Groupe de travail Réseau
Request for Comments : 3519
Catégorie : En cours de normamisation
Traduction Claude Brière de L'Isle

H. Levkowetz, ipUnplugged
S. Vaarala, Netseal
avril 2003

Traversée d'IP mobile par les appareils de traduction d'adresse réseau (NAT)

Statut de ce mémoire
Le présent document spécifie un protocole Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et des suggestions pour son amélioration. Prière de se reporter à l'édition actuelle du STD 1 "Normes des protocoles officiels de l'Internet" pour connaître l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Le tunnelage de datagramme IP mobile est incompatible avec la traduction d'adresse réseau (NAT, *Network Address Translation*). Le présent document présente des extensions au protocole IP mobile et une méthode de tunnelage qui permet aux nœuds mobiles qui utilisent IP mobile de fonctionner dans les réseaux d'adresses privés qui sont séparés de l'Internet public par des appareils de NAT. La traversée de NAT se fonde sur l'utilisation de l'accès UDP d'agent de rattachement IP mobile pour encapsuler le trafic de données.

Table des Matières

1. Introduction

1.1 Terminologie

Le présent document utilise la terminologie se rapportant à IP mobile décrite dans la [RFC3344]. De plus, les termes suivants sont utilisés :

Tunnel vers l'avant *(Forward Tunnel)*
C'est un tunnel qui transmet les paquets vers le nœud mobile. Il commence à l'agent de rattachement, et se termine à l'adresse d'entretien du nœud mobile.

Tunnel inverse
Tunnel qui commence à l'adresse d'entretien du nœud mobile et se termine à l'agent de rattachement.

NAT *(Network Address Translation)*
Traduction d'adresse réseau. "Un NAT traditionnel permettrait aux hôtes au sein d'un réseau privé d'accéder de façon transparente aux hôtes dans le réseau externe, dans la plupart des cas. Dans un NAT traditionnel, les sessions sont unidirectionnelles, en sortie du réseau privé." [RFC2663]. Le NAT de base et le NAPT sont deux variétés de NAT.

NAT de base
"Avec un NAT de base, un bloc d'adresses externes est mis de côté pour traduire les adresses des hôtes dans un domaine privé lorsque elles génèrent des sessions avec le domaine externe. Pour les paquets sortants du réseau privé, l'adresse IP de source et les champs qui s'y rapportent comme les sommes de contrôle d'en-tête IP, TCP, UDP et ICMP sont traduits. Pour les paquets entrants, l'adresse IP de destination et les sommes de contrôle citées ci-dessus sont traduites." [RFC2663].

NAPT (*Network Address Port Translation*)
Traduction d'accès d'adresse réseau. "NAPT étend la notion de traduction d'une étape en traduisant aussi l'identifiant de transport (par exemple, les numéros d'accès TCP et UDP, les identifiants d'interrogation ICMP). Cela permet que les identifiants de transport d'un certain nombre d'hôtes privés soient multiplexés dans les identifiants de transport d'une seule adresse externe. NAPT permet à un ensemble d'hôtes de partager une seule adresse externe. Noter que NAPT peut être combiné avec le NAT de base afin qu'un réservoir d'adresses externes soit utilisé en conjonction avec la traduction d'accès." [RFC2663].

Dans le présent document, le terme NAT le plus général est utilisé pour couvrir à la fois les NAT et les NAPT. Dans la plupart des cas de déploiement d'aujourd'hui, on pense que les NAT utilisés sont de la variété NAPT.

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

1.2 Description du problème

Une hypothèse de base que fait IP mobile [RFC3344] est que les nœuds mobiles et les agents étrangers sont identifiables de façon univoque par une adresse IP à acheminement mondial. Cette hypothèse ne tient pas lorsque un nœud mobile tente de communiquer de derrière un NAT.

IP mobile s'appuie sur l'envoi de trafic du réseau de rattachement au nœud mobile ou à l'agent étranger à travers le tunnelage d'IP dans IP. Les nœuds IP qui communiquent de derrière un NAT ne sont joignables qu'à travers la ou les adresses publiques du NAT. Le tunnelage d'IP dans IP ne contient généralement pas assez d'informations pour permettre une traduction univoque des adresses publiques courantes à l'adresse d'entretien particulière d'un nœud mobile ou agent étranger qui réside derrière le NAT ; en particulier, il n'y a pas de numéros d'accès TCP/UDP disponibles pour qu'un NAT travaille avec eux. Pour cette raison, les tunnels IP dans IP ne peuvent en général pas passer à travers un NAT, et IP mobile ne va pas fonctionner à travers un NAT.

Les demandes et réponses d'enregistrement d'IP mobile vont d'un autre côté être capables de passer à travers les NAT et les NAPT sur le côté du nœud mobile ou de l'agent étranger, car ce sont des datagrammes UDP générés de l'intérieur du NAT ou NAPT. Lorsque ils sortent, ils font que le NAT établit une transposition d'adresse/accès à travers laquelle la réponse d'enregistrement va être capable de passer au receveur correct. Le protocole IP mobile actuel ne permet cependant pas un enregistrement où l'adresse IP de source du nœud mobile n'est ni l'adresse d'entretien, ni l'adresse de rattachement, ni 0.0.0.0.

Ce qui est nécessaire est un mécanisme de remplacement du tunnelage des données pour IP mobile qui puisse fournir le moyen pour qu'un appareil de NAT fasse une transposition univoque afin que la traduction d'adresse fonctionne, et un mécanisme d'enregistrement qui permette qu'un tel mécanisme de tunnelage de remplacement soit établi lorsque approprié.

Ce mécanisme va traiter trois scénarios différents :
- un nœud mobile avec une adresse colocalisée derrière un NAT ; pas d'agent étranger (FA, *Foreign Agent*) ;
- un nœud mobile enregistré auprès d'un agent étranger où le nœud mobile et l'agent étranger sont tous deux derrière le même NAT ;
- un nœud mobile avec une adresse colocalisée utilisant un agent étranger qui demande que les enregistrements passent à travers le FA (établit le bit "R") où le nœud mobile et le FA sont tous deux derrière le même NAT.

1.3 Hypothèses

La principale hypothèse du présent document est que le réseau permet la communication entre un accès UDP choisi par le nœud mobile et l'agent de rattachement UDP à l'accès 434. Si cette hypothèse ne tient pas, ni l'enregistrement IP mobile ni le tunnelage des données ne vont fonctionner.

Le présent document NE suppose PAS que la mobilité est restreinte à un espace commun d'adresses IP. Au contraire, le système d'acheminement entre le nœud mobile et l'agent de rattachement peut être partagé en un réseau "privé" et un réseau "public", et l'hypothèse est qu'un mécanisme est nécessaire en plus de l'IP mobile de base selon la [RFC3344] afin de réaliser la mobilité au sein d'espaces d'adresses IP disparates.

Pour une discussion plus complète des problèmes posés par les espaces d'adresses disparates, et comment ils peuvent se résoudre, voir la [RFC3024].

Les tunnels inverses considérés ici sont symétriques, c'est-à-dire, ils utilisent la même configuration (méthode d'encapsulation, points d'extrémité d'adresse IP) que le tunnel vers l'avant.

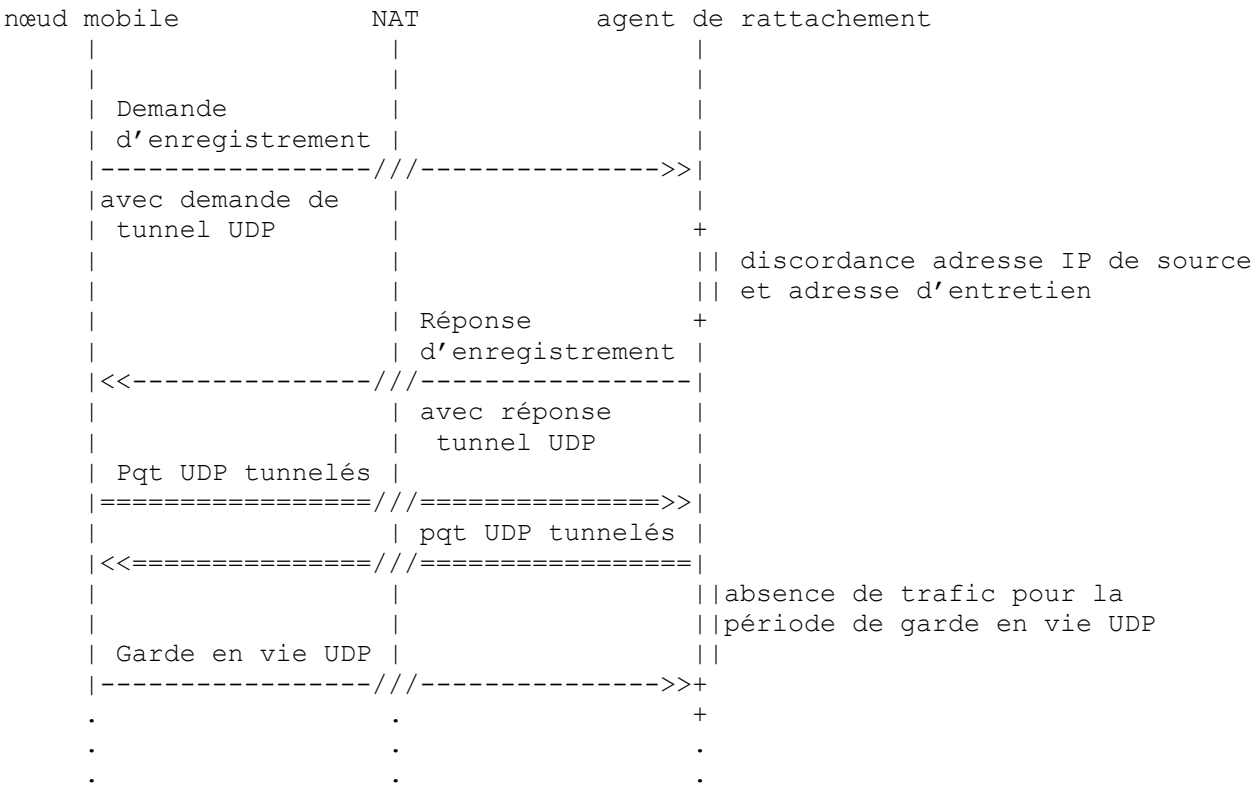
2. Généralités sur la traversée de NAT

La présente section fait un bref survol du mécanisme de tunnelage MIP UDP qui peut être utilisé pour réaliser la traversée de NAT pour IP mobile.

Dans le tunnelage MIP UDP, le nœud mobile peut utiliser une extension (décrite plus loin) dans ses demandes d'enregistrement pour indiquer qu'il est capable d'utiliser le tunnelage IP mobile UDP au lieu du tunnelage IP mobile standard si l'agent de rattachement voit que la demande d'enregistrement semble être passée à travers un NAT. L'agent de rattachement peut alors envoyer une réponse d'enregistrement avec une extension indiquant l'acceptation (ou le refus). Avec l'assentiment de l'agent de rattachement, le tunnelage MIP UDP sera disponible pour une utilisation dans les deux sens de tunnelage, vers l'avant et vers l'arrière. Les paquets UDP tunnelés envoyés par le nœud mobile utilisent les mêmes accès que le message de demande d'enregistrement. En particulier, l'accès de source peut varier entre de nouveaux enregistrements, mais rester le même pour toutes les données et réenregistrements tunnelés. L'accès de destination est toujours 434. Les paquets UDP tunnelés envoyés par l'agent de rattachement utilisent les mêmes accès, mais inversés.

2.1 Séquence de message de base

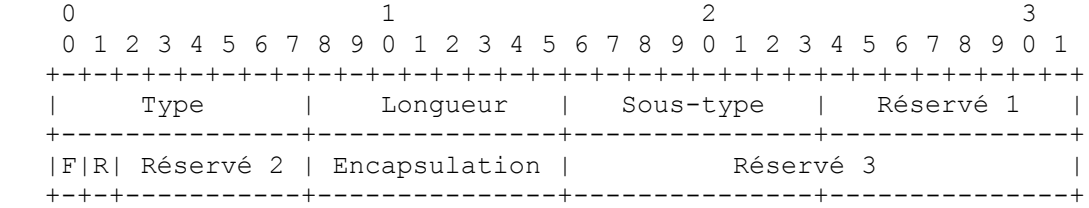
Le diagramme de séquence de message ci-dessous donne un exemple de l'établissement et de l'utilisation d'un tunnel IP mobile UDP comme décrit dans le présent document. Le tunnel est établi par l'utilisation d'extensions spécifiques dans l'échange initial d'une demande et réponse d'enregistrement IP mobile. À partir de là, tout le trafic de l'agent de rattachement au nœud mobile est envoyé à travers le tunnel UDP. Le nœud mobile peut, à sa discrétion, utiliser ou non le tunnel UDP pour le tunnelage inverse, bien que dans la plupart des cas où le tunnelage MIP UDP est nécessaire, le tunnelage inverse le sera aussi.



3. Nouveaux formats de message

3.1 Extension de demande de tunnel UDP

Cette extension peut être sautée. Elle signifie que l'envoyeur est capable de traiter le tunnelage MIP UDP, et facultativement qu'un format particulier d'encapsulation est demandé dans le tunnel MIP UDP. Le format de cette extension est montré ci-dessous. Il se conforme au format d'extension court décrit dans la [RFC3344].



Type : 144
Longueur : 6. Longueur en octets de cette extension, non inclus les octets de Type et Longueur.
Sous-type : 0

Réservé 1 : Réservé pour utilisation future. DOIT être à 0 à l'envoi, DOIT être ignoré à la réception.

F : Fanion Force. Indique que le nœud mobile veut forcer l'établissement du tunnelage MIP UDP.

R : Fanion R (Enregistrement à travers le FA exigé). Indique que le bit R était établi dans l'annonce d'agent du FA. L'enregistrement se fait en utilisant une adresse d'entretien colocalisée, mais à travers le FA.

Réservé 2 : Réservé pour utilisation future. DOIT être à 0 à l'envoi, DOIT être ignoré à réception.

Encapsulation : Indique le type des données tunnelées, en utilisant la même numérotation que le champ Protocole de l'en-tête IP.

Réservé 3 : Réservé pour utilisation future. DOIT être à 0 à l'envoi, DOIT être vérifié comme 0 à réception ; autrement, l'extension doit être traitée comme non comprise et sautée en silence.

3.1.1 Fanion F (Force)

Il indique que le nœud mobile veut utiliser la traversée sans considération du résultat de la détection de NAT effectuée par l'agent de rattachement. Ceci est utile si le chemin entre le nœud mobile et l'agent de rattachement travaille pour les paquets de signalisation IP mobile, mais pas pour les paquets de données génériques (par exemple, à cause des règles de filtrage du pare-feu). Si l'agent de rattachement prend en charge ce protocole, il DEVRAIT soit accepter la traversée et répondre par une extension Réponse de tunnel UDP, soit rejeter la demande d'enregistrement. Dans le cas d'échec de l'enregistrement, l'agent de rattachement (HA, *Home Agent*) DEVRAIT envoyer une réponse d'enregistrement avec le champ Code réglé à 129 ("administrativement interdit").

Si le HA ne comprend pas l'extension Demande de tunnel UDP, il va l'éliminer en silence, et si tout le reste va bien, il va faire une réponse d'enregistrement avec le code de réponse 0 (enregistrement accepté) mais sans aucune extension Réponse de tunnel UDP. Dans ce cas, le nœud mobile NE DOIT PAS utiliser le tunnelage MIP UDP.

3.1.2 Fanion R (Enregistrement par FA exigé)

Ce fanion DOIT être établi par le nœud mobile lorsque il utilise une adresse colocalisée, mais qu'il s'enregistre à travers un FA parce qu'il a reçu une annonce d'agent avec le bit 'R' établi.

3.1.3 Champs réservés

Les champs 'Réservé 1' et 'Réservé 2' doivent être ignorés à réception, tandis que le champ 'Réservé 3' doit être à 0 à réception ; autrement, cette extension DOIT être traitée comme non comprise et sautée en silence. Cela permettra de faire de futurs ajouts à cette extension qui puissent soit coexister avec les vieilles mises en œuvre, soit forcer le rejet de l'extension par une vieille mise en œuvre.

3.1.4 Encapsulation

Le champ 'Encapsulation' définit le mode d'encapsulation demandé si le tunnelage MIP UDP est accepté par l'agent de rattachement. Ce champ utilise les mêmes valeurs que le champ Protocole de l'en-tête IP :

4 En-tête IP (tunnelage IP dans UDP) [RFC2003]
47 En-tête GRE (tunnelage GRE dans UDP) [RFC2784]
55 En-tête d'encapsulation IP minimal [RFC2004]

Si l'agent de rattachement trouve que le tunnelage UDP n'est pas nécessaire, l'encapsulation sera déterminée par les fanions 'M' et 'G' de la demande d'enregistrement ; mais si l'agent de rattachement trouve que le tunnelage MIP UDP devrait être fait, l'encapsulation est déterminée à partir de la valeur du champ Encapsulation. Si la valeur de ce champ est zéro, elle prend par défaut la valeur des champs 'M' et 'G' dans le message de demande d'enregistrement, mais si elle n'est pas zéro, elle indique qu'une encapsulation particulière est désirée.

3.1.5 Bits d'enregistrement d'IP mobile

Les bits d'enregistrement IP mobile S, B, D, M, G et T conservent leur signification comme décrit dans les [RFC3344] et [RFC3024] (excepté que la signification des bits M et G peut être modifiée par le champ Encapsulation lorsque le tunnelage MIP UDP est utilisé, comme décrit ci-dessus). L'utilisation des bits M et G avec le tunnelage MIP UDP est aussi évoqué au paragraphe 4.1.

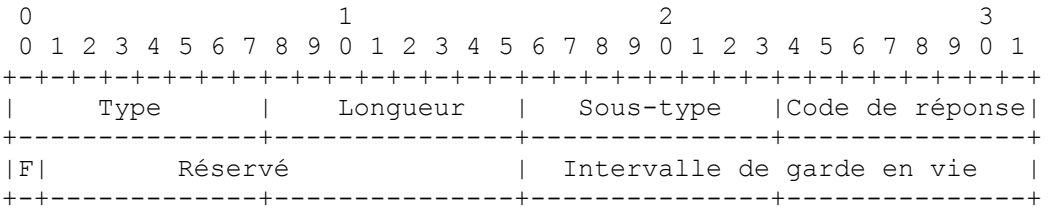
Lorsque le réseau mobile (MN, *Mobile Network*) demande le tunnelage MIP UDP, le bit 'D' (Désencapsulation par le nœud mobile) DOIT être établi, autrement, le tunnelage n'aurait pas de sens.

Le MN et le FA DEVRAIENT tous deux établir le bit 'T' lors d'une demande de tunnelage MIP UDP, même si tout le trafic ne sera pas tunnelé en inverse. Cela assure qu'un HA qui n'est pas prêt à accepter le tunnelage inverse ne va pas accepter un enregistrement qui peut se révéler ultérieurement inutilisable. Voir aussi la discussion de l'utilisation du bit 'T' dans les considérations sur l'agent étranger (paragraphe 4.5).

3.2 Extension Réponse de tunnel UDP

Cette extension ne peut pas être sautée. Elle est envoyée en réponse à une extension Demande de tunnel UDP, et indique si le HA va ou non utiliser le tunnelage MIP UDP pour le lien de mobilité actuel. Le format de cette extension est indiqué ci-

dessous.



Type : 44
Longueur : 6. Longueur en octets de cette extension, non inclus les octets de Type et Longueur.
Sous-type : 0
Code de réponse : Indique si le HA accepte ou refuse d'utiliser le tunnelage UDP pour le lien de mobilité en cours. Voir le paragraphe 3.2.1.
F : Fanion Forcé. Indique que le tunnelage est forcé parce que le fanion F était établi dans la demande de tunnelage, sans considération de la détection ou non d'un NAT.
Intervalle de garde en vie : Spécifie l'intervalle de garde en vie du NAT que le nœud mobile DEVRAIT utiliser. Un paquet Garde en vie DEVRAIT être envoyé si Intervalle-de-garde-en-vie secondes se sont écoulées sans envoi de trafic de signalisation ou de données. Si ce champ est réglé à 0, le nœud mobile DOIT utiliser son intervalle de garde en vie configuré par défaut.
Réservé : Réservé pour utilisation future. DOIT être réglé à 0 à l'envoi, DOIT être ignoré à réception.

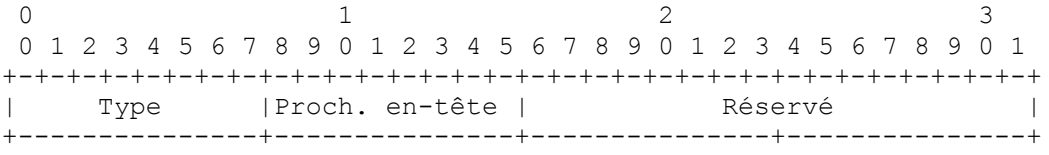
3.2.1 Code de réponse

Le champ Code de réponse de l'extension Réponse de tunnel UDP indique si le tunnelage UDP a été accepté et sera utilisé par le HA. Les valeurs dans la gamme 0 à 63 indiquent l'assentiment, c'est-à-dire que le tunnelage sera fait, tandis que les valeurs dans la gamme 64 à 255 indiquent que le tunnelage ne devrait pas être fait. Plus d'informations peuvent être données par la valeur du code de réponse.

Les codes de réponse suivants sont définis pour être utilisés dans le champ Code de l'extension Réponse de tunnel UDP :
0 Le tunnelage sera fait
64 Tunnelage refusé, raison non spécifiée

3.3 Message Données de tunnel MIP

Cet en-tête de message MIP sert à différencier le trafic tunnelé à travers l'accès bien connu 434 des autres messages IP mobile, par exemple, demandes d'enregistrement et réponses d'enregistrement.



Type : 4
Prochain en-tête : Indique le type de données tunnelées, en utilisant la même numérotation que le champ d'en-tête IP Protocole.
Réservé : Réservé pour utilisation future. DOIT être réglé à 0 à l'envoi, DOIT être ignoré à réception.

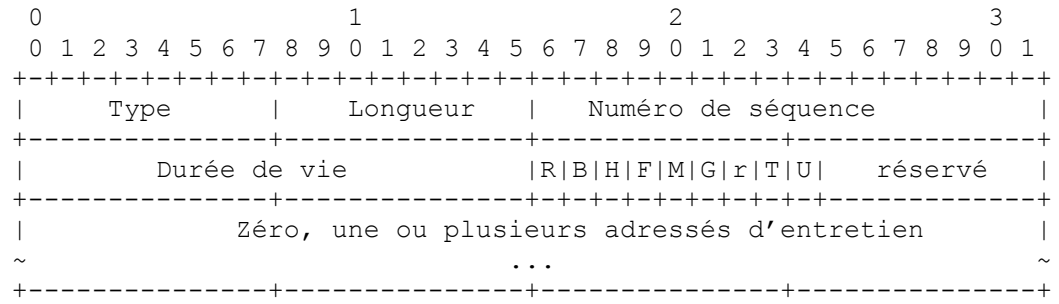
Le champ Prochain en-tête utilise les mêmes valeurs que le champ d'en-tête IP Protocole. Les valeurs suivantes peuvent être actuellement utilisées pour IP mobile :
4 En-tête IP (tunnelage IP dans UDP) [RFC2003]
47 En-tête GRE (tunnelage GRE dans UDP) [RFC2784]
55 En-tête d'encapsulation IP minimal [RFC2004]

Le receveur d'un paquet tunnelé DOIT vérifier que la valeur de Prochain en-tête correspond au mode de tunnelage établi pour le lien de mobilité avec lequel le paquet a été envoyé. Si une discordance est détectée, le paquet DOIT être éliminé. Une entrée de journal d'événements PEUT être créée, mais dans ce cas, le receveur DEVRAIT s'assurer que la quantité d'entrées de journaux créée n'est pas excessive.

En plus des formes d'encapsulation énumérées ci-dessus, le tunnelage MIP UDP peut prendre éventuellement en charge d'autres encapsulations, en utilisant le champ Prochain en-tête dans l'en-tête de données de tunnel MIP et le champ En-tête d'encapsulation de l'extension Demande de tunnel UDP (paragraphe 3.1).

3.4 Fanion Tunnelage UDP dans les annonces d'agent

Le seul changement à l'extension Annonce d'agent de mobilité définie dans la [RFC3344] est un fanion qui indique que l'agent étranger qui génère l'annonce d'agent prend en charge le tunnelage MIP UDP. Le fanion est inséré après les fanions définis dans la [RFC3344].



Le fanion est défini comme suit :

U : Prise en charge du tunnelage UDP. Cet agent prend en charge le tunnelage MIP UDP comme spécifié dans le présent document. Ce fanion DEVRAIT être établi dans les annonces envoyées par un agent étranger qui prend en charge le tunnelage MIP UDP et est situé derrière un NAT. Il NE DOIT PAS être établi dans les annonces des agents étrangers qui ne sont pas situés derrière un NAT, et donc n'ont pas besoin d'annoncer cette capacité.

3.5 Nouveaux codes de réponse d'enregistrement

Un nouveau code de réponse d'enregistrement est défini :

ERROR_HA_UDP_ENCAP_UNAVAIL : Encapsulation de tunnel UDP demandée indisponible

Ceci est utilisé par le HA pour distinguer le refus d'enregistrement causé par un mode d'encapsulation de tunnel indisponible d'un refus causé par une encapsulation de tunnel standard indisponible demandée par l'utilisation du bit 'T' avec le bit 'M' ou 'G'.

4. Comportement du protocole

4.1 Relation au tunnelage MIP standard

Le mode d'encapsulation par défaut pour le tunnelage MIP UDP est l'encapsulation IP dans UDP. Le nœud mobile PEUT demander l'utilisation d'autres formes d'encapsulation avec le tunnelage UDP en réglant le bit 'M' et/ou le bit 'G' d'une demande d'enregistrement IP mobile, ou en demandant explicitement une encapsulation particulière pour le tunnel MIP UDP en utilisant le champ Encapsulation. Les bits M et G conservent la signification décrite dans la [RFC3344] dans le contexte du tunnelage MIP UDP. La version du tunnelage UDP des méthodes d'encapsulation de MIP classique peut être résumée de la façon suivante :

IP dans UDP. Lorsque le tunnelage UDP IP mobile est utilisé, c'est le type d'encapsulation par défaut. Tout agent de rattachement et nœud mobile qui met en œuvre le tunnelage UDP IP mobile DOIT mettre en œuvre ce type d'encapsulation.

GRE dans UDP. Si le bit 'G' est établi dans une demande d'enregistrement et si le champ Encapsulation est zéro, le nœud mobile demande que son agent de rattachement utilise l'encapsulation GRE [RFC1701] pour les datagrammes tunnelés au nœud mobile. Si le tunnelage MIP UDP est aussi demandé et accepté, l'encapsulation GRE dans UDP DEVRA être utilisée dans les mêmes cas où serait utilisée l'encapsulation GRE dans IP si le tunnelage MIP UDP n'avait pas été demandé.

Encapsulation minimale dans UDP. Si le bit 'M' est établi et si le champ Encapsulation est zéro, le nœud mobile demande que son agent de rattachement utilise l'encapsulation minimale [RFC2004] pour les datagrammes tunnelés au nœud mobile. Si le tunnelage MIP UDP est aussi utilisé, l'encapsulation minimale dans UDP DEVRA être utilisée dans les mêmes cas où l'encapsulation minimale conformément à la [RFC2004] serait utilisée si le tunnelage MIP UDP n'avait pas été demandé.

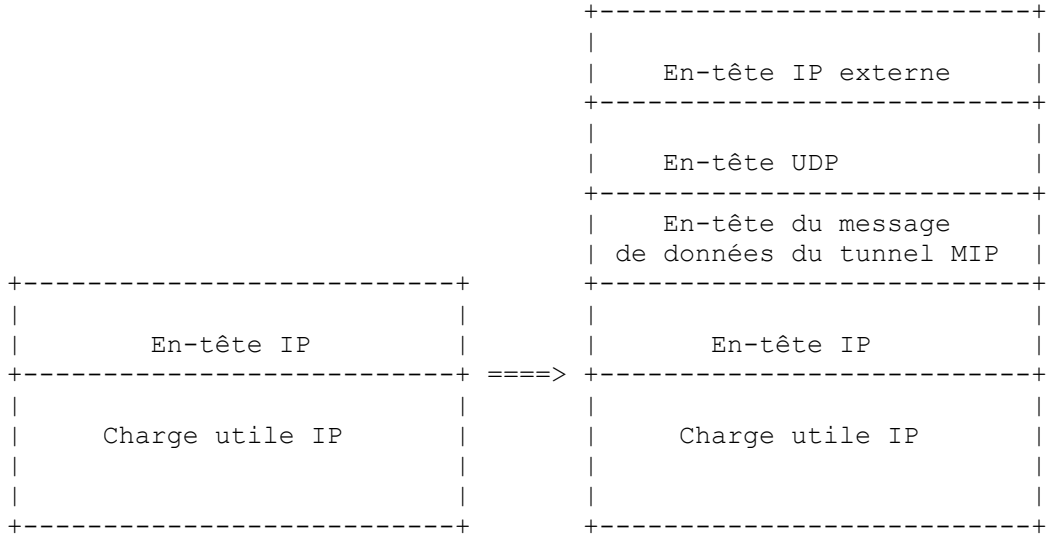
Lorsque le champ Encapsulation n'est pas zéro, un format particulier d'encapsulation est demandé pour le tunnel MIP UDP. Si le tunnelage est indiqué, la demande DOIT soit être acceptée en utilisant l'encapsulation demandée, soit rejetée avec le code d'erreur ERROR_HA_UDP_ENCAP_UNAVAIL, "Encapsulation de tunnel UDP demandée indisponible" défini au paragraphe 3.5. À réception de cette erreur, le nœud mobile PEUT choisir d'envoyer une nouvelle demande d'enregistrement avec des exigences différentes sur l'encapsulation de tunnelage MIP UDP.

4.2 Encapsulation d'en-têtes IP dans UDP

Le tunnelage MIP IP dans UDP, ou tunnelage UDP en abrégé, est fait d'une manière analogue à celle décrite pour le tunnelage IP dans IP de la [RFC2003], à l'exception de l'ajout d'un en-tête UDP [RFC0768] et d'un en-tête Message MIP [RFC3344] entre l'en-tête IP externe et interne.

Les demandes d'enregistrement et les réponses d'enregistrement IP mobile sont déjà sous la forme de messages UDP, et NE DEVRONT PAS être tunnelées même lorsque le tunnelage MIP IP dans UDP est en vigueur.

Pour encapsuler un datagramme IP en utilisant l'encapsulation MIP IP dans UDP, un en-tête IP externe [RFC0791], un en-tête UDP [RFC0768] et un en-tête de message MIP [RFC3344] sont insérés avant l'en-tête IP existant du datagramme, comme suit :



L'adresse de source et l'adresse de destination de l'en-tête IP externe, avec l'accès de source et l'accès de destination de l'en-tête UDP, identifient les "points d'extrémité" du tunnel. L'adresse de source et l'adresse de destination de l'en-tête IP interne identifient respectivement l'envoyeur d'origine et le receveur du datagramme. L'en-tête IP interne n'est pas changé par l'encapsulateur, sauf pour décrémenter le TTL de un si le tunnelage est fait au titre de la transmission du datagramme comme noté dans la [RFC2003], et reste inchangé durant sa livraison au point de sortie du tunnel. Aucun changement aux options IP ne survient dans l'en-tête interne durant la livraison du datagramme encapsulé à travers le tunnel. Noter que les options de sécurité de l'en-tête IP interne PEUVENT affecter le choix des options de sécurité pour l'en-tête IP (externe) encapsulant.

L'encapsulation minimale et l'encapsulation GRE sont faites d'une manière analogue, suivant la [RFC2004] pour l'encapsulation minimale et la [RFC2784] pour l'encapsulation GRE, mais en utilisant les en-têtes IP, UDP et MIP externes à la place de l'en-tête IP externe.

Toutes les autres dispositions et exigences de la [RFC2003] et de la [RFC3024] sont en vigueur, sauf à l'égard de la fragmentation de paquet (paragraphe 4.8).

4.3 Désencapsulation

Avant que la désencapsulation soit réellement faite, le nœud de désencapsulation DOIT vérifier que les adresses IP externes et les numéros d'accès UDP correspondent exactement aux valeurs utilisées pour le tunnel, à l'exception des tunnels qui sont "à moitié liés" (comme décrit au paragraphe 4.11) où l'accès UDP de source peut changer.

Le trafic encapsulé IP dans UDP est désencapsulé simplement en supprimant les en-têtes IP, UDP et MIP externes, ce qui laisse le paquet IP d'origine qui est transmis tel quel.

L'encapsulation IP minimale est traitée conceptuellement comme suit par le receveur. D'abord, les en-têtes UDP et IP mobile sont retirés du paquet, et le champ Protocole de l'en-tête IP remplacé par le champ Prochain en-tête dans l'en-tête Données de tunnel MIP. Ensuite, la longueur totale de l'en-tête IP restant et la somme de contrôle sont ajustées pour correspondre au paquet dépouillé. Enfin, le traitement ordinaire d'encapsulation IP minimale est effectué.

Le trafic encapsulé GRE est traité conformément aux [RFC2784] et [RFC1701], avec l'en-tête de livraison consistant en les en-têtes IP, UDP et MIP externes.

4.4 Considérations sur les nœuds mobiles

L'extension Demande de tunnel UDP PEUT être utilisée dans une demande d'enregistrement IP mobile du nœud mobile à l'agent de rattachement lorsque le nœud mobile utilise une adresse d'entretien colocalisée. Elle NE DEVRA PAS être utilisée par le nœud mobile lorsque il s'enregistre avec une adresse d'entretien d'agent étranger.

L'objet de cette extension est d'indiquer à l'agent de rattachement que le nœud mobile est capable d'accepter le tunnelage MIP UDP si l'agent de rattachement a une indication que le nœud mobile réside derrière un NAT ou NAPT. Elle fonctionne donc comme une sollicitation conditionnelle pour l'utilisation du tunnelage MIP UDP.

Selon les paragraphes 3.2 et 3.6.1.3 de la [RFC3344], le nœud mobile DOIT placer cette extension avant l'extension Authentification mobile-rattachement dans les messages d'enregistrement, afin qu'elle soit couverte par l'extension d'authentification mobile-rattachement.

Si le nœud mobile inclut l'extension Demande de tunnel UDP dans une demande d'enregistrement, mais reçoit une réponse d'enregistrement sans une extension Réponse de tunnel UDP, il DOIT supposer que le HA ne comprend pas cette extension, et il NE DOIT PAS utiliser le tunnelage UDP. Si le nœud mobile est en fait derrière un NAT, l'enregistrement peut alors réussir, mais le trafic ne sera pas capable de traverser le NAT.

Lorsque le nœud mobile envoie des données MIP UDP tunnelées, il DOIT utiliser le même accès de source UDP que celui utilisé pour la plus récente demande d'enregistrement.

Lorsque le nœud mobile se réenregistre sans s'être déplacé, il DEVRAIT veiller à utiliser le même accès de source qu'utilisé pour l'enregistrement d'origine du lien de mobilité actuel. Autrement, alors que l'agent de rattachement va changer d'accès de destination à l'acceptation du nouvel enregistrement, et que le nœud mobile va vraisemblablement commencer à écouter sur le nouvel accès, les paquets en vol depuis l'agent de rattachement au moment du changement vont être éliminés à l'arrivée à l'ancien accès du nœud mobile. (Cela ne signifie pas que l'agent de rattachement devrait refuser une demande d'enregistrement en utilisant le tunnelage MIP UDP lorsque un nouvel accès a été utilisé, car ce peut être le résultat de l'état d'abandon du NAT, du réamorçage du nœud mobile, d'un changement d'interface, etc.).

Si un nœud mobile s'enregistre à travers un agent étranger mais en utilisant une adresse d'entretien colocalisée, et si l'annonce d'agent provenant de l'agent étranger avait le bit 'U' établi, le nœud mobile DOIT établir le fanion 'R' dans son extension Demande de tunnel UDP, afin de faire que le HA utilise le tunnelage MIP UDP. Dans ce cas, le nœud mobile DOIT aussi envoyer un garder-en-vie aussitôt que son enregistrement a été accepté.

Si un nœud mobile s'enregistre à travers un agent étranger mais en utilisant une adresse d'entretien colocalisée, et si l'annonce d'agent provenant de l'agent étranger n'a pas le bit 'U' établi, le nœud mobile NE DOIT PAS inclure une extension Demande de tunnel UDP dans la demande d'enregistrement.

4.5 Considérations sur l'agent étranger

L'extension Demande de tunnel UDP PEUT être utilisée par un agent étranger lorsque il transmet une demande d'enregistrement IP mobile à un agent de rattachement, lorsque l'agent étranger est situé derrière un NAT ou a quelque autre raison impérieuse d'exiger le tunnelage MIP UDP.

L'objet de cette extension est d'indiquer à l'agent de rattachement que l'agent étranger est capable d'accepter le tunnelage MIP UDP si l'agent de rattachement a une indication que l'agent étranger réside derrière un NAT ou NAPT. Elle fonctionne donc comme une sollicitation conditionnelle pour l'utilisation du tunnelage MIP UDP.

Un agent étranger qui exige que le nœud mobile s'enregistre à travers un agent étranger en établissant le bit 'R' dans l'annonce d'agent, NE DOIT PAS ajouter l'extension Demande de tunnel UDP lorsque il transmet une demande d'enregistrement qui utilise une adresse d'entretien colocalisée, car cela conduirait à l'établissement d'un tunnel UDP de l'agent de rattachement à l'agent étranger au lieu du nœud mobile.

Selon les paragraphes 3.2 et 3.7.2.2 de la [RFC3344], lorsque l'agent étranger utilise cette extension, il DOIT la placer après l'extension d'authentification mobile-rattachement dans le message d'enregistrement. Si l'agent étranger partage une association de sécurité de mobilité avec l'agent de rattachement et donc ajoute une extension Authentification étranger-rattachement, l'extension Demande de tunnel UDP DOIT être placée avant l'extension Authentification étranger-rattachement.

Lorsque l'agent de rattachement détecte la présence d'un NAT dans le chemin entre l'envoyeur et lui-même en voyant une discordance entre l'adresse IP de source et l'adresse d'entretien donnée dans la demande d'enregistrement, il est EXIGÉ que l'agent étranger, lorsque il utilise cette extension, envoie la demande d'enregistrement avec une adresse IP de source qui corresponde à l'adresse d'entretien.

Un agent étranger qui utilise le tunnelage MIP UDP vers un agent de rattachement parce que le FA est situé derrière un NAT peut être configuré à encourager le tunnelage inverse, ou à être neutre à son égard, selon les caractéristiques du NAT. Si le NAT traduit toutes les adresses de source des paquets sortants en sa propre adresse publique, il ne sera pas possible de conserver les sessions lors d'un déplacement hors de ce réseau si le nœud mobile a utilisé l'acheminement triangulaire au lieu du tunnelage inverse. D'un autre côté, si on sait que le NAT est assez intelligent pour ne pas traduire les adresses de source publiquement acheminables, ET ne fait pas de filtrage d'entrée, l'acheminement triangulaire peut réussir. La jambe de l'agent de rattachement à l'agent étranger va toujours utiliser le tunnelage MIP UDP pour passer à travers le NAT.

Donc, si on sait lors de la configuration d'un agent étranger derrière un NAT que le NAT va traduire les adresses publiques aussi bien que privées, ou si on sait que le filtrage d'entrée est effectué entre le réseau privé et le réseau public, l'agent étranger DEVRAIT répondre aux demandes d'enregistrement qui n'ont pas le bit 'T' établi par un code de réponse de 75, "le tunnel inverse est obligatoire et le bit 'T' n'est pas établi".

À l'inverse, si on sait que le NAT est assez intelligent pour ne pas traduire les adresses publiques, et qu'aucun filtrage d'entrée n'est fait, il est donc raisonnable de penser qu'un nœud mobile avec une adresse publiquement acheminable peut être capable de garder les sessions tout en allant et venant d'un réseau à l'autre, l'agent étranger PEUT être configuré à transmettre les demandes d'enregistrement même si elles n'ont pas le bit 'T' établi.

Si le comportement du NAT est inconnu à cet égard, on DEVRAIT supposer qu'il va traduire toutes les adresses, et donc l'agent étranger DEVRAIT être configuré à répondre aux demandes d'enregistrement qui n'ont pas le bit 'T' établi avec un code de réponse de 75, "le tunnel inverse est obligatoire et le bit 'T' n'est pas établi".

4.6 Considérations sur l'agent de rattachement

L'objet de l'extension MIP Réponse de tunnel UDP est d'indiquer si l'agent de rattachement accepte ou non l'utilisation du tunnelage MIP UDP pour ce lien de mobilité, et pour informer le nœud mobile ou l'agent étranger de l'intervalle suggéré de garde-en-vie de tunnel à utiliser.

L'extension Réponse de tunnel UDP DOIT être utilisée dans une réponse d'enregistrement IP mobile de l'agent de rattachement au nœud mobile lorsque il a reçu et accepté une demande de tunnel UDP (paragraphe 3.1) d'un nœud mobile.

L'agent de rattachement DOIT utiliser une discordance entre adresse IP de source et adresse d'entretien dans le message de demande d'enregistrement IP mobile comme l'indication qu'un nœud mobile peut résider derrière un NAT. Si la demande d'enregistrement contient aussi l'extension Demande de tunnel UDP sans le fanion 'R' établi, et si l'agent de rattachement est capable de tunnelage MIP UDP, et le permet, l'agent de rattachement DEVRA répondre par une réponse d'enregistrement contenant une extension Réponse de tunnel UDP d'assentiment comme décrit au paragraphe 3.2. Si le fanion 'R' est établi, des

considérations particulières s'appliquent, comme on le décrit ci-dessous.

Si l'agent de rattachement reçoit une demande d'enregistrement avec correspondance d'adresse IP de source et d'adresse d'entretien colocalisée qui contient une extension MIP Demande de tunnel UDP, l'agent de rattachement DEVRAIT répondre par une réponse d'enregistrement contenant une réponse de refus de tunnel UDP – sauf si le tunnelage a été explicitement demandé par le nœud mobile en utilisant le fanion 'F' comme décrit au paragraphe 3.1.

Si l'agent de rattachement consent au tunnelage UDP, il DOIT utiliser l'adresse de source de la demande d'enregistrement comme adresse d'entretien effective, plutôt que l'adresse d'entretien donnée dans la demande d'enregistrement, sauf dans le cas où le fanion 'R' est établi dans l'extension Demande de tunnel UDP.

Si l'agent de rattachement reçoit une demande d'enregistrement avec le fanion 'R' établi dans l'extension Demande de tunnel UDP, il DEVRAIT répondre par une extension Réponse de tunnel UDP d'acquiescement si il est capable de tunnelage MIP UDP et le permet. Dans ce cas, cependant, l'adresse et l'accès de source de la demande d'enregistrement peuvent être une version avec NAT de l'adresse et accès de source de l'agent étranger. Afin de diriger correctement le trafic tunnelé vers le nœud mobile, l'agent de rattachement DOIT attendre qu'arrive le premier paquet garder-en-vie provenant du nœud mobile, avant de pouvoir renvoyer du trafic à l'accès de NAT correct (celui qui est transposé au nœud mobile). Dans ce cas, l'agent de rattachement DOIT vérifier que l'adresse de source externe (mais pas l'accès) de ce paquet garder-en-vie est identique à l'adresse de source de la demande d'enregistrement correspondante. L'adresse de source interne (celle de la demande d'écho ICMP encapsulée) DOIT être l'adresse de rattachement du nœud mobile, et l'adresse de destination interne DOIT être celle de l'agent de rattachement. Si tout cela est vérifié, l'adresse et l'accès externes de source de ce paquet garder-en-vie DEVRONT être utilisés par le HA comme adresse et accès externes de destination du tunnel MIP UDP lors de la transmission de trafic au nœud mobile.

L'agent de rattachement DEVRAIT être cohérent en accusant réception de la prise en charge ou non du tunnelage UDP. Un agent de rattachement qui comprend l'extension Demande de tunnel UDP et est prêt à répondre positivement à une telle demande DEVRAIT aussi répondre par une extension Réponse de tunnel UDP contenant un code de réponse de refus si l'utilisation du tunnelage MIP UDP n'est pas indiquée pour une session. Le nœud mobile NE DOIT PAS supposer un tel comportement de la part de l'agent de rattachement, car celui-ci peut entreprendre un changement de logiciel avec réamorçage, un changement ou remplacement de politique, et par conséquent, un changement de comportement.

4.6.1 Traitement des erreurs

Les actions suivantes sont entreprises lorsque les choses tournent mal.

Le HA ne prend pas en charge l'extension Demande de tunnel UDP :
L'agent de rattachement ignore l'extension et continue normalement, ce qui revient à refuser l'enregistrement si l'adresse IP de source ne correspond pas à l'adresse d'entretien, à l'adresse de rattachement ou à 0.0.0.0. Même si le HA accepte par erreur l'enregistrement, le nœud mobile ne sera pas capable de recevoir les données tunnelées transmises si il est derrière un NAT.
(Il serait avantageux que le nœud mobile se désenregistre dans ce cas. Le nœud mobile n'a cependant normalement aucun moyen de dire qu'il est derrière un NAT si il ne reçoit pas une réponse de tunnelage UDP.)

NAT détecté par l'agent de rattachement, mais traversée non admise :
Dans certains cas, l'agent de rattachement peut désactiver la traversée de NAT bien qu'il prenne en charge l'extension Demande de tunnel UDP et qu'un NAT soit détecté. Dans ce cas, l'agent de rattachement DEVRAIT envoyer une réponse d'enregistrement avec le champ Code réglé à 129, "administrativement interdit".

NAT non détecté, fanion 'F' établi, mais l'agent de rattachement ne permet pas l'utilisation forcée du tunnelage MIP UDP :
L'agent de rattachement DEVRAIT envoyer une réponse d'enregistrement avec le champ Code réglé à 129, "administrativement interdit".

Extension Demande de tunnel UDP envoyée par le nœud mobile (placée avant l'extension Authentification MN-HA) mais le bit 'D' dans l'en-tête de la demande d'enregistrement n'est pas établi : L'agent de rattachement DEVRAIT envoyer une réponse d'enregistrement avec le champ Code réglé à 134, "Demande mal formée".

Extension Demande de tunnel UDP envoyée par l'agent étranger (placée après l'extension Authentification MN-HA) mais le bit 'D' est établi : L'agent de rattachement DEVRAIT envoyer une réponse d'enregistrement avec le champ Code réglé à 134, "Demande mal formée".

Le champ Réservé 3 de l'extension Demande de tunnel UDP n'est pas à zéro : L'agent de rattachement DEVRAIT envoyer une réponse d'enregistrement avec le champ Code réglé à 134, "Demande mal formée".

Type d'encapsulation demandé dans l'extension Demande de tunnel UDP non pris en charge : L'agent de rattachement DEVRAIT envoyer une réponse d'enregistrement avec le champ Code réglé à ERROR_HA_UDP_ENCAP_UNAVAIL, "Encapsulation de tunnel UDP demandée indisponible" défini au paragraphe 3.5.

4.7 Signalisation IP et tunnelage

Le tunnelage UDP DEVRA n'être utilisé que pour les paquets de données, et seulement quand le lien de mobilité utilisé pour l'envoi a été établi en utilisant la demande de tunnel UDP, et acceptée par une réponse de tunnel UDP provenant de l'agent de rattachement. Après l'établissement du tunnelage MIP UDP pour un lien de mobilité, les paquets de données qui sont transmis ou tunnelés en inverse en utilisant ce lien de mobilité DOIVENT être tunnelés en utilisant le tunnelage MIP UDP, et non le tunnelage IP dans IP ou quelque autre méthode de tunnelage.

Par conséquent :
- La signalisation IP mobile n'est jamais tunnelée.
- Lors de l'utilisation de liens simultanés, chaque lien peut avoir un type différent (c'est-à-dire que les liens de tunnelage UDP peuvent être mêlés à des liens de tunnelage non UDP).
- Le tunnelage n'est permis que pour la durée de vie du lien.

4.8 Fragmentation de paquet

D'après le paragraphe 6.3 de la [RFC3022] :
"La traduction de fragments TCP/UDP sortants (c'est-à-dire, ceux générés d'hôtes privés) dans un dispositif NAPT est vouée à l'échec. La raison en est la suivante. Seul le premier fragment contient l'en-tête TCP/UDP qui serait nécessaire pour associer le paquet à une session pour les besoins de la traduction. Les fragments suivants ne contiennent pas les informations sur l'accès TCP/UDP, mais portent simplement le même identifiant de fragmentation que spécifié dans le premier fragment. Disons que deux hôtes privés ont généré des paquets TCP/UDP fragmentés pour le même hôte de destination. Et il se trouve qu'ils utilisent le même identifiant de fragmentation. Lorsque l'hôte cible reçoit les deux datagrammes sans relation entre eux, qui portent le même identifiant de fragmentation et provenant de la même adresse d'hôte allouée, il sera incapable de déterminer à laquelle des deux sessions appartient le datagramme. Par conséquent, les deux sessions seront endommagées."

À cause de cela, si le nœud mobile ou l'agent étranger a besoin pour une raison quelconque d'envoyer des paquets fragmentés, la fragmentation DOIT être faite avant l'encapsulation. Cela diffère du cas du tunnelage IP dans IP, où la fragmentation peut être faite avant ou après l'encapsulation, bien que la [RFC2003] recommande de le faire avant l'encapsulation.

Un problème similaire existe avec certains pare-feu, qui peuvent avoir des règles qui ne permettent le trafic que sur certains accès TCP et UDP, et pas de trafic IP sortant (ou entrant arbitraire. Si c'est le cas et si le pare-feu n'est pas conçu pour faire le réassemblage de paquet, un agent de rattachement derrière un pare-feu aura aussi à faire la fragmentation de paquet avant l'encapsulation MIP UDP. Autrement, seul le premier fragment (qui contient l'en-tête UDP) va avoir l'autorisation de l'agent de rattachement de passer à travers le pare-feu.

Pour cette raison, l'agent de rattachement DEVRAIT faire la fragmentation de paquet avant de faire l'encapsulation MIP UDP.

4.9 Conservation de tunnel

Comme l'existence du tunnel UDP bidirectionnel à travers le NAT dépend des informations de conservation d'état du NAT associées à une session, comme décrit dans la [RFC2663], et comme le NAT peut décider que la session s'est terminée après un certain temps, les messages de garde-en-vie peuvent être nécessaires pour garder le tunnel ouvert. Les garde-en-vie devraient être envoyés plus souvent que la valeur de temporisation utilisée par le NAT.

Cette temporisation peut être supposée durer une à deux minutes, selon la [RFC2663], mais on peut concevoir que des temporisations plus courte existent dans certains NAT.

Pour cette raison, l'extension utilisée pour établir le tunnel UDP a l'option de régler l'intervalle des messages garde-en-vie à une autre valeur que la valeur par défaut ; voir au paragraphe 3.2.

Le message garde-en-vie envoyé DOIT consister en une demande d'écho ICMP correctement encapsulée dans UDP dirigée sur l'agent de rattachement.

Pour chaque lien de mobilité qui a établi le tunnelage UDP, le point d'extrémité non HA du tunnel UDP IP mobile DOIT

envoyer un paquet garde-en-vie si aucun autre paquet pour le HA n'a été envoyé dans les K secondes. Ici K est un paramètre avec une valeur par défaut de 110 secondes. K peut être réglé à une autre valeur par le HA comme décrit dans l'extension Réponse de tunnelage UDP (paragraphe 3.2).

Sauf dans le cas où le nœud mobile s'enregistre avec une adresse colocalisée à travers un FA (voir au paragraphe 4.11) le tunnelage MIP UDP est fait en utilisant les mêmes accès que ceux qui ont déjà été utilisés pour l'échange de demande/réponse d'enregistrement. Le MN ou le FA va envoyer son premier message garder-en-vie au plus tôt K secondes après l'envoi de la demande d'enregistrement. Le même accès UDP de source DOIT être utilisé pour les messages garde-en-vie que celui utilisé pour les messages d'enregistrement d'origine et les messages de données.

Le point d'extrémité distant de tunnel UDP DOIT utiliser des garde-en-vie bidirectionnels consistant en messages de demande/réponse d'écho ICMP encapsulés dans UDP. La raison de l'utilisation de garde-en-vie bidirectionnels est double :

1. Les garde-en-vie bidirectionnels permettent au nœud mobile de détecter la perte d'une transposition de NAT. La détection de la perte de transposition de NAT permet à son tour au MN de compenser en se réenregistrant et en utilisant un garde-en-vie plus court pour éviter la perte des transpositions de NAT à l'avenir.
2. Des garde-en-vie unidirectionnels (envoyés par le MN ou le FA, mais sans réplique de l'agent de rattachement) causent en fait plus de redondance de trafic de garde-en-vie ; les messages garde-en-vie doivent être envoyés plus fréquemment pour compenser la perte occasionnelle de messages garde-en-vie. À l'opposé, les garde-en-vie bidirectionnels sont acquittés, et les retransmissions n'interviennent que lorsque une réponse n'est pas reçue pour une demande garde-en-vie dans un délai raisonnable.

4.10 Détection et compensation de perte de transposition de NAT

Lorsque un nœud mobile utilise des messages de demande/réponse d'écho ICMP encapsulés dans UDP comme garde-en-vie, il va se trouver face à la possibilité qu'une transposition de NAT soit perdue par un appareil de NAT. La chose cruciale ici n'est bien sûr pas la perte d'une transposition de NAT en elle-même, mais plutôt que l'agent de rattachement, en l'absence d'une demande d'enregistrement à travers la nouvelle transposition, va continuer d'envoyer du trafic à l'accès de NAT associé à l'ancienne transposition.
Si le nœud mobile ne donne pas de réplique à sa demande d'écho ICMP encapsulée en UDP même après un certain nombre de retransmissions, et est toujours connecté au même routeur qu'utilisé pour établir le lien de mobilité actuel, le nœud mobile DEVRAIT se réenregistrer auprès de l'agent de rattachement en envoyant une demande d'enregistrement. Cela fait savoir au HA la nouvelle transposition de NAT et restaure la connexité entre le nœud mobile et l'agent de rattachement.

Ayant établi un nouveau lien de mobilité, le nœud mobile PEUT utiliser un intervalle garde-en-vie plus court qu'avant la perte de la transposition de NAT ; en particulier, le nœud mobile PEUT dévier de l'intervalle de garde-en-vie alloué par l'agent de rattachement. Si la perte de lien continue de se produire, le nœud mobile peut raccourcir l'intervalle de garde-en-vie chaque fois qu'il se réenregistre, afin de finir par un intervalle de garde en vie qui soit suffisant pour garder en vie la transposition de NAT. La tactique utilisée pour arriver à un intervalle de garde-en-vie lorsque est perdue une transposition de NAT dépend de la mise en œuvre. Cependant, le nœud mobile NE DOIT PAS utiliser un intervalle de garde-en-vie de moins de 10 secondes.

Noter que la discussion ci-dessus ne s'applique que lorsque le nœud mobile se réenregistre à travers le même routeur, et donc vraisemblablement à travers le même appareil de NAT qui a perdu antérieurement une transposition de NAT. Si le MN se déplace et se trouve toujours derrière un NAT, il DEVRAIT retourner à son intervalle de garde-en-vie d'origine (la valeur par défaut, ou comme allouée par l'agent de rattachement) et il NE DEVRAIT PAS faire de compensation d'intervalle de garde-en-vie sauf si il découvre une perte de transposition de NAT dans le nouvel environnement.

L'agent de rattachement NE DOIT PAS tenter de détecter ou compenser une perte de lien de NAT en changeant de façon dynamique l'intervalle de garde-en-vie alloué dans la réponse d'enregistrement ; l'agent de rattachement n'a pas assez d'informations pour faire cela de façon fiable et il ne devrait donc pas le faire du tout. Le nœud mobile est dans une bien meilleure position pour déterminer quand une transposition de NAT a en fait été perdue. Noter aussi qu'il est permis à un MN de laisser une transposition de NAT arriver à expiration si le MN n'a plus besoin de la connexité.

La discussion ci-dessus ne s'applique que dans un sens limité à un agent étranger qui est situé derrière un NAT et utilise le tunnelage MIP UDP. Dans ce cas, c'est une affaire de configuration permanente du FA pour utiliser un intervalle de garde-en-vie qui soit inférieur à la durée de vie de la transposition de NAT, plutôt que d'essayer de s'adapter de façon dynamique aux durées de vie de liens de NAT différents.

4.11 Enregistrement colocalisé à travers l'agent étranger

Ce paragraphe résume les détails du protocole qui ont été nécessaires pour traiter et prendre en charge le cas où un nœud mobile s'enregistre avec une adresse colocalisée à travers un agent étranger, du fait que les annonces du FA ont le bit 'R' établi. Il donne les informations de base, mais ne formule aucune nouvelle exigence.

Lorsque un mobile enregistre une adresse d'entretien colocalisée à travers un FA, la demande d'enregistrement qui atteint le HA aura une adresse d'entretien différente dans la demande d'enregistrement comparée à l'adresse de source dans l'en-tête IP de la demande d'enregistrement. Si la demande d'enregistrement contient aussi une extension Demande de tunnel UDP, le HA va à tort établir un tunnel UDP, qui va aller au FA au lieu du MN. Pour cette raison, comme mentionné au paragraphe 4.4, le nœud mobile ne doit pas inclure une extension Demande de tunnel UDP dans l'enregistrement si il enregistre une adresse colocalisée à travers un FA qui n'a pas le bit 'U' établi dans ses annonces.

Pour continuer d'être capable d'utiliser le tunnelage MIP UDP dans ce cas, les agents étrangers qui sont situés derrière un NAT sont invités à envoyer des annonces avec le bit 'U' établi, comme décrit au paragraphe 3.4.

Si l'annonce du FA a le bit 'U' établi, indiquant qu'il est derrière un NAT, et aussi le bit 'R' établi, et si le nœud mobile souhaite utiliser une adresse d'entretien colocalisée, il DOIT établir le fanion 'R' dans l'extension Demande de tunnel UDP, afin d'informer le HA de la situation et qu'il puisse agir de la façon appropriée, comme décrit au paragraphe 4.4.

Parce que le tunnel UDP prend maintenant un autre chemin que les demandes d'enregistrement, l'agent de rattachement, lorsque il traite des enregistrements de ce type, doit attendre l'arrivée du premier paquet garde-en-vie avant qu'il puisse établir le tunnel pour l'adresse et l'accès corrects. Pour réduire les possibilités de capture de tunnel par l'envoi de garde-en-vie avec une adresse de source fantaisiste, il est exigé que seul l'accès du garde-en-vie puisse être différent de celui de la demande d'enregistrement ; l'adresse de source doit être la même. Cela signifie que si le FA et le MN communiquent avec le HA à travers des NAT différents, la connexion va échouer.

5. Questions de mise en œuvre

5.1 Détection de mouvement et alias d'adresse privée

En fournissant à un nœud mobile un mécanisme pour que le trafic IP mobile traverse le NAT, on étend l'espace d'adresses où un nœud mobile peut fonctionner et acquérir des adresses d'entretien. Cela entraîne un nouveau problème de détection de mouvement et d'alias d'adresse. On a là un cas qui peut ne pas se produire fréquemment, mais il est mentionné pour être complet :
Comme les réseaux privés utilisent des espaces d'adresses qui se chevauchent, ils peuvent dans certaines situations en prendre par erreur une pour une autre ; c'est ce qu'on appelle dans le présent document l'alias d'adresse privée. Pour cette raison, il peut être nécessaire que les nœuds mobiles qui mettent en œuvre la présente spécification surveillent les adresses de couche liaison de la ou des passerelles utilisées pour l'envoi des paquets. Un changement de l'adresse de couche liaison indique un probable mouvement vers un nouveau réseau, même si l'adresse IP reste joignable en utilisant la nouvelle adresse de couche liaison.

Par exemple, un nœud mobile peut obtenir l'adresse d'entretien colocalisée 10.0.0.1, le gabarit réseau 255.0.0.0, et la passerelle 10.255.255.254 en utilisant le DHCP du réseau n° 1. Il passe alors au réseau n° 2, qui utilise un schéma d'adressage identique. La seule différence pour le nœud mobile est l'adresse de couche liaison de la passerelle. Le nœud mobile devrait mémoriser l'adresse de couche liaison qu'il a obtenue initialement pour la passerelle (en utilisant, par exemple, ARP). Le nœud mobile peut alors détecter des changements de l'adresse de couche liaison dans les échanges ARP successifs au titre de son mécanisme ordinaire de détection de mouvement.

Dans de rares cas, les nœuds mobiles peuvent n'être pas capables de surveiller l'adresse de couche liaison de la ou des passerelles qu'il utilise, et peut donc confondre un point de rattachement avec un autre. La présente spécification ne traite pas explicitement ce problème. Le trou potentiel de trafic causé par cette situation peut être limité en s'assurant que la durée de vie du lien de mobilité est assez courte ; le réenregistrement causé par l'expiration du lien de mobilité règle le problème (voir le paragraphe 5.2).

5.2 Durée de vie de lien de mobilité

Lorsque il répond à une demande d'enregistrement avec une réponse d'enregistrement, il est permis à l'agent de rattachement de diminuer la durée de vie indiquée dans la demande d'enregistrement [RFC3344]. Si on utilise le tunnelage UDP, il y a des cas où une courte durée de vie est bénéfique.

D'abord, si la transposition de NAT entretenue par l'appareil de NAT est abandonnée, un trou de connexion va se produire. Les nouveaux paquets envoyés par le nœud mobile (ou l'agent étranger) vont établir une nouvelle transposition de NAT, que l'agent de rattachement ne va pas reconnaître tant que n'est pas établi un nouveau lien de mobilité par une nouvelle demande d'enregistrement.

Un second cas où une courte durée de vie est utile se rapporte à l'alias des adresses de réseau privé. Dans le cas où le nœud mobile n'est pas capable de détecter la mobilité et se retrouve derrière un nouvel appareil de NAT (comme décrit au paragraphe 5.1) une courte durée de vie va assurer que le trou de trafic ne sera pas excessivement long, et se termine par un réenregistrement.

La définition de "courte durée de vie" dans ce contexte dépend des exigences du scénario d'utilisation. La durée de vie maximum suggérée retournée par l'agent de rattachement est de 60 secondes, mais dans le cas où les scénarios susmentionnés ne posent pas de problème, des durées de vie plus longues peuvent bien sûr être utilisées.

6. Considérations pour la sécurité

Les mécanismes ordinaires de la sécurité IP mobile sont aussi utilisés avec le mécanisme de traversée de NAT décrit dans le présent document. Cependant, il y a un changement notable : le mécanisme de traversée de NAT exige que le HA fasse confiance à des champs d'adresse (et d'accès) non authentifiés potentiellement modifiés par les NAT.

S'appuyer sur des informations d'adresse non authentifiées lors de la formation ou de la mise à jour d'un lien de mobilité conduit à plusieurs faiblesses face à une attaque de redirection. Par essence, un attaquant peut faire ce que fait le NAT, c'est-à-dire, modifier les adresses et les accès et donc causer la redirection du trafic sur une adresse choisie. Les mêmes vulnérabilités s'appliquent aux deux traversées de NAT de MN à HA et de FA à HA.

Plus en détails, sans un NAT, l'adresse d'entretien dans la demande d'enregistrement sera directement utilisée par le HA pour renvoyer le trafic au MN (ou au FA) et l'adresse d'entretien est protégée par l'extension d'authentification MN-HA (ou FA-HA). Lors d'une communication à travers un NAT, l'adresse d'entretien effective du point de vue du HA est celle du NAT, qui n'est pas protégée par une extension d'authentification, mais déduite de l'adresse IP de source apparente des paquets reçus. Cela signifie qu'en utilisant les extensions d'enregistrement mobile IP décrites dans le présent document pour permettre la traversée des NAT, on s'offre soi-même à ce que l'adresse d'entretien d'un MN (ou FA) soit malicieusement changée par un attaquant.

Certaines des attaques, mais pas toutes, pourraient être atténuées dans une certaine mesure par l'utilisation d'une simple vérification d'acheminement. Cependant, le présent document ne spécifie pas un tel mécanisme pour des raisons de simplicité et parce que le mécanisme ne protègerait pas contre toutes les attaques de redirection. Pour limiter la durée de telles attaques de redirection, il est RECOMMANDÉ d'utiliser une durée de vie de lien de mobilité prudente (c'est-à-dire, courte) lorsque on utilise le mécanisme de traversée de NAT spécifié dans le présent document.

Les questions de sécurité connues sont décrites dans les paragraphes suivants.

6.1 Vulnérabilités de la redirection de trafic

6.1.1 Manipulation du message de demande d'enregistrement

Un attaquant sur le chemin entre le nœud mobile (ou agent étranger) et l'agent de rattachement peut rediriger les liens de mobilité sur une adresse désirée simplement en modifiant les en-têtes IP et UDP du message de demande d'enregistrement. Ayant modifié le lien, l'attaquant n'a plus besoin d'écouter (ou de manipuler) le trafic. La redirection est en vigueur jusqu'à l'expiration du lien de mobilité ou que le nœud mobile se réenregistrer.

Cette vulnérabilité peut être utilisée par un attaquant pour lire le trafic destiné à un nœud mobile, et pour envoyer du trafic se faisant passer pour celui du nœud mobile. La vulnérabilité peut aussi être utilisée pour rediriger le trafic sur un hôte victime afin de causer un déni de service à la victime.

La seule défense contre cette vulnérabilité est d'avoir un temps court entre les réenregistrements, ce qui limite la durée de l'attaque de redirection après que l'attaquant a cessé de modifier les messages d'enregistrement.

6.1.2 Envoi d'un message de garde en vie défectueux

Lors d'un enregistrement à travers un FA en utilisant une adresse d'entretien colocalisée, une autre vulnérabilité de redirection s'ouvre. Ayant échangé les messages de demande/réponse d'enregistrement avec le HA à travers le FA, le MN est supposé envoyer le premier message de garde-en-vie au HA, finalisant donc le lien de mobilité (le lien va rester dans un état "à moitié lié" jusqu'à la réception du garde-en-vie).

Ayant observé un échange de demande/réponse d'enregistrement, un attaquant peut envoyer un message garde-en-vie défectueux en supposant que le lien de mobilité est dans l'état "à moitié lié". Cela ouvre une attaque de redirection similaire à celle exposée au paragraphe 6.1.1. Noter cependant que l'attaquant n'a pas besoin d'être capable de modifier les paquets en vol ; il suffit simplement d'être capable d'observer l'échange de messages de demande/réponse d'enregistrement pour monter l'attaque.

En gardant ceci à l'esprit, l'agent de rattachement NE DOIT PAS accepter un message garde-en-vie provenant d'une adresse IP de source différente de celle d'où est venue la demande d'enregistrement, comme spécifié au paragraphe 4.6. Cette exigence limite l'étendue de l'attaque à la redirection du trafic sur un accès UDP erroné, alors que l'adresse IP doit rester la même que dans la demande d'enregistrement initiale.

Les seules défenses contre cette faiblesse sont : (1) d'avoir un temps court entre les réenregistrements, ce qui limite la durée de l'attaque de redirection après que l'attaquant a cessé d'envoyer des messages garde-en-vie frauduleux, et (2) de minimiser la durée pendant laquelle un lien est dans l'état "à moitié lié" en faisant que le nœud mobile envoie le premier message garde-en-vie immédiatement après avoir reçu une réponse d'enregistrement affirmative.

6.2 Utilisation de IPsec

Si le réseau intermédiaire est considéré comme peu sûr, il est recommandé d'utiliser IPsec pour protéger le trafic de données d'utilisateur. Cependant, IPsec ne protège pas contre les attaques de redirection décrites précédemment, autrement qu'en protégeant la confidentialité du trafic de données d'utilisateur capturé.

Le mécanisme de traversée de NAT décrit dans le présent document permet à tout les trafics en rapport avec IPsec de passer à travers les NAT sans aucune modification à IPsec. De plus, les associations de sécurité IPsec n'ont pas besoin d'être rétablies lorsque le nœud mobile se déplace.

6.3 Considérations de pare-feu

Le présent document ne spécifie pas de mécanisme général de traversée de pare-feu. Cependant, le mécanisme rend possible l'utilisation de une seule adresse et d'un seul accès pour toutes les communication MN-HA (ou FA-HA). De plus, l'utilisation du même accès pour le trafic MIP tunnelé par UDP que pour les messages de commande rend assez probable que si un enregistrement MIP peut atteindre l'agent de rattachement, le tunnelage MIP et le tunnelage inverse utilisant le mécanisme décrit va fonctionner aussi.

7. Considérations relatives à l'UNSAF

Le mécanisme décrit dans le présent document n'est pas un mécanisme de "réparation d'auto adressage unilatéral" (UNSAF, *UNilateral Self-Address Fixing*). Bien que le nœud mobile ne tente pas de déterminer ou utiliser l'adresse traduite du NAT, le nœud mobile tente bien à travers le processus d'enregistrement de garder vivante la transposition du NAT à travers des messages de rafraîchissement. Cette section tente de régler les problèmes qui peuvent être soulevés par cette utilisation dans le cadre des considérations de l'IAB sur l'UNSAF [RFC3424].

1. Définition précise :
Cette proposition étend le processus d'enregistrement IPv4 mobile pour qu'il fonctionne à travers les NAT intermédiaires. L'agent de rattachement détecte la présence du NAT en examinant l'adresse de source dans l'en-tête de paquet et en la comparant avec celle contenue dans le message d'enregistrement.
L'adresse et l'accès de NAT détectés par l'agent de rattachement ne sont pas exportés ou communiqués à d'autre nœud.

2. Stratégie de sortie :
Ce mécanisme sera dépassé par le déploiement de IPv6 et IPv6 mobile, palliant le besoin de traversée de NAT pour MIPv4.
On peut aussi noter que ce mécanisme ne fait pas de changement au protocole MIPv4 de base qui le rend dépendant de la présence de NAT ou des extensions actuelles - c'est-à-dire, aucun changement supplémentaire du protocole n'est nécessaire si les NAT disparaissent.

3. Problèmes qui rendent les systèmes plus fragiles :
Les questions spécifiques pertinentes ici sont que l'adresse d'entretien effective (qui est l'adresse de source dans l'en-tête IP reçu par le HA) n'est pas protégée par l'extension d'authentification de IP mobile, et peut donc être imitée. Ceci est discuté avec un certain détail dans la Section 6, Considérations pour la sécurité.

4. Exigences pour des solutions à plus long terme :
La solution à long terme triviale est une transition vers un environnement où on n'a plus besoin des NAT. Le plus évident de ces environnements serait un Internet fondé sur IPv6.

En présence de NAT, une solution améliorée exigerait :
* la capacité de découvrir les traductions faites par chaque NAT le long du chemin,
* la capacité de valider l'autorité de chaque NAT à faire ces traductions,
* de communiquer au titre de la demande d'enregistrement signée l'adresse du NAT le plus proche du HA pour l'utiliser comme l'adresse d'entretien effective du point de due du HA,
* la configuration de tous les NAT intermédiaires à n'accepter que les paquets provenant des NAT du voisinage.

5. Impact sur les NAT déployés existants :
Un précurseur du mécanisme décrit ici a été utilisé avec succès dans les NAT déployés en Suède, Allemagne, Royaume-Uni, Japon et les USA, sans nécessiter ni ajustement des NAT en question, ni ajustement de paramètre de protocole. Au moment de la rédaction, on a peu d'expérience de la mise en œuvre exacte de la proposition de ce document, mais l'effort a porté sur faire ce mécanisme encore plus robuste et adaptable que ses précurseurs.

Par rapport à la spécification IP mobile de base, l'impact de ce document est qu'une fréquence accrue de demandes d'enregistrement est recommandée du point de vue de la sécurité lorsque le mécanisme de traversée de NAT est utilisé.

8. Considérations relatives à l'IANA

Les numéros pour les extensions définies dans ce document ont été tirés de l'espace de numérotation défini pour les messages IP mobile, les extensions d'enregistrement et les codes d'erreur définis dans la [RFC3344]. Ce document propose un nouveau message, deux nouvelles extensions et un nouveau code d'erreur qui exigent des numéros de type et une valeur de code d'erreur qui ont été alloués par l'IANA. Les deux nouvelles extensions introduisent aussi deux nouveaux sous types d'espace de numérotation à gérer par l'IANA.

Le paragraphe 3.1 définit une nouvelle extension IP mobile, l'extension Demande de tunnel UDP. Le numéro de type de cette extension est 144. Cette extension introduit un nouvel espace de numérotation de sous type où la valeur 0 a été allouée à cette extension. L'approbation des nouveaux numéros de sous-type d'extension de demande de tunnel est soumise à revue d'expert, et une spécification est exigée [RFC2434].

Le paragraphe 3.2 définit une nouvelle extension IP mobile, l'extension Réponse de tunnel UDP. La valeur du type de cette extension est 44. Cette extension introduit un nouvel espace de numérotation de sous-type où la valeur 0 a été allouée à cette extension. L'approbation des nouveaux numéros de sous-type d'extension Réponse de tunnel est soumise à révision par expert, et une spécification est exigée [RFC2434].

Le paragraphe 3.3 définit un nouveau message IP mobile, le message Données de tunnel. La valeur du type de ce message est 4.

Le paragraphe 3.5 définit un nouveau code d'erreur, ERROR_HA_UDP_ENCAP_UNAVAIL : "Encapsulation de tunnel UDP demandée indisponible", de l'espace de numérotation pour les valeurs définies pour être utilisées avec le champ Code des messages de réponse d'enregistrement IP mobile. Le numéro de code 142 a été alloué du sous-ensemble "Codes d'erreur provenant de l'agent de rattachement".

Les valeurs pour le champ Prochain en-tête dans le message Données de tunnel MIP (paragraphe 3.3) devront être les mêmes que celles utilisées pour le champ Protocole de l'en-tête IP [RFC0791], et n'exigent pas de nouvelle allocation de numéro.

9. Droits de propriété intellectuelle

Des droits de propriété intellectuelle ont été notifiés à l'IETF, revendiqués à l'égard de tout ou partie de la spécification contenue dans le présent document. Pour plus d'informations, consulter la liste en ligne des droits revendiqués à www.ietf.org/ipr.html.

10. Remerciements

Beaucoup du texte du paragraphe 4.2 a été emprunté presque mot pour mot à la [RFC2003], Encapsulation IP dans IP.

L'ajout de la prise en charge du cas de l'agent étranger a été suggéré par George Tsirtsis et Frode B. Nilsen. Roy Jose a soulevé un problème de mise à jour de liens, et Frode, Roy et George ont montré qu'il y a des cas où des chemins triangulaires peuvent fonctionner, et ont suggéré que le tunnelage inverse n'a pas besoin d'être obligatoire. Roy et Qiang Zhang ont attiré notre attention sur un certain nombre de paragraphes qui devaient être corrigés ou rédigés plus clairement.

Phil Roberts a aidé a arrondir un certain nombre d'angles. Farid Adrangi a soulevé le problème du déni de service maintenant traité dans la Section 6 Considérations sur la sécurité. Les utiles commentaires de Francis Dupont nous ont fait étendre la section des considérations sur la sécurité pour la compléter et la préciser. Milind Kulkarni et Madhavi Chandra ont soulevé la question de l'exigence d'une correspondance entre la source de l'agent étranger et les adresses d'entretien lorsque le mécanisme est utilisé par un FA, et ont aussi contribué à un certain nombre de précisions dans le texte.

Merci aussi à nos co-auteurs, Ilkka Pietikainen, Antti Nuopponen et Timo Aalto de Netseal et à Hans Sjostrand, Fredrik Johansson et Erik Liden de ipUnplugged. Ils ont lu et relu le texte, et contribué à de nombreuses corrections et ajouts précieux.

11. 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.

[RFC1701] S. Hanks, T. Li, D. Farinacci et P. Traina, "Encapsulation générique d'acheminement (GRE)", octobre 1994. *(Info.)*

[RFC2003] C. Perkins, "Encapsulation de IP dans IP", octobre 1996.

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

[RFC2019] M. Crawford, "Transmission de paquets IPv6 sur FDDI", octobre 1996. (*Obsolète, voir* RFC2467) *(P.S.)*

[RFC2434] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, octobre, 1998. *(Rendue obsolète par la* RFC5226)

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

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

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

12. Références pour information

[RFC2663] P. Srisuresh, M. Holdrege, "Terminologie et considérations sur les traducteurs d'adresse réseau IP (NAT)", août 1999. *(Information)*

[RFC3022] P. Srisuresh, K. Egevang, "Traducteur d'adresse réseau IP traditionnel", janvier 2001. *(Information)*

[RFC3424] L. Daigle, éd., IAB, "Considérations de l'IAB sur la réparation d'auto adressage unilatéral (UNSAF) à travers la traduction d'adresse réseau", novembre 2002. *(Information)*

13. Adresse des auteurs

Henrik Levkowetz
ipUnplugged AB
Arenavagen 23
Stockholm S-121 28
SWEDEN
téléphone : +46 708 32 16 08
mél : henrik@levkowetz.com

Sami Vaarala
Netseal
Niittykatu 6
Espoo 02201
FINLAND
téléphone : +358 9 435 310
mél : sami.vaarala@iki.fi

14. Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est actuellement fourni par l'Internet Society.