- Autrement (l'adresse de destination interne NEST PAS la même que l'adresse de destination externe) l'agent de rattachement DEVRAIT encapsuler à nouveau le datagramme (encapsulation incorporée) avec la nouvelle adresse de destination externe réglée égale à l'adresse d'entretien du nœud mobile. C'est-à-dire que l'agent de rattachement transmet le datagramme entier au nœud mobile de la même façon que tout autre datagramme (déjà encapsulé ou non).

### 4.3 Datagrammes en diffusion

Quand un agent de rattachement reçoit un datagramme en diffusion, il NE DOIT le transmettre à aucun nœud mobile de sa liste de liens de mobilité autre que ceux qui ont demandé la transmission des datagrammes en diffusion. Un nœud mobile PEUT demander la transmission des datagrammes en diffusion en établissant le bit "B" dans son message Demande d'enregistrement (paragraphe 3.3). Pour chacun de ces nœuds mobiles enregistrés, l'agent de rattachement DEVRAIT transmettre les datagrammes en diffusion reçus au nœud mobile, bien que ce soit une question de configuration chez l'agent de rattachement de savoir quelles catégories spécifiques de datagrammes en diffusion vont être transmises à de tels nœuds mobiles.

Si le bit "D" était établi dans le message Demande d'enregistrement du nœud mobile, indiquant que le nœud mobile utilise une adresse d'entretien colocalisée, l'agent de rattachement tunnelle simplement les datagrammes en diffusion appropriés à l'adresse d'entretien du nœud mobile. Autrement (le bit "D" N'était PAS établi) l'agent de rattachement encapsule d'abord le datagramme en diffusion dans un datagramme en envoi individuel adressé à l'adresse de rattachement du nœud mobile, et ensuite tunnelle ce datagramme encapsulé à l'agent étranger. Ce niveau supplémentaire d'encapsulation est exigé afin que l'agent étranger puisse déterminer quel nœud mobile devrait recevoir le datagramme après qu'il sera désencapsulé. Quand il est reçu par l'agent étranger, le datagramme encapsulé en envoi individuel est détunnelé et livré au nœud mobile de la même façon que tout autre datagramme. Dans l'un et l'autre cas, le nœud mobile doit désencapsuler le datagramme qu'il reçoit afin de récupérer le datagramme en diffusion d'origine.

### 4.4 Acheminement de datagramme en diffusion groupée

Comme mentionné précédemment, un nœud mobile connecté à son réseau de rattachement fonctionne de la même façon que tout autre hôte ou routeur (fixe). Donc, quand il est chez lui, un nœud mobile fonctionne d'une façon identique aux autres envoyeurs et receveurs de diffusion groupée. Ce paragraphe décrit donc le comportement d'un nœud mobile qui visite un réseau étranger.

Afin de recevoir des messages en diffusion groupée, un nœud mobile DOIT se joindre au groupe de diffusion groupée d'une des deux façons suivantes. Premièrement, un nœud mobile PEUT se joindre au groupe via un routeur de diffusion groupée (local) sur le sous réseau visité. Cette option suppose qu'un routeur de diffusion groupée est présent sur le sous réseau visité. Si le nœud mobile utilise une adresse d'entretien colocalisée, il DEVRAIT utiliser cette adresse comme adresse IP de source de ses messages IGMP [RFC1112]. Autrement, il PEUT utiliser son adresse de rattachement. Autrement, un nœud mobile qui souhaite recevoir des messages en diffusion groupée PEUT se joindre à des groupes via un tunnel bidirectionnel à son agent de rattachement, en supposant que son agent de rattachement soit un routeur de diffusion groupée. Le nœud mobile tunnelle les messages IGMP à son agent de rattachement, et l'agent de rattachement transmet les datagrammes en diffusion groupée sur le tunnel au nœud mobile. Pour les paquets tunnelés à l'agent de rattachement, l'adresse de source dans l'en-tête IP DEVRAIT être l'adresse de rattachement du nœud mobile.

Les règles pour la livraison de datagrammes en diffusion groupée aux nœuds mobiles sont dans ce cas identiques à celles pour les datagrammes en diffusion (paragraphe 4.3). À savoir que si le nœud mobile utilise une adresse d'entretien colocalisée (le bit "D" était établi dans la demande d'enregistrement du nœud mobile) alors l'agent de rattachement DEVRAIT tunneler le datagramme à cette adresse d'entretien ; autrement, l'agent de rattachement DOIT d'abord encapsuler le datagramme dans un datagramme en envoi individuel adressé à l'adresse de rattachement du nœud mobile et ensuite DOIT tunneler le datagramme résultant (tunnelage incorporé) à l'adresse d'entretien du nœud mobile. Pour cette raison, le nœud mobile DOIT être capable de désencapsuler les paquets envoyés à son adresse de rattachement afin de recevoir les datagrammes en diffusion groupée en utilisant cette méthode.

Un nœud mobile qui souhaite envoyer des datagrammes à un groupe de diffusion groupée a aussi deux options : (1) envoyer directement sur le réseau visité, ou (2) envoyer via un tunnel à son agent de rattachement. Comme en général l'acheminement de diffusion groupée dépend de l'adresse IP de source, un nœud mobile qui envoie des datagrammes en diffusion groupée directement sur le réseau visité DOIT utiliser une adresse d'entretien colocalisée comme adresse IP de source. De même, un nœud mobile qui tunnelle un datagramme en diffusion groupée à son agent de rattachement DOIT utiliser son adresse de rattachement comme adresse IP de source des deux datagrammes de diffusion groupée (interne) et encapsulant (externe). Cette seconde option suppose que l'agent de rattachement est un routeur de diffusion groupée.

### 4.5 Routeurs mobiles

Un nœud mobile peut être un routeur responsable de la mobilité d'un ou plusieurs réseaux entiers bougeant ensemble, peut-être sur un avion, un bateau, un train, une automobile, une bicyclette, ou un kayak. Les nœuds connectés à un réseau desservi par le routeur mobile peuvent eux-mêmes être des nœuds fixes ou des nœuds mobiles ou des routeurs. Dans le présent document, de tels réseaux sont appelés des "réseaux mobiles".

Un routeur mobile PEUT agir comme agent étranger et fournir une adresse d'entretien d'agent étranger aux nœuds mobiles connectés au réseau mobile. L'acheminement normal pour un nœud mobile via un routeur mobile est illustré dans ce cas par l'exemple suivant :

a. un ordinateur portable est déconnecté de son réseau de rattachement et plus tard rattaché à un accès réseau dans le siège arrière d'un avion. L'ordinateur portable utilise IP mobile pour s'enregistrer sur ce réseau étranger, en utilisant une adresse d'entretien d'agent étranger découverte par une annonce d'agent provenant de l'agent étranger de l'avion.
b. Le réseau de l'avion est lui-même mobile. Supposons que le nœud qui sert d'agent étranger sur l'avion serve aussi de routeur par défaut qui connecte le réseau de l'avion au reste de l'Internet. Quand l'avion est chez lui, ce routeur est rattaché à un réseau fixe au siège de la compagnie d'aviation, qui est le réseau de rattachement du routeur. Lorsque l'avion est en vol, ce routeur s'enregistre de temps en temps sur sa liaison radio avec une série d'agents étrangers au sol en dessous de lui. Cet agent de rattachement de routeur est un nœud sur le réseau fixe au siège de la compagnie aérienne.
c. Si un nœud correspondant envoie un datagramme à l'ordinateur portable, adressant le datagramme à l'adresse de rattachement de l'ordinateur portable, ce datagramme est initialement acheminé au réseau de rattachement de l'ordinateur portable.
d. L'agent de rattachement de l'ordinateur portable intercepte le datagramme sur le réseau de rattachement et le tunnelle à l'adresse d'entretien de l'ordinateur portable, qui dans cet exemple est une adresse du nœud qui sert de routeur et d'agent étranger sur l'avion. L'acheminement IP normal va acheminer le datagramme au réseau fixe du siège de la compagnie d'aviation.
e. Le routeur de l'avion et l'agent de rattachement de l'agent étranger interceptent alors le datagramme et le tunnellent à son adresse d'entretien actuelle, qui dans cet exemple est un agent étranger sur le sol en dessous de l'avion. Le datagramme d'origine provenant du nœud correspondant a maintenant été encapsulé deux fois : une fois par l'agent de rattachement de l'ordinateur portable et une fois encore par l'agent de rattachement de l'avion.
f. L'agent étranger au sol désencapsule le datagramme, donnant un datagramme toujours encapsulé par l'agent de rattachement de l'ordinateur, avec une adresse de destination qui est l'adresse d'entretien de l'ordinateur. L'agent étranger au sol envoie le datagramme résultant sur sa liaison radio à l'avion.
g. L'agent étranger sur l'avion désencapsule le datagramme, donnant le datagramme original du nœud correspondant, avec une adresse de destination qui est l'adresse de rattachement de l'ordinateur portable. L'agent étranger de l'avion livre le datagramme sur le réseau de l'avion à l'adresse de couche de liaison de l'ordinateur portable.

Cet exemple illustre le cas où un nœud mobile est rattaché à un réseau mobile. C'est-à-dire que le nœud mobile est mobile par rapport au réseau, qui est aussi lui-même mobile (ici par rapport au sol). Si, à la place, le nœud est fixe par rapport au réseau mobile (le réseau mobile est le réseau de rattachement du nœud fixe) alors l'une ou l'autre des deux méthodes peut être utilisée pour causer l'acheminement des datagrammes des nœuds correspondants au nœud fixe.

Pour le nœud fixe, un agent de rattachement PEUT être configuré à avoir un enregistrement permanent qui indique l'adresse du routeur mobile comme adresse d'entretien de l'hôte fixe. L'agent de rattachement du routeur mobile va normalement être utilisé à cette fin. L'agent de rattachement est alors chargé d'annoncer au nœud fixe la connexité en utilisant les protocoles normaux d'acheminement. Tous les datagrammes envoyés au nœud fixe vont donc utiliser le tunnelage incorporé décrit ci-dessus.

Autrement, le routeur mobile PEUT annoncer la connexité au réseau mobile entier en utilisant les protocoles normaux d'acheminement IP à travers un tunnel bidirectionnel à son propre agent de rattachement. Cette méthode évite le besoin d'un tunnelage incorporé des datagrammes.

### 4.6 ARP, mandataire ARP, et ARP gratuit

L'utilisation de ARP [RFC0826] exige des règles particulières pour un fonctionnement correct quand des nœuds sans fil mobiles sont impliqués. Les exigences spécifiées dans ce paragraphe s'appliquent à tous les réseaux de rattachement dans lesquels ARP est utilisé pour la résolution d'adresse.

En plus de l'utilisation normale d'ARP pour résoudre l'adresse de couche de liaison du nœud cible à partir de son adresse IP, le présent document distingue deux utilisations particulières de ARP :

o Un ARP mandataire [RFC0925] est une réponse ARP envoyée par un nœud au nom d'un autre nœud qui est incapable de répondre, ou ne veut pas répondre, à ses propres demandes ARP. L'envoyeur d'un ARP mandataire inverse les champs d'adresse de protocole d'envoyeur et de cible comme décrit dans la [RFC0826], mais fournit une adresse

configurée de couche de liaison (généralement, la sienne) dans le champ Adresse de matériel envoyeur. Le nœud qui reçoit la réponse va alors associer cette adresse de couche de liaison à l'adresse IP du nœud cible original, causant la transmission des futurs datagrammes pour ce nœud cible au nœud qui a cette adresse de couche de liaison.

- Un ARP gratuit [TCP/IP] est un paquet ARP envoyé par un nœud afin de causer la mise à jour spontanée par les autres nœuds d'une entrée dans leur antémémoire ARP. Un ARP gratuit PEUT utiliser un paquet de demande ou de réponse ARP. Dans les deux cas, l'adresse de protocole d'envoyeur ARP et l'adresse de protocole cible ARP sont toutes deux réglées à l'adresse IP de l'entrée d'antémémoire à mettre à jour, et l'adresse de matériel d'envoyeur ARP est réglée à l'adresse de couche de liaison à laquelle cette entrée d'antémémoire devrait être mise à jour. Quand on utilise un paquet de réponse ARP, l'adresse de matériel cible est aussi réglée à l'adresse de couche de liaison à laquelle cette entrée d'antémémoire devrait être mise à jour (ce champ n'est pas utilisé dans un paquet de demande ARP).

Dans l'un et l'autre cas, pour un ARP gratuit, le paquet ARP DOIT être transmis comme un paquet de diffusion locale sur la liaison locale. Comme spécifié dans la [RFC0826], tout nœud qui reçoit un paquet ARP (demande ou réponse) DOIT mettre à jour son antémémoire ARP locale avec les adresses d'envoyeur de protocole et de matériel dans le paquet ARP, si le nœud receveur a déjà une entrée pour cette adresse IP dans son antémémoire ARP. Cette exigence dans le protocole ARP s'applique même pour les paquets de demande ARP, et pour les paquets de réponse ARP qui ne correspondent à aucune demande ARP transmise par le nœud receveur [RFC0826].

Lorsque un nœud mobile est enregistré sur un réseau étranger, son agent de rattachement utilise un mandataire ARP [RFC0925] pour répondre aux demandes ARP qu'il reçoit qui cherchent l'adresse de couche de liaison du nœud mobile. Quand il reçoit une demande ARP, l'agent de rattachement DOIT examiner l'adresse IP cible de la demande, et si cette adresse IP correspond à l'adresse de rattachement d'un nœud mobile pour lequel il a enregistré un lien de mobilité, l'agent de rattachement DOIT transmettre une réponse ARP au nom du nœud mobile. Après l'échange des adresses d'envoyeur et de cible dans le paquet [RFC0925], l'agent de rattachement DOIT régler l'adresse de couche de liaison de l'envoyeur dans le paquet à l'adresse de couche de liaison de sa propre interface sur laquelle la réponse va être envoyée.

Quand un nœud mobile laisse son réseau de rattachement et enregistre un lien sur un réseau étranger, son agent de rattachement utilise ARP gratuit pour mettre à jour les antémémoires ARP des nœuds sur le réseau de rattachement. Cela cause l'association par ces nœuds de l'adresse de couche de liaison de l'agent de rattachement à l'adresse (IP) de rattachement du nœud mobile. Quand il enregistre un lien pour un nœud mobile pour lequel l'agent de rattachement n'avait précédemment pas de lien (le nœud mobile était supposé être chez lui) l'agent de rattachement DOIT transmettre un ARP gratuit au nom du nœud mobile. Ce paquet ARP gratuit DOIT être transmis comme paquet en diffusion sur la liaison sur laquelle est située l'adresse de rattachement du nœud mobile. Comme il n'est généralement pas garanti que les diffusions sur la liaison locale (comme Ethernet) soient fiables, le paquet ARP gratuit DEVRAIT être retransmis un petit nombre de fois pour augmenter sa fiabilité.

Quand un nœud mobile retourne à son réseau de rattachement, le nœud mobile et son agent de rattachement utilisent ARP gratuit pour faire que tous les nœuds sur le réseau de rattachement du nœud mobile mettent à jour leurs antémémoires ARP pour associer une fois encore la propre adresse de couche de liaison du nœud mobile à l'adresse (IP) de rattachement du nœud mobile. Avant de transmettre le message de demande d'enregistrement/désenregistrement à son agent de rattachement, le nœud mobile DOIT transmettre des ARP gratuits sur son réseau de rattachement comme une diffusion locale sur cette liaison. Le paquet ARP gratuit DEVRAIT être retransmis un petit nombre de fois pour augmenter sa fiabilité, mais ces retransmissions DEVRAIT se faire en parallèle avec la transmission et le traitement de la demande d'enregistrement/désenregistrement du nœud mobile.

Quand l'agent de rattachement du nœud mobile reçoit et accepte cette demande d'enregistrement/désenregistrement, l'agent de rattachement DOIT aussi transmettre un ARP gratuit sur le réseau de rattachement du nœud mobile. Cet ARP gratuit est aussi utilisé pour associer l'adresse de rattachement du nœud mobile à la propre adresse de couche de liaison du nœud mobile. Un ARP gratuit est transmis par le nœud mobile et par son agent de rattachement, car dans le cas d'interfaces de réseau sans fil, la zone de transmission du nœud mobile va probablement différer de celle de son agent de rattachement. Le paquet ARP provenant de l'agent de rattachement DOIT être transmis comme diffusion locale sur la liaison de rattachement du nœud mobile, et DEVRAIT être retransmis un petit nombre de fois pour augmenter sa fiabilité ; ces retransmissions DEVRAIENT cependant se faire en parallèle avec la transmission et le traitement de la réponse d'enregistrement/désenregistrement du nœud mobile.

Lorsque le nœud mobile est hors de chez lui, il NE DOIT PAS transmettre de messages de demande ou réponse ARP en diffusion. Finalement, lorsque le nœud mobile est hors de chez lui, il NE DOIT PAS répondre aux demandes ARP dans lesquelles l'adresse IP cible est sa propre adresse de rattachement sauf si la demande ARP est en envoi individuel par un agent étranger avec lequel le nœud mobile tente de s'enregistrer ou un agent étranger avec lequel le nœud mobile a un enregistrement non arrivé à expiration. Dans ce dernier cas, le nœud mobile DOIT utiliser une réponse ARP en envoi individuel pour répondre à l'agent étranger. Noter que si le nœud mobile utilise une adresse d'entretien colocalisée et reçoit une demande ARP dans laquelle l'adresse IP cible est cette adresse d'entretien, le nœud mobile DEVRAIT alors répondre à cette demande ARP. Noter aussi que, quand il transmet une demande d'enregistrement sur un réseau étranger, un nœud

mobile peut découvrir l'adresse de couche de liaison d'un agent étranger en mémorisant l'adresse comme elle est reçue de l'annonce d'agent provenant de cet agent étranger, mais non en transmettant un message de demande ARP en diffusion.

L'ordre spécifique dans lequel sont appliquées les exigences ci-dessus pour l'utilisation de ARP, de ARP mandataire, et de ARP gratuit, relativement à la transmission et au traitement des messages de demande et réponse d'enregistrement de nœud mobile quand il quitte ou revient à son réseau de rattachement, est important pour le fonctionnement correct du protocole.

Pour résumer les exigences ci-dessus, quand un nœud mobile quitte son réseau de rattachement, les étapes suivantes DOIVENT être suivies dans l'ordre indiqué :

- o le nœud mobile décide de s'enregistrer hors de chez lui, peut-être parce que il a reçu une annonce d'agent d'un agent étranger et n'en a pas reçu récemment de son agent de rattachement ;
- o avant de transmettre la demande d'enregistrement, le nœud mobile désactive son propre futur traitement de toutes les demandes ARP qu'il pourrait ultérieurement recevoir lui demandant l'adresse de couche de liaison correspondant à son adresse de rattachement, sauf autant que nécessaire pour communiquer avec les agents étrangers sur les réseaux visités ;
- o le nœud mobile transmet sa demande d'enregistrement ;
- o quand l'agent de rattachement du nœud mobile reçoit et accepte la demande d'enregistrement, il effectue un ARP gratuit au nom du nœud mobile, et commence à utiliser ARP mandataire pour répondre aux demandes ARP qu'il reçoit et qui demandent l'adresse de couche de liaison du nœud mobile. Dans l'ARP gratuit, l'adresse du matériel envoyeur ARP est réglée à l'adresse de couche de liaison de l'agent de rattachement. Si, au lieu de cela, l'agent de rattachement rejette la demande d'enregistrement, aucun traitement ARP (ni gratuit ni mandataire) n'est effectué par l'agent de rattachement.

Quand un nœud mobile retourne ultérieurement à son réseau de rattachement, les étapes qui suivent DOIVENT être effectuées dans cet ordre :

- o le nœud mobile décide de s'enregistrer chez lui, peut-être parce que il a reçu une annonce d'agent de son agent de rattachement ;
- o avant de transmettre la demande d'enregistrement, le nœud mobile réactive son propre futur traitement des demandes ARP qu'il pourrait ultérieurement recevoir pour lui demander son adresse de couche de liaison ;
- o le nœud mobile effectue un ARP gratuit pour lui-même. Dans cet ARP gratuit, l'adresse de matériel envoyeur ARP est réglée à l'adresse de couche de liaison du nœud mobile ;
- o le nœud mobile transmet sa demande d'enregistrement ;
- o quand l'agent de rattachement du nœud mobile reçoit et accepte la demande d'enregistrement, il arrête d'utiliser l'ARP mandataire pour répondre aux demandes ARP qu'il reçoit et qui demandent l'adresse de couche de liaison du nœud mobile, et effectue ensuite un ARP gratuit au nom du nœud mobile. Dans cet ARP gratuit, l'adresse de matériel d'envoyeur ARP est réglée à l'adresse de couche de liaison du nœud mobile. Si au lieu de cela, l'agent de rattachement rejette la demande d'enregistrement, l'agent de rattachement NE DOIT PAS changer sa façon d'effectuer le traitement d'ARP (ni gratuit ni mandataire) pour le nœud mobile. Dans ce dernier cas, l'agent de rattachement devrait opérer comme si le nœud mobile n'était pas retourné chez lui, et continuer d'effectuer l'ARP mandataire au nom du nœud mobile.

## 5. Considérations sur la sécurité

L'environnement de calcul mobile est potentiellement très différent de l'environnement de calcul ordinaire. Dans de nombreux cas, l'ordinateur mobile va être connecté au réseau via des liaisons sans fil. De telles liaisons sont particulièrement vulnérables à l'espionnage passif, aux attaques actives de répétition, et autres attaques actives.

### 5.1 Codes d'authentification de message

Les agents de rattachement et les nœuds mobiles DOIVENT être capables d'effectuer l'authentification. L'algorithme par défaut est HMAC-MD5 [RFC2104], avec une taille de clé de 128 bits. L'agent étranger DOIT aussi prendre en charge l'authentification utilisant HMAC-MD5 et les tailles de clés de 128 bits ou plus, avec une distribution de clé manuelle. Les clés avec des valeurs binaires arbitraires DOIVENT être acceptées.

L'utilisation "préfixe + suffixe" de MD5 pour protéger les données et un secret partagé est considérée comme vulnérable à l'attaque par la communauté cryptographique. Lorsque la rétro compatibilité avec les mises en œuvre existantes de IP mobile qui utilisent ce mode est nécessaire, les nouvelles mises en œuvre DEVRAIENT inclure MD5 chiffré [RFC1321] comme un des algorithmes d'authentification supplémentaires à utiliser lors de la production et vérification des données d'authentification qui sont fournies avec les messages d'enregistrement IP mobile, par exemple, dans les extensions spécifiées aux paragraphes 3.5.2, 3.5.3, et 3.5.4.

Plus d'algorithmes d'authentification, de modes d'algorithmes, de méthodes de distribution de clés, et tailles de clés PEUVENT aussi être pris en charge pour toutes ces extensions.

### 5.2 Étendue des problèmes de sécurité concernant ce protocole

Le protocole d'enregistrement décrit dans le présent document aura pour résultat que le trafic d'un nœud mobile sera tunnelé à son adresse d'entretien. Cette caractéristique de tunnelage pourrait être une vulnérabilité significative si l'enregistrement n'était pas authentifié. Comme la redirection à distance, par exemple, telle qu'elle est effectuée par le protocole d'enregistrement mobile, est largement comprise comme étant un problème de sécurité dans l'Internet actuel si il n'est pas authentifié [TCPIP]. De plus, le protocole de résolution d'adresse (ARP, *Address Resolution Protocol*) n'est pas authentifié, et peut éventuellement être utilisé pour voler le trafic d'un autre hôte. L'utilisation de ARP gratuit (paragraphe 4.6) comporte tous les risques associés à l'utilisation de ARP.

### 5.3 Gestion des clés

La présente spécification exige un fort mécanisme d'authentification (MD5 chiffré) qui empêche toutes les nombreuses attaques potentielles qui se fondent sur le protocole d'enregistrement IP mobile. Cependant, parce que la distribution de clés est difficile en l'absence d'un protocole de gestion des clés de réseau, il n'est pas exigé que tous les messages avec l'agent étranger soient authentifiés. Dans un environnement commercial, il peut être important d'authentifier tous les messages entre l'agent étranger et l'agent de rattachement, de sorte que la facturation soit possible et que les fournisseurs de service ne fournissent pas de service aux usagers qui ne sont pas des consommateurs légitimes de ce fournisseur.

### 5.4 Choix de bons nombres aléatoires

La force de tout mécanisme d'authentification dépend de plusieurs facteurs, parmi lesquels la force intrinsèque de l'algorithme d'authentification, le secret de la clé utilisée, la force de la clé utilisée, et la qualité de la mise en œuvre. La présente spécification exige la mise en œuvre de MD5 chiffré pour l'authentification, mais n'empêche pas l'utilisation d'autres algorithmes et modes d'authentification. Pour que l'authentification MD5 chiffré soit utile, la clé de 128 bits doit être à la fois secrète (c'est-à-dire, connue des seules parties autorisées) et pseudo aléatoire.

Si des noms occasionnels sont utilisés en connexion avec la protection contre la répétition, ils doivent aussi être choisis avec soin. La [RFC4086] écrite par Eastlake, et autres, donne plus d'informations sur la génération des nombres pseudo aléatoires.

### 5.5 Confidentialité

Les utilisateurs qui ont des données sensibles qu'ils ne veulent pas faire voir à d'autres devraient utiliser des mécanismes qui sortent du domaine d'application du présent document (comme le chiffrement) pour fournir la protection appropriée. Les utilisateurs qui se soucient de l'analyse de trafic devraient envisager l'utilisation appropriée du chiffrement de liaison. Si la confidentialité absolue de la localisation est désirée, le nœud mobile peut créer un tunnel vers son agent de rattachement. Les datagrammes destinés aux nœuds correspondants vont paraître émaner du réseau de rattachement, et il peut être plus difficile de déterminer la localisation du nœud mobile. De tels mécanismes sortent tous du domaine d'application du présent document.

### 5.6 Filtrage d'entrée

De nombreux routeurs mettent en œuvre des politiques de sécurité telles que le "filtrage d'entrée" [RFC2827] qui ne permettent pas la transmission des paquets qui ont une adresse de source qui apparaît comme topologiquement incorrecte. Dans des environnements où cela pose un problème, les nœuds mobiles peuvent utiliser le tunnelage inverse [RFC3024] avec l'adresse d'entretien fournie par l'agent étranger comme adresse de source. Les paquets qui font l'objet d'un tunnelage inverse seront capables de passer normalement à travers de tels routeurs, tandis que les règles de filtrage d'entrée vont quand même être capables de localiser la vraie source topologique du paquet de la même façon que pour les paquets provenant de nœuds non mobiles.

### 5.7 Protection contre la répétition pour les demandes d'enregistrement

Le champ Identification est utilisé pour permettre à l'agent de rattachement de vérifier qu'un message d'enregistrement a été fraîchement généré par le nœud mobile, et non répété par un attaquant à partir d'un enregistrement précédent. Deux méthodes sont décrites dans cette section : les horodatages (obligatoires) et les "noms occasionnels" (facultatifs). Tous les nœuds mobiles et agents de rattachement DOIVENT mettre en œuvre la protection contre la répétition fondée sur l'horodatage. Ces nœuds PEUVENT aussi mettre en œuvre la protection contre la répétition fondée sur le nom occasionnel.

Le style de protection contre la répétition entre un nœud mobile et son agent de rattachement fait partie de l'association de sécurité mobile. Un nœud mobile et son agent de rattachement DOIVENT s'accorder sur la méthode de protection qui va être utilisée. L'interprétation du champ Identification dépend de la méthode de protection contre la répétition comme décrit dans les paragraphes qui suivent.

Quelle que soit la méthode utilisée, les 32 bits de moindre poids du champ Identification DOIVENT être copiés inchangés de la demande d'enregistrement à la réponse. L'agent étranger utilise ces bits (et l'adresse de rattachement du nœud mobile) pour confronter les demandes d'enregistrement aux réponses correspondantes. Le nœud mobile DOIT vérifier que les 32 bits de moindre poids de toute réponse d'enregistrement sont identiques aux bits qu'il a envoyés dans la demande d'enregistrement.

Le champ Identification dans une nouvelle demande d'enregistrement NE DOIT PAS être le même que dans une demande qui la précède immédiatement, et NE DEVRAIT PAS se répéter alors que le même contexte de sécurité est utilisé entre le nœud mobile et l'agent de rattachement. La retransmission comme au paragraphe 3.6.3 est permise.

### 5.7.1 Protection contre la répétition avec des horodatages

Le principe de base de la protection contre la répétition par horodatage est que le nœud qui génère un message insère l'heure courante, et le nœud qui reçoit le message vérifie que cet horodatage est suffisamment proche de sa propre heure. Sauf spécification contraire dans l'association de sécurité entre les nœuds, une valeur par défaut de 7 secondes PEUT être utilisée pour limiter la différence d'heure. Cette valeur DEVRAIT être supérieure de 3 secondes. Évidemment, les deux nœuds doivent avoir adéquatement synchronisé l'heure de leurs horloges. Comme avec tous les messages, les messages de synchronisation de l'heure peuvent être protégés contre l'altération par un mécanisme d'authentification déterminé par le contexte de sécurité entre les deux nœuds.

Si les horodatages sont utilisés, le nœud mobile DOIT régler le champ Identification à une valeur de 64 bits formatée comme spécifié par le protocole de l'heure du réseau [RFC5905]. Les 32 bits de moindre poids du format NTP représentent les fractions de secondes, et ces bits qui ne sont pas disponibles à partir d'une source horaire DEVRAIENT être générés à partir d'une bonne source d'aléa. Noter, cependant, que quand on utilise les horodatages, les 64 bits d'identification utilisés dans une demande d'enregistrement provenant du nœud mobile DOIVENT être supérieurs à ceux utilisés dans toute demande d’enregistrement antérieure, car l'agent de rattachement utilise cette valeur comme un numéro de séquence. Sans un tel numéro de séquence, il serait possible à un duplicata retardé d'une demande d'enregistrement antérieure d'arriver à l'agent de rattachement (dans le délai de synchronisation d'horloge exigé par l'agent de rattachement) et donc d'être appliqué décalé, altérant de façon erronée l'adresse d'entretien courante du nœud mobile.

À réception d'une demande d'enregistrement avec une extension d'activation d'autorisation, l'agent de rattachement DOIT vérifier la validité du champ Identification. Afin d'être valide, l'horodatage contenu dans le champ Identification DOIT être assez proche de l’heure de l'horloge de l'agent de rattachement, et l'horodatage DOIT être supérieur à tous les horodatages acceptés précédemment pour ce nœud mobile demandeur. Les tolérances d'heure et les détails de resynchronisation sont spécifiques d'une association de sécurité mobile particulière.

Si l'horodatage est valide, l'agent de rattachement copie le champ Identification entier dans la réponse d'enregistrement qu'il retourne au nœud mobile. Si l'horodatage n'est pas valide, l'agent de rattachement copie seulement les 32 bits de moindre poids dans la réponse d'enregistrement, et fournit les 32 bits de poids fort de sa propre heure. Dans ce dernier cas, l'agent de rattachement DOIT rejeter l'enregistrement en retournant le code 133 (Discordance d'identification d'enregistrement) dans la réponse d'enregistrement.

Comme décrit au paragraphe 3.6.2.1, le nœud mobile DOIT vérifier que les 32 bits de moindre poids du champ Identification dans la réponse d'enregistrement sont identiques à ceux de la tentative d'enregistrement rejetée, avant d'utiliser les bits de poids fort pour la resynchronisation des horloges.

### 5.7.2 Protection contre la répétition avec des noms occasionnels

Le principe de base de la protection contre la répétition par un nom occasionnel est que le nœud A inclut un nouveau nombre aléatoire dans chaque message au nœud B, et vérifie que le nœud B retourne ce même nombre dans son prochain message au nœud A. Les deux messages utilisent un code d'authentification pour la protection contre l'altération par un attaquant. En même temps, le nœud B peut envoyer ses propres noms occasionnels dans tous les messages au nœud A (pour que le nœud A les renvoie en écho) de sorte qu'il puisse aussi vérifier qu'il reçoit des messages frais.

L'agent de rattachement peut être supposé avoir des ressources pour calculer des nombres pseudo aléatoires utilisés comme noms occasionnels [RFC4086]. Il insère un nouveau nom occasionnel comme les 32 bits de poids fort du champ

Identification de chaque réponse d'enregistrement. L'agent de rattachement copie les 32 bits de moindre poids du champ Identification provenant du message Demande d'enregistrement dans les 32 bits de moindre poids du champ Identification de la réponse d'enregistrement. Quand le nœud mobile reçoit une réponse d'enregistrement authentifiée de l'agent de rattachement, il sauvegarde les 32 bits de poids fort du champ Identification pour les utiliser comme les 32 bits de poids fort de sa prochaine demande d'enregistrement.

Le nœud mobile est responsable de la génération des 32 bits de moindre poids du champ Identification de chaque demande d'enregistrement. Idéalement, il devrait générer ses propres noms occasionnels aléatoires. Cependant, il peut utiliser toute méthode convenable, y compris la duplication de la valeur aléatoire envoyée par l'agent de rattachement. La méthode choisie est de la seule compétence du nœud mobile, parce que il est le nœud qui vérifie les valeurs valides dans la réponse d'enregistrement. Les valeurs des 32 bits de poids fort et de moindre poids de l'identification choisie DEVRAIENT toutes deux différer de leurs valeurs précédentes. L'agent de rattachement utilise une nouvelle valeur des bits de poids fort, et le nœud mobile utilise une nouvelle valeur de bits de moindre poids pour chaque message d'enregistrement. L'agent étranger utilise la valeur de moindre poids (et l'adresse de rattachement de l'hôte mobile) pour faire correspondre correctement les réponses d'enregistrement avec les demandes en instance (paragraphe 3.7.1).

Si un message d'enregistrement est rejeté parce que le nom occasionnel est invalide, la réponse fournit toujours au nœud mobile un nouveau nom occasionnel à utiliser dans le prochain enregistrement. Donc, le protocole de nom occasionnel est auto synchronisé.

## 6. Considérations relatives à l'IANA

IP mobile spécifie plusieurs nouveaux espaces de nombres pour les valeurs à utiliser dans divers champs de messages. Ces espaces de nombres incluent :

- Les types de messages IP mobile envoyés à l'accès UDP 434, comme défini au paragraphe 1.8.
- Les types d'extensions aux messages de demande et réponse d'enregistrement (voir les paragraphes 3.3 et 3.4, et aussi consulter les [RFC3024], [RFC2356], [RFC2794], [RFC4721], et [RFC3115]).
- Les valeurs pour le code dans le message de réponse d'enregistrement (voir au paragraphe 3.4, et aussi consulter les [RFC3024], [RFC2356], [RFC2794], [RFC4721], et [RFC3115]).
- IP mobile définit des messages de sollicitation d'agent et d'annonce d'agent. Ces messages sont en fait des messages de découverte de routeur [RFC1256] augmentés par des extensions spécifiques de IP mobile. Donc, il ne définit pas un nouvel espace de noms, mais définit des extensions supplémentaires de découverte de routeur comme décrit au paragraphe 6.2. Voir aussi le paragraphe 2.1, et consulter les [RFC4721] et [RFC3115].

Ce sont les espaces supplémentaires de numérotation IP mobile spécifiés dans la [RFC4721].

Des informations sur les allocations de numéros IP mobile déduites de spécifications externes au présent document sont données par l'IANA à http://www.iana.org/protocols. À partir de cet URL, voir la section "Mobile Internet Protocol (IP) Numbers".

Dans cette spécification révisée, une nouvelle valeur de code (pour le champ du message de réponse d'enregistrement) est nécessaire dans la gamme normalement utilisée pour les messages d'agent étranger. Ce code d'erreur est nécessaire pour indiquer l'état "Adresse d'agent de rattachement invalide". Voir les détails au paragraphe 3.7.2.

### 6.1 Types de message IP mobile

Les messages IP mobile sont définis comme étant ceux qui sont envoyés à un receveur de message à l'accès 434 (UDP ou TCP). L'espace de nombres pour les messages IP mobile est spécifié au paragraphe 1.8. L'approbation de nouveaux numéros d'extension est soumis à revue d'expert, et une spécification est exigée [RFC5226]. Les types de messages actuellement normalisés ont les numéros suivants, et sont spécifiés aux paragraphes indiqués.

| Type | Nom | Paragraphe |
|---|---|---|
| 1 | Demande d'enregistrement | 3.3 |
| 3 | Réponse d'enregistrement | 3.4 |

### 6.2 Extensions à l'annonce de routeur de la RFC 1256

La RFC 1256 définit deux types de message ICMP, annonce de routeur et sollicitation de routeur. IP mobile définit un espace de numéros pour les extensions d'annonce de routeur, qui pourrait être utilisé par les protocoles autres que IP mobile. Les types d'extension actuellement normalisés pou l'usage de IP mobile ont les numéros suivants :

| Type | Nom | Paragraphe |
|---|---|---|
| 0 | Bourrage d'un octet | 2.1.3 |
| 16 | Annonce d'agent de mobilité | 2.1.1 |
| 19 | Longueurs de préfixe | 2.1.2 |

L'approbation de nouveaux numéros d'extension à l'usage de IP mobile est soumise à revue d'expert, et une spécification est exigée [RFC5226].

### 6.3 Extensions aux messages d'enregistrement IP mobile

Les messages IP mobile spécifiés dans le présent document et mentionnés aux paragraphes 1.8 et 6.1 peuvent avoir des extensions. Les extensions de messages IP mobile partagent toutes le même espace de numéros, même si elles sont à appliquer à des messages IP mobile différents. L'espace de numéros pour les extensions de message IP mobile est spécifié dans le présent document. L'approbation de nouveaux numéros d'extension est soumis à revue d'expert, et une spécification est exigée [RFC5226].

| Type | Nom | Paragraphe |
|---|---|---|
| 0 | Bourrage d'un octet | 2.1.3 |
| 32 | Authentification mobile-rattachement | 3.5.2 |
| 33 | Authentification mobile-étranger | 3.5.3 |
| 34 | Authentification étranger-rattachement | 3.5.4 |

### 6.4 Valeurs de code pour les messages de réponse d'enregistrement IP mobile

Le message IP mobile réponse d'enregistrement, spécifié au paragraphe 3.4, a un champ Code. L'espace de numéros pour les valeurs du champ Code est aussi spécifié au paragraphe 3.4. L'espace de nombres de Code est structuré selon que l'enregistrement a réussi, que l'agent étranger a refusé la demande d'enregistrement, ou que l'agent de rattachement a refusé la demande d'enregistrement, comme suit :

| Numéros de code | Lignes directrices |
|---|---|
| 0-8 | Codes de succès |
| 9-63 | Lignes directrices d'allocation non spécifiées dans le présent document |
| 64-127 | Codes d'erreur provenant de l'agent étranger |
| 128-192 | Codes d'erreur provenant de l'agent de rattachement |
| 193-200 | Codes d'erreur provenant de la passerelle d'agent étranger [RFC4857] |
| 201-255 | Lignes directrices d'allocation non spécifiées dans le présent document |

**Table 1 : Lignes directrices pour l'allocation des valeurs de code**

## 7. Remerciements

Des remerciement particuliers à Steve Deering (Xerox PARC) qui avec Dan Duchamp et John Ioannidis (JI) (Columbia University) ont formé le groupe de travail, l'ont présidé, et déployé tant d'efforts dans ses premiers développements. Les premiers travaux de l'Universite de Columbia sur IP mobile se trouvent dans [MOBILE], [DESIGN], [IOANNIDIS].

Merci aussi à Kannan Alaggapan, Greg Minshall, Tony Li, Jim Solomon, Erik Nordmark, Basavaraj Patil, et Phil Roberts de leurs contributions au groupe lors de leur mandat de président, ainsi que pour leurs nombreux commentaires utiles.

Merci aux membres actifs du groupe de travail IP mobile, en particulier à ceux qui ont fourni des contributions écrites, incluant (par ordre alphabétique) : Ran Atkinson (Naval Research Lab), Samita Chakrabarti (Sun Microsystems), Ken Imboden (Candlestick Networks, Inc.), Dave Johnson (Carnegie Mellon University), Frank Kastenholz (FTP Software), Anders Klemets (KTH), Chip Maguire (KTH), Alison Mankin (ISI), Andrew Myles (Macquarie University), Thomas Narten (IBM), Al Quirt (Bell Northern Research), Yakov Rekhter (IBM), Fumio Teraoka (Sony), Alper Yegin (NTT DoCoMo).

Merci à Charlie Kunzinger et Bill Simpson, les éditeurs qui ont produit les premiers projets du présent document, reflétant les discussions du groupe de travail. Beaucoup du nouveau texte des dernières révisions précédant la RFC 2002 est dû à Jim Solomon et Dave Johnson.

Merci à Greg Minshall (Novell), Phil Karn (Qualcomm), Frank Kastenholz (FTP Software), et Pat Calhoun (Sun Microsystems) de leur généreux soutien en hébergeant les réunions du groupe de travail intérimaire.

Les paragraphes 1.10 et 1.11, qui spécifient les formats des nouvelles extensions à utiliser avec les types agrégeables d'extension, ont été inclus à partir d'un document de spécification (intitulé "Mobile IP Extensions Rationalization (MIER)", qui a été écrit par Mohamed Khalil (Nortel Networks), Raja Narayanan (nVisible Networks), Haseeb Akhtar (Nortel Networks) et Emad Qaddoura (Nortel Networks).

Merci à ces auteurs, et aussi pour le travail supplémentaire sur MIER, auquel ont contribué Basavaraj Patil, Pat Calhoun, Neil Justusson, N. Asokan, et Jouni Malinen.

Merci à Vijay Devarapalli, qui a passé de longues heures à convertir la source de ce document en format XML.

## 8. Références

### 8.1 Références normatives

[RFC0768] J. Postel, "Protocole de datagramme d'utilisateur (UDP)", (STD 6), 28 août 1980.

[RFC0791] J. Postel, éd., "Protocole Internet - Spécification du protocole du programme Internet", STD 5, septembre 1981.

[RFC0826] D. Plummer, "Protocole de résolution d'adresses Ethernet : conversion des adresses de protocole réseau en adresses Ethernet à 48 bits pour transmission sur un matériel Ethernet", STD 37, novembre 1982.

[RFC1112] S. Deering, "Extensions d'hôte pour diffusion groupée sur IP", STD 5, août 1989. *(Mise à jour par la* RFC2236*)*

[RFC1256] S. Deering, éditeur, "Messages ICMP de découverte de routeur", septembre 1991.

[RFC1321] R. Rivest, "Algorithme de résumé de message MD5", avril 1992. *(Information)*

[RFC2003] C. Perkins, "Encapsulation de IP dans IP", octobre 1996. (*MàJ par* RFC 3168, RFC 6864, Errata) *(P.S.)*

[RFC2004] C. Perkins, "Encapsulation minimale au sein de IP", octobre 1996. *(P.S.)*

[RFC2005] J. Solomon, "Déclaration d'applicabilité pour la prise en charge de la mobilité sur IP", octobre 1996. *(P.S.)*

[RFC2006] D. Cong, M. Hamlen, C. Perkins, "Définitions des objets gérés pour la prise en charge de la mobilité sur IP avec SMIv2", octobre 1996. *(P.S.)*

[RFC2104] H. Krawczyk, M. Bellare et R. Canetti, "HMAC : Hachage de clés pour l'authentification de message", février 1997.

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

[RFC2784] D. Farinacci, T. Li, S. Hanks, D. Meyer et P. Traina, "Encapsulation d'acheminement générique (GRE)", mars 2000.

[RFC2794] P. Calhoun, C. Perkins, "Extension d'identifiant d'accès à un réseau mobile IP pour IPv4", mars 2000. *(P.S.)*

[RFC3024] G. Montenegro, éd., "Tunnelage inverse pour IP mobile, révisé", janvier 2001. *(P.S.)*

[RFC3115] G. Dommety et K. Leung, "Extensions spécifiques de l'organisation/fabricant à IP pour les mobiles", avril 2001. *(PS)*

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

[RFC4086] D. Eastlake 3rd, J. Schiller, S. Crocker, "Exigences d'aléa pour la sécurité", juin 2005. (*Remplace* RFC1750) (BCP0106)

[RFC4302] S. Kent, "En-tête d'authentification IP", décembre 2005. *(P.S.)*

[RFC4721] C. Perkins et autres, "Extensions de mise en cause/réponse de IPv4 mobile (révisé)", janvier 2007. *(P.S.)*

[RFC5226] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, mai 2008. (*Remplace* RFC2434 *; remplacée par* RFC8126)

[RFC5905] D. Mills, J. Martin, J. Burbank, W. Kasch, "Protocole de l'heure du réseau version 4 (NTPv4) : Spécification du protocole et des algorithmes ", juin 2010. (*Remplace* RFC1305, RFC4330) *(P. S ; MàJ par* RFC7822, RFC8573)

### 8.2 Références poiur information

[CONGESTION] Jacobson, V., "Congestion Avoidance et Control", dans Proceedings of the SIGCOMM '88 Workshop, ACM SIGCOMM, ACM Press, pages 314-329, août 1998.

[DESIGN] Ioannidis, J. and G. Maguire, "The Design and Implementation of a Mobile Internetworking Architecture", dans Proceedings of the Winter USENIX Technical Conference, pages 489-500, janvier 1993.

[IANA] IANA, "Mobile IPv4 Numbers", http://www.iana.org.

[IOANNIDIS] Ioannidis, J., "Protocols for Mobile Internetworking", PhD Dissertation - Columbia University in the City of New York, juillet 1993.

[MOBILE] Ioannidis, J., Duchamp, D., and G. Maguire, "IP-Based Protocols for Mobile Internetworking", dans Proceedings of the SIGCOMM '01 Conference: Communications Architectures and Protocols, pages 235-245, septembre 1991.

[PERF] Caceres, R. and L. Iftode, "Improving the Performance of Reliable Transport Protocols in Mobile Computing Environments", IEEE Journal on Selected Areas in Communication, 13(5):850-857, juin 1995.

[RFC0925] J. Postel, "Résolution d'adresse dans les multi-LAN", octobre 1984.

[RFC1144] V. Jacobson, "Compression des en-têtes TCP/IP pour les liaisons série à faible débit", février 1990.

[RFC1332] G. McGregor, "Protocole de contrôle de protocole Internet point à point (IPCP)", mai 1992. *(MàJ par* RFC3241*)*

[RFC1661] W. Simpson, éditeur, "Protocole point à point (PPP)", STD 51, juillet 1994. *(MàJ par la* RFC2153)

[RFC2002] C. Perkins, éd., "Prise en charge de la mobilité sur IP", octobre 1996. (*Obsolète, voir* RFC3220) *(P.S.)*

[RFC2131] R. Droms, "Protocole de configuration dynamique d'hôte", mars 1997. *(DS) (Mà J par* RFC3396, RFC4361, RFC5494, et RFC6849)

[RFC2290] J. Solomon, S. Glass, "Option de configuration IPv4 mobile pour PPP IPCP", février 1998. (*MàJ par* RFC2794) *(P.S.)*

[RFC2356] G. Montenegro, V. Gupta, "Traversée de pare-feu SKIP de Sun pour IP mobile", juin 1998. *(Information)*

[RFC2488] M. Allman et autres, "Amélioration de TCP sur canal satellite avec les mécanismes standard", janvier1999. (BCP0028)

[RFC2757] G. Montenegro et autres, "Longs réseaux fins", janvier 2000. *(Information)*

[RFC2827] P. Ferguson, D. Senie, "Filtrage d'entrée de réseau : Combattre les attaques de déni de service qui utilisent l'usurpation d'adresse de source IP", mai 2000. (*MàJ par* RFC3704) (BCP0038)

[RFC2863] K. McCloghrie, F. Kastenholz, "MIB de groupe Interfaces", juin 2000. *(D.S.)*

[RFC2988] V. Paxson, M. Allman, "Calcul du temporisateur de retransmission de TCP", novembre 2000. *(P.S.)(Obs., voir* RFC6298)

[RFC3135] J. Border et autres, "Amélioration des performances des mandataires destinée à atténuer les dégradations concernant la liaison", juin 2001. *(Information)*

[RFC3155] S. Dawkins et autres, "Implications des liaisons avec des erreurs sur les performances de bout en bout", août 2001. (BCP0050)

[RFC3220] C. Perkins, éd., "Prise en charge de la mobilité IP pour IPv4", janvier 2002. (*Obsolète, voir* RFC3344) *(P.S.)*

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

[RFC3543] S. Glass, M. Chandra, "Révocation d'enregistrement dans IPv4 mobile", août 2003. *(P.S.)*

[RFC3957] C. Perkins, P. Calhoun, "Clés d'enregistrement d'authentification, d'autorisation, et de comptabilité (AAA) pour IPv4 mobile", mars 2005. *(P.S.)*

[RFC4857] E. Fogelstroem et autres, "Enregistrement régional de IPv4 mobile", juin 2007. *(Expérimentale)*

[TCPIP] Bellovin, S., "Security Problems in the TCP/IP Protocol Suite", ACM Computer Communications Review, 19(2), mars 1989.

[TCP/IP] Stevens, R., "TCP/IP Illustrated, Volume 1: The Protocols", Addison-Wesley, Reading, Massachusetts, 1994.

## Appendice A. Considérations sur la couche de liaison

Le nœud mobile PEUT utiliser les mécanismes de couche de liaison pour décider que son point de rattachement a changé. De telles indications incluent l'état d'interface Down/Testing/Up [RFC2863], et les changements de cellule ou d'administration. Les mécanismes seront spécifiques de la technologie particulière de couche de liaison, et sortent du domaine d'application du présent document.

Le protocole point à point (PPP) [RFC1661] et son protocole de contrôle du protocole Internet (IPCP) [RFC1332] négocient l'utilisation des adresses IP.

Le nœud mobile DEVRAIT d'abord tenter de spécifier son adresse de rattachement, afin que si le nœud mobile est attaché à son réseau de rattachement, la liaison sans acheminement fonctionne correctement. Quand l'adresse de rattachement n'est pas acceptée par l'homologue, mais qu'une adresse IP transitoire est allouée dynamiquement au nœud mobile, et que le nœud mobile est capable de prendre en charge une adresse d'entretien colocalisée, le nœud mobile PEUT enregistrer cette adresse comme adresse d'entretien colocalisée. Quand l'homologue spécifie sa propre adresse IP, cette adresse NE DOIT PAS être supposée être une adresse d'entretien d'agent étranger ou l'adresse IP d'un agent de rattachement. Les extensions PPP pour IP mobile ont été spécifiées dans la [RFC2290]. Prière de consulter ce document pour les détails de la façon de traiter l'allocation de l'adresse d'entretien à partir de PPP d'une façon plus efficace.

## Appendice B. Considérations sur TCP

### B.1 Temporisateurs TCP

Quand des liaisons à fort délai (par exemple, SATCOM) ou faible bande passante (par exemple, la radio à hautes fréquences) sont utilisées, des piles TCP peuvent avoir des temporisations de retransmission insuffisamment adaptatives (non standard). Il peut y avoir des temporisations de retransmission parasites, même quand la liaison et le réseau fonctionnent en fait correctement, mais juste avec un fort retard à cause du support utilisé. Cela peut causer l'incapacité de créer ou maintenir les connexions TCP sur de telles liaisons, et peut aussi causer des retransmissions inutiles qui consomment une bande passante déjà rare. Les fabricants sont encouragés à suivre les algorithmes de la [RFC2988] quand ils mettent en œuvre des temporisateurs de retransmission TCP. Les fabricants de systèmes conçus pour les liaisons à faible bande passante et fort délai devraient consulter les [RFC2757], [RFC2488]. Les concepteurs d'applications visant à opérer sur des nœuds mobiles devraient être sensibles à la possibilité de difficultés en rapport avec les temporisations.

### B.2 Gestion d'encombrement sur TCP

Les nœuds mobiles utilisent souvent des supports qui vont très probablement introduire des erreurs, causant effectivement l'élimination de plus de paquets. Cela introduit un conflit avec les mécanismes de gestion de l'encombrement qui se trouvent dans les versions modernes de TCP [CONGESTION]. Maintenant, quand un paquet est abandonné, la mise en œuvre TCP du nœud correspondant va probablement réagir comme si il y avait une source d'encombrement du réseau, et initier les mécanismes de démarrage lent [CONGESTION] conçus pour contrôler ce problème. Cependant, ces mécanismes sont inappropriés pour surmonter les erreurs introduites par les liaisons elles-mêmes, et avoir pour effet d'augmenter la discontinuité introduite par le paquet éliminé. Ce problème a été analysé par Caceres, et al. [PERF]. Les approches de TCP du problème du traitement des erreurs qui pourraient interférer avec la gestion de l'encombrement sont discutées dans les documents du groupe de travail PILC [RFC3135], [RFC3155]. Bien que de telles approches sortent du domaine d'application du présent document, elles illustrent que fournir la transparence des performances aux nœuds mobiles implique de comprendre les mécanismes hors de la couche réseau. Les problèmes introduits par des taux d'erreurs supérieurs sur le support indiquent aussi qu'il faut éviter les conceptions qui éliminent systématiquement les paquets ; de telles conceptions pourraient autrement être considérées favorablement quand on fait des compromis sur l'ingénierie.

## Appendice C. Exemples de scénarios

Cette section donne des exemples de demandes d'enregistrement pour plusieurs scénarios courants.

### C.1 Enregistrement avec une adresse d'entretien d'agent étranger

Le nœud mobile reçoit une annonce d'agent d'un agent étranger et souhaite s'enregistrer auprès de cet agent en utilisant l'adresse d'entretien annoncée par l'agent étranger. Le nœud mobile souhaite seulement l'encapsulation IP dans IP, ne veut pas de diffusions, et ne veut pas de liens de mobilité simultanés :

Champs IP :
- Adresse de source = adresse de rattachement du nœud mobile
- Adresse de destination = copiée de l'adresse IP de source de l'annonce d'agent
- Durée de vie = 1

Champs UDP :
- Accès de source = <any>
- Accès de destination = 434

Champs de demande d'enregistrement :
- Type = 1
- S=0,B=0,D=0,M=0,G=0
- Durée de vie = durée de vie d'enregistrement copiée de l'extension Annonce d'agent de mobilité du message Annonce de routeur
- Adresse de rattachement = adresse de rattachement du nœud mobile
- Agent de rattachement = adresse IP de l'agent de rattachement du nœud mobile
- Adresse d'entretien = adresse d'entretien copiée de l'extension Annonce d'agent de mobilité du message Annonce de routeur
- Identification = horodatage NTP ou nom occasionnel.

Extensions : une extension d'activation d'autorisation (par exemple, l'extension Authentification mobile-rattachement)

### C.2 Enregistrement avec une adresse d'entretien colocalisée

Le nœud mobile entre dans un réseau étranger qui ne contient pas d'agent étranger. Le nœud mobile obtient une adresse d'un serveur DHCP [RFC2131] pour l'utiliser comme adresse d'entretien colocalisée. Le nœud mobile prend en charge toutes les formes d'encapsulation (IP dans IP, encapsulation minimale, et GRE) désire une copie des datagrammes diffusés sur le réseau de rattachement, et ne veut pas de liens de mobilité simultanés :

Champs IP :
- Adresse de source = adresse d'entretien obtenue du serveur DHCP
- Adresse de destination = adresse IP de l'agent de rattachement
- Durée de vie = 64

Champs UDP :
- Accès de source = <any>
- Accès de destination = 434

Champs de demande d'enregistrement :

Type = 1
S=0,B=1,D=1,M=1,G=1
Durée de vie = 1800 (secondes)
Adresse de rattachement = adresse de rattachement du nœud mobile
Agent de rattachement = adresse IP de l'agent de rattachement du nœud mobile
Adresse d'entretien = adresse d'entretien obtenue du serveur DHCP
Identification = horodatage NTP ou nom occasionnel
Extensions : extension Authentification mobile-rattachement

### C.3 Désenregistrement

Le nœud mobile retourne chez lui et souhaite désenregistrer toutes les adresses d'entretien avec son agent de rattachement :

Champs IP :
Adresse de source = adresse de rattachement du nœud mobile
Adresse de destination = adresse IP de l'agent de rattachement
Durée de vie = 1
Champs UDP :
Accès de source = <any>
Accès de destination = 434
Champs de Demande d'enregistrement :
Type = 1
S=0,B=0,D=0,M=0,G=0
Durée de vie = 0
Adresse de rattachement = adresse de rattachement du nœud mobile
Agent de rattachement = adresse IP de l'agent de rattachement du nœud mobile
Adresse d'entretien = adresse de rattachement du nœud mobile
Identification = horodatage NTP ou nom occasionnel
Extensions : extension d'activation d'autorisation (par exemple, l'extension Authentification mobile-rattachement)

## Appendice D. Applicabilité de l'extension des longueurs de préfixes

Il est conseillé d'être prudent avec l'utilisation de l'extension Longueurs de préfixe sur les liaisons sans fil, à cause de la couverture irrégulière des zones par les émetteurs sans fil. Par suite, il est possible que deux agents étrangers qui annoncent le même préfixe puissent en fait fournir une connexité différente aux nœuds mobiles candidats. L'extension Longueurs de préfixe NE DEVRAIT PAS être incluse dans les annonces envoyées par les agents dans cette configuration.

Les agents étrangers qui utilisent des interfaces sans fil différentes vont devoir coopérer en utilisant des protocoles spéciaux pour fournir une couverture spatiale identique, et donc être capables de proclamer qu'ils ont des interfaces sans fil situées sur le même sous réseau. Dans le cas d'interfaces filaires, un nœud mobile qui se déconnecte et ensuite se connecte à un nouveau point de rattachement peut bien envoyer une nouvelle demande d'enregistrement sans considérer si la nouvelle annonce est sur le même support que la dernière annonce enregistrée. Et finalement, dans des zones de population dense d'agents étrangers, il ne semblerait pas pertinent d'exiger la propagation via des protocoles d'acheminement des préfixes de sous réseau associés à chaque agent étranger sans fil individuel ; une telle tactique pourrait conduire à un épuisement rapide de l'espace disponible pour les tableaux d'acheminements, une augmentation incontrôlée de temps requis pour le traitement de la mise à jour des tableaux d'acheminement, et de plus longs délais de décision pour le choix des chemins si des chemins sont mémorisés pour les "sous réseaux" sans fil (ce qui est presque toujours inutile).

## Appendice E. Considérations d'interopérabilité

Le présent document spécifie des révisions à la RFC 2002 qui sont destinées à améliorer l'interopérabilité en résolvant les ambiguïtés contenues dans le texte antérieur. Les mises en œuvre qui effectuent l'authentification conformément au nouvel algorithme plus précisément spécifié seront interopérables avec les mises en œuvre antérieures qui font ce qui était attendu à l'origine pour produire les données d'authentification. Cela était auparavant une source majeure de non interopérabilité.

Cependant, la présente spécification n'a pas de nouvelles caractéristiques qui si elles étaient utilisées, causeraient des problèmes d'interopérabilité avec les mises en œuvre plus anciennes. Toutes les caractéristiques spécifiées dans la RFC 2002 vont fonctionner avec les nouvelles mises en œuvre, sauf pour la compression V-J [RFC1144]. La liste qui suit

détaille les domaines possibles de problèmes de compatibilité que pourraient rencontrer les nœuds qui se conforment à la présente spécification révisée, quand ils tentent d'interopérer avec des nœuds qui obéissent à la RFC 2002.

- Un client qui attend d'un agent étranger (FA) certaines des nouvelles caractéristiques obligatoires (comme le tunnelage inverse) va rester interopérable si il fait attention au bit "T".

- Les nœuds mobiles (MN) qui utilisent l'extension NAI pour s'identifier ne vont pas fonctionner avec les vieux agents de mobilité.

- Les nœuds mobiles qui utilisent une adresse de rattachement de zéro et s'attendent à recevoir leur adresse de rattachement dans la réponse d'enregistrement ne fonctionneront pas avec les vieux agents de mobilité.

- Les nœuds mobiles qui tentent de s'authentifier sans utiliser l'extension Authentification mobile-rattachement vont être incapables de réussir à s'enregistrer auprès de leur agent de rattachement.

Dans tous ces cas, un nœud mobile robuste et bien configuré va très probablement être capable de récupérer si il prend des mesures raisonnables à réception d'une réponse d'enregistrement avec un code d'erreur indiquant la cause du rejet. Par exemple, si un nœud mobile envoie une demande d'enregistrement qui est rejetée parce que elle contient la mauvaise sorte d'extension d'authentification, le nœud mobile pourrait réessayer l'enregistrement avec une extension Authentification mobile-rattachement, car dans ce cas l'agent étranger et/ou l'agent de rattachement ne va pas être configuré à demander les données de remplacement pour l'authentification.

## Appendice F. Changements par rapport à la RFC 3344

On précise ici les révisions de la spécification qui dans le présent document ont été faites après la publication de la RFC 3344. Une liste des changements faits à la RFC 2002 durant le développement de la [RFC3344] se trouve dans cette dernière. Pour les éléments marqués avec un numéros d'issue, on trouvera des informations supplémentaires en consultant les archives de la liste de diffusion de MIP4.

- On montre plus de définitions de bits dans la structure de message d'annonce d'agent (voir au paragraphe 2.1.1). Les nouveaux bits d'annonce ont été définis par d'autres spécifications, mais non reflétés dans les publications précédentes de cette spécification, ce qui a conduit à une certaine confusion. Les citations des autres spécification ont aussi été incluses.

- (Issue 6) Le comportement de l'agent de rattachement a changé pour éviter de rendre obligatoires les réponses d'erreur aux demandes d'enregistrement qui ont été invalidées parce que l'agent étranger a échoué à l'authentification. L'intention est de rendre l'agent de rattachement plus robuste contre les attaques de déni de service dans lesquelles l'appareil malveillant n'a pas l'intention de fournir de demande d'enregistrement valide mais veut seulement encombrer le trafic sur le réseau de rattachement. Voir au paragraphe 3.8.2.1.

- Du fait de la non unicité de l'allocation des adresses IPv4 dans de nombreux domaines, il est possible que différents nœuds mobiles aient la même adresse de rattachement. Si il utilise le NAI, l'agent étranger peut encore les distinguer. Du texte a été ajouté aux paragraphes 3.7.1 et 3.7.3.1 pour spécifier que l'agent étranger DOIT utiliser le NAI pour distinguer les nœuds mobiles qui ont la même adresse de rattachement.

- (Issue 45) Spécifié qu'un agent étranger NE DOIT PAS appliquer une extension Authentification étranger-rattachement à une demande de désenregistrement d'un nœud mobile. Aussi, l'agent étranger NE DOIT PAS appliquer une extension Authentification étranger-rattachement à moins que l'adresse d'entretien dans la demande d'enregistrement corresponde à une adresse annoncée par l'agent étranger.

- Spécifié que l'association de sécurité mobile à utiliser par l'agent étranger et l'agent de rattachement dépend des valeurs contenues dans les données du message, pas dans les en-têtes IP.

- (Issues 9, 18) Un nouveau code d'erreur est créé à l'usage de l'agent étranger, pour le cas où l'agent étranger ne sert pas le nœud mobile comme agent de rattachement. Anciennement, l'agent étranger pouvait utiliser un code d'erreur de 136 pour ce cas.

- (Issue 17) Spécifié que si l'agent de rattachement ne prend pas en charge l'adresse d'envoi individuel non zéro exigée dans le champ Adresse de rattachement de la demande d'enregistrement, il DOIT alors rejeter l'enregistrement avec un code d'erreur de 129. Voir au paragraphe 3.8.3.2.

- (Issue 19) Spécifié que plusieurs extensions d'activation d'autorisation peuvent être présentes dans le message demande d'enregistrement, mais que l'agent de rattachement doit s'assurer que toutes ont été vérifiées (voir au paragraphe 3.8.3.1).

- (Issue 20) Spécifié que l'agent étranger NE DEVRAIT PAS modifier de champ du message de réponse d'enregistrement couvert par l'extension Authentification mobile-rattachement, quand il relaye le paquet au nœud mobile.

- (Issue 21) Précisé que l'agent étranger retire les extensions qui ne précèdent aucune extension d'activation d'autorisation, pas seulement l'extension Authentification mobile-rattachement (paragraphe 3.7.3.2).

- (Issue 44) Spécifié que l'adresse annoncée par l'agent étranger dans les annonces d'agent est l'adresse d'entretien offerte sur cette interface réseau, pas nécessairement l'adresse de l'interface réseau (paragraphe 3.7.2.2).

- (Issue 45) Précision au paragraphe 3.7.2.1 que le code 77 peut seulement s'appliquer à une demande d'enregistrement avec une durée de vie non zéro.

- Créé un nouveau code d'erreur à utiliser quand un agent étranger peut détecter que le champ Adresse d'agent de rattachement est incorrecte.

- Interdit l'utilisation de l'extension d'autorisation étranger-rattachement sur les messages de désenregistrement.

- Nettoyage de la formulation ayant à voir avec les extensions d'activation d'autorisation.

- Pour des questions de cohérence, changement de la formulation de la copie d'accès UDP.

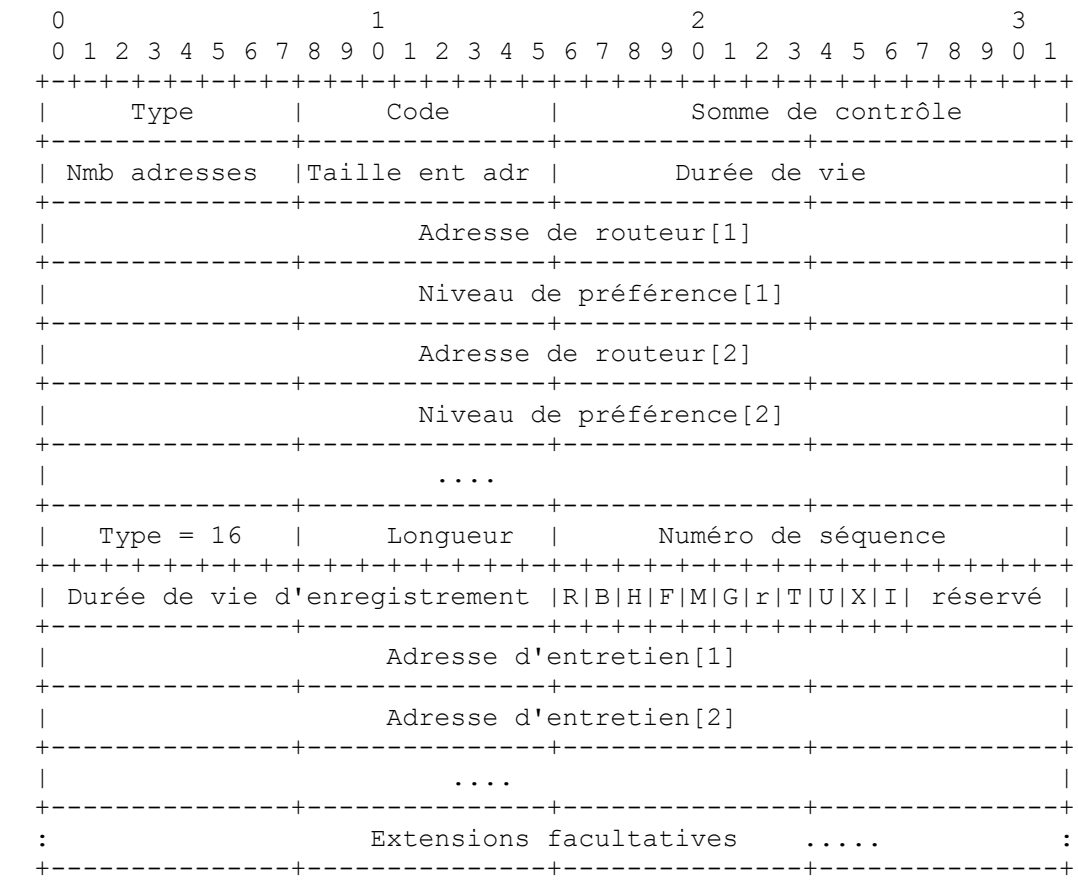
- Ajout de texte pour clairement ne pas interdire le gabarit réseau à configuration dynamique et les informations de sécurité au nœud mobile.

- Reformulation de la section Changements.

- Mise à jour des citations.

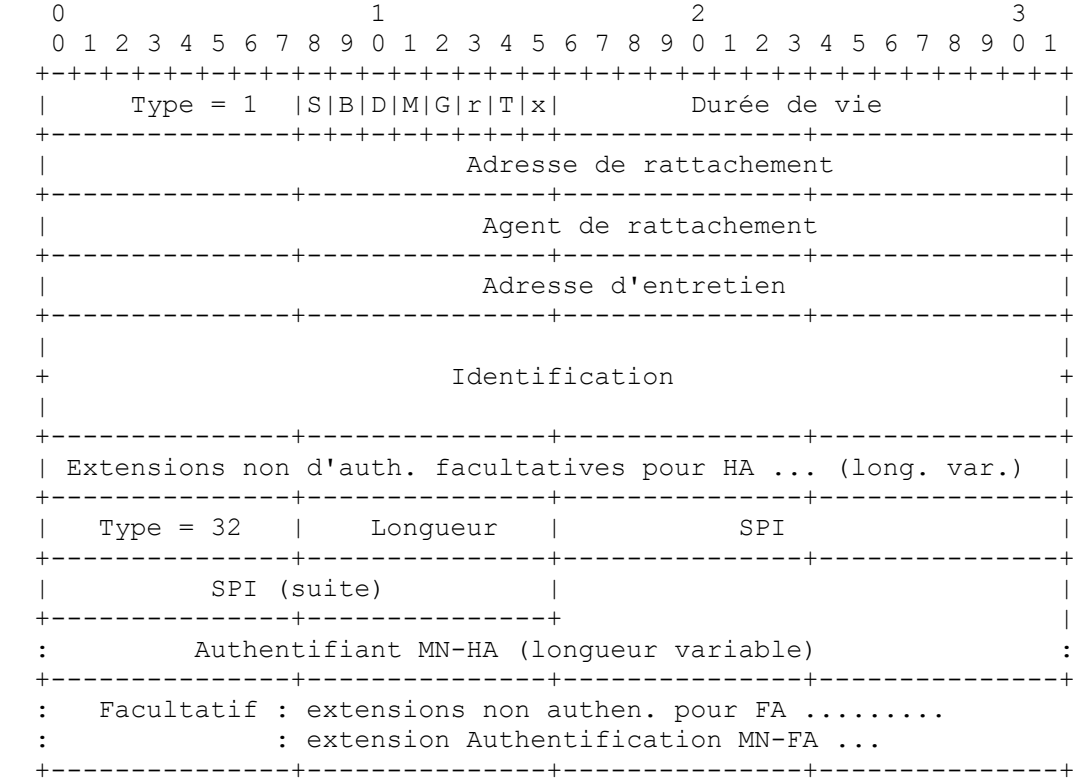
# Appendice G. Exemple de messages

## G.1 Exemple de format de message ICMP d'annonce d'agent



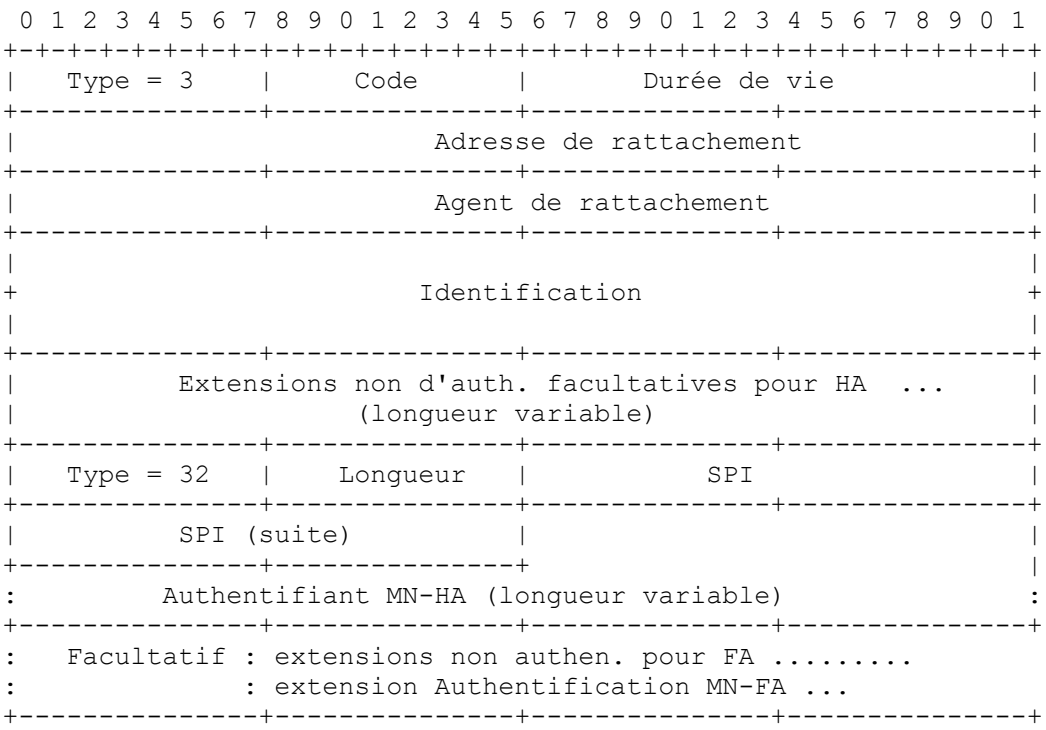

## G.2 Exemple de format de message Demande d'enregistrement

L'en-tête UDP est suivi par les champs IP mobile montrés ci-dessous :



### G.3 Exemple de format de message de réponse d'enregistrement

L'en-tête UDP est suivi par les champs IP mobile montrés ci-dessous :




## Adresse de l'auteur

Charles E. Perkins (éditeur)
WiChorus Inc.
3590 N. 1st Street, Suite 300
San Jose, CA 95134
USA
mél : charliep@computer.org