Groupe de travail Réseau
Request for Comments : 3024
RFC rendue obsolète : 2344
Catégorie : En cours de normalisation

G. Montenegro, éditeur
Sun Microsystems, Inc.
janvier 2001
Traduction Claude Brière de L'Isle

Tunnelage inverse pour IP mobile, révision

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 protocole Internet mobile utilise le tunnelage de l'agent de rattachement à l'adresse d'entretien du nœud mobile, mais rarement dans la direction inverse. Normalement, un nœud mobile envoie ses paquets à travers un routeur sur le réseau étranger, et suppose que l'acheminement est indépendant de l'adresse de source. Lorsque cette hypothèse n'est pas vraie, il est pratique d'établir un tunnel inverse topologiquement correct de l'adresse d'entretien à l'agent de rattachement.

Le présent document propose des extensions rétro compatibles à IP mobile pour prendre en charge les tunnels inverses topologiquement corrects. Le présent document ne tente pas de résoudre les problèmes posés par les pare-feu situés entre l'agent de rattachement et l'adresse d'entretien du nœud mobile.

Le présent document rend obsolète la RFC2344.

Table of Contents

1. Introduction

Le paragraphe 1.3 de la spécification IP mobile [RFC2002] fait la liste des hypothèses suivantes :

On suppose que les datagrammes IP en envoi individuel sont acheminés sur la base de l'adresse de destination dans l'en-tête du datagramme (c'est-à-dire, pas par l'adresse de source).

À cause de problèmes de sécurité (par exemple, attaques par usurpation d'identité IP) et conformément à la [RFC2267] et aux conseils du CERT [CERT] à cet effet, les routeurs qui rompent avec cette hypothèse sont de plus en plus courants.

En présence de tels routeurs, l'adresse IP de source et de destination dans un paquet doit être topologiquement correcte. Le tunnel vers l'avant se conforme à cela, car ses points d'extrémité (adresse d'agent de rattachement et adresse d'entretien) sont des adresses correctement allouées pour leurs situations respectives. D'un autre côté, l'adresse IP de source d'un paquet transmis par le nœud mobile ne correspond pas au préfixe du réseau d'où il émane.

Le présent document discute des tunnels inverses topologiquement corrects.

IP mobile n'impose pas l'utilisation des tunnels inverses dans le contexte de l'acheminement des datagrammes en diffusion groupée et des routeurs mobiles. Cependant, l'adresse IP de source est réglée sur l'adresse de rattachement du nœud mobile, de sorte que ces tunnels ne sont pas topologiquement corrects.

Remarquer qu'il y a plusieurs utilisations des tunnels inverses, sans considération de leur correction topologique :
- Routeurs mobiles : les tunnels inverses évitent le besoin de tunnelage récurrent [RFC2002].
- Diffusion groupée : les tunnels inverses permettent à un nœud mobile loin de son point de rattachement de (1) se joindre à des groupes de diffusion groupée dans son réseau de rattachement, et (2) de transmettre des paquets en diffusion groupée tels qu'ils émanent de son réseau de rattachement [RFC2002].
- Le TTL des paquets envoyés par le nœud mobile (par exemple, lors de l'envoi de paquets à d'autres hôtes dans son réseau de rattachement) peut être si bas qu'ils peuvent expirer avant d'atteindre leur destination. Un tunnel inverse résout le problème car il représente une diminution de TTL de un [5].

1.1 Terminologie

L'exposé ci-dessous utilise des termes définis dans la spécification IP mobile. De plus, on utilise les termes suivants :

Tunnel vers l'avant
Un tunnel qui achemine 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
Un tunnel qui commence à l'adresse d'entretien du nœud mobile et se termine à l'agent de rattachement.

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 Hypothèses

La mobilité est restreinte à un espace commun d'adresses IP (c'est-à-dire que le système d'acheminement entre, disons, le nœud mobile et l'agent de rattachement n'est pas partagé en un réseau "privé" et un réseau "public").

Le présent document ne tente pas de résoudre le problème de la traversée de pare-feu. Il suppose plutôt qu'une des conditions suivantes est vraie :

- Il n'y a pas de pare-feu intercalé le long du chemin des paquets tunnelés.
- Tout pare-feu intercalé partage l'association de sécurité nécessaire au traitement de tout en-tête d'authentification [RFC2402] ou de chiffrement [RFC2406] qui pourrait avoir été ajouté aux paquets tunnelés.

Les tunnels inverses considérés ici sont symétriques, c'est-à-dire qu'ils utilisent la même configuration (méthode d'encapsulation, points d'extrémité d'adresse IP) que le tunnel vers l'avant. L'encapsulation IP dans IP [RFC2003] est supposée sauf mention contraire.

L'optimisation de chemin [RFC3775] introduit des tunnels vers l'avant initiés chez un hôte correspondant. Comme un nœud mobile peut ne pas savoir si l'hôte correspondant peut désencapsuler les paquets, les tunnels inverses dans ce contexte ne sont pas discutés ici.

1.3 Justification

Pourquoi ne pas laisser le nœud mobile initier lui-même le tunnel avec l'agent de rattachement ? C'est bien sûr ce qu'il devrait faire si il fonctionne déjà avec une adresse d'entretien colocalisée topologiquement correcte.

Cependant, un des principaux objectifs de la spécification IP mobile n'est pas d'exiger ce mode de fonctionnement.

Les mécanismes décrits dans le présent document sont principalement destinées à être utilisés par des nœuds mobiles qui s'appuient sur l'agent étranger pour la prise en charge du tunnel vers l'avant. Il est souhaitable de continuer de prendre en charge des nœuds mobiles, même en présence de routeurs filtrants.

2. Généralités

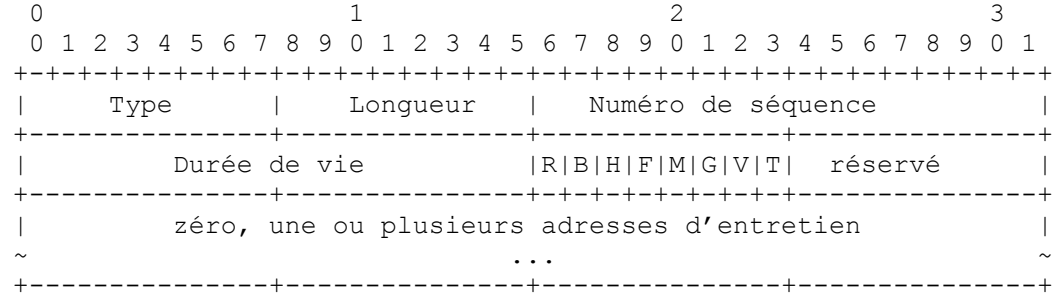
Un nœud mobile arrive à un réseau étranger, écoute les annonces d'agent et choisit un agent étranger qui prend en charge les tunnels inverses. Il demande ce service lorsque il s'enregistre à travers l'agent étranger choisi. À ce moment, et selon la façon dont le nœud mobile souhaite livrer les paquets à l'agent étranger, il demande aussi soit le style de livraison directe, soit le style de livraison encapsulante (section 5).

Dans le style de livraison directe, le nœud mobile désigne l'agent étranger comme son routeur par défaut et procède à l'envoi des paquets directement à l'agent étranger, c'est-à-dire, sans encapsulation. L'agent étranger les intercepte, et les tunnelle à l'agent de rattachement.

Dans le style de livraison encapsulante, le nœud mobile encapsule tous ses paquets sortants à l'agent étranger. L'agent étranger les désencapsule et les re-tunnelle à l'agent de rattachement, en utilisant l'adresse d'entretien de l'agent étranger comme point d'entrée de ce nouveau tunnel.

3. Nouveaux formats de paquet

3.1 Extension Annonce d'agent de mobilité



Le seul changement à l'extension Annonce d'agent de mobilité [RFC2002] est le bit 'T' supplémentaire :

T : l'agent offre le service de tunnel inverse.

Un agent étranger qui établit le bit 'T' DOIT prendre en charge le style de livraison directe. Le style de livraison encapsulante

DEVRAIT aussi être pris en charge (Section 5).

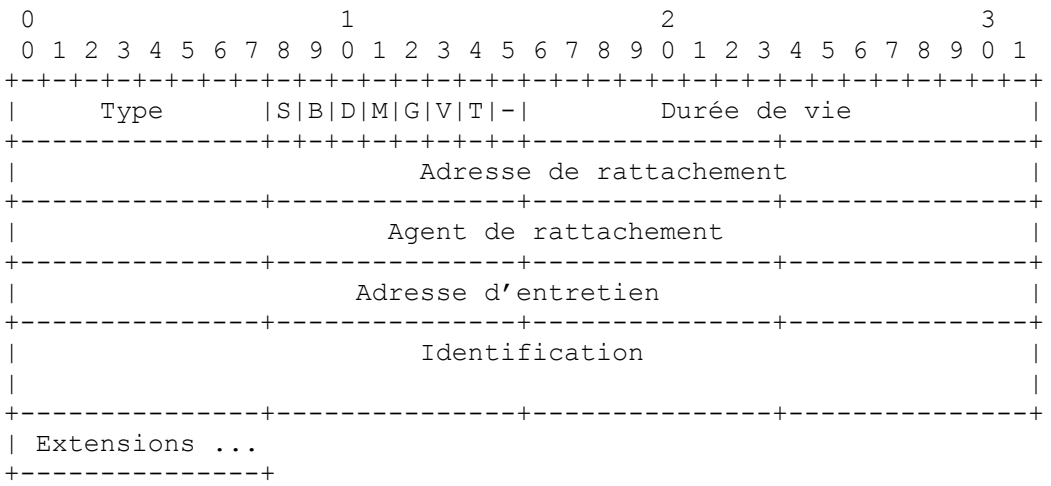
En utilisant cette information, un nœud mobile est capable de choisir un agent étranger qui prend en charge les tunnels inverses. Noter que si un nœud mobile ne comprend pas ce bit, il l'ignore simplement selon la [RFC2002].

3.2 Demande d'enregistrement

La prise en charge du tunnelage inverse est ajoutée directement dans la demande d'enregistrement en utilisant un des bits "réservé". Si un agent étranger ou de rattachement qui ne prend pas en charge les tunnels inverses reçoit une demande avec le bit 'T' établi, la demande d'enregistrement échoue. Il en résulte un refus d'enregistrement (les codes d'échec sont spécifiés au paragraphe 3.4).

Les agents de rattachement NE DEVRAIENT PAS refuser de fournir la prise en charge de tunnel inverse, parce que ils "DEVRAIENT être capables de désencapsuler et ensuite livrer les paquets adressés à eux-mêmes, envoyés par un nœud mobile" [RFC2002]. Dans le cas de tunnels inverses topologiquement corrects, les paquets ne sont pas envoyés par le nœud mobile tel que désigné par son adresse de rattachement. C'est plutôt l'adresse IP de source la plus externe (encapsulante) de tels datagrammes qui est l'adresse d'entretien du nœud mobile.

Dans les demandes d'enregistrement envoyées par un nœud mobile, le champ Durée de vie (TTL) dans l'en-tête IP DOIT être réglé à 255. Cela limite une attaque de déni de service dans laquelle des hôtes malveillants envoient de fausses demandes d'enregistrement (voir la Section 6).



Le seul changement au paquet de demande d'enregistrement est le bit 'T' supplémentaire :

T : Si le bit 'T' est établi, le nœud mobile demande à son agent de rattachement d'accepter un tunnel inverse à partir de l'adresse d'entretien. Les nœuds mobile qui utilisent une adresse d'entretien d'agent étranger demandent à l'agent étranger de faire le tunnelage inverse de ses paquets.

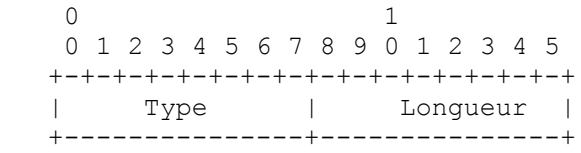
3.3 Extension Style de livraison encapsulant

L'extension Style de livraison encapsulant PEUT être incluse par le nœud mobile dans des demandes d'enregistrement pour mieux spécifier le comportement d'inversion de tunnel. Elle est supposée n'être utilisée que par l'agent étranger. En conséquence, l'agent étranger DOIT consommer cette extension (c'est-à-dire qu'il ne doit pas la relayer à l'agent de rattachement ou l'inclure dans ses réponses au nœud mobile). Selon le paragraphe 3.6.1.3 de la [RFC2002], le nœud mobile DOIT inclure l'extension Style de livraison encapsulant après l'extension Authentification de rattachement mobile, et avant l'extension Authentification de mobile étranger, si elles sont présentes.

L'extension Style de livraison encapsulant NE DOIT PAS être incluse si le bit 'T' n'est pas établi dans la demande d'enregistrement.

Si cette extension est absente, la livraison directe est supposée. L'encapsulation est faite conformément à ce qui a été négocié pour le tunnel vers l'avant (c'est-à-dire que IP dans IP est supposé sauf mention contraire). Pour plus de détails sur les styles de livraison, prière de se reporter à la section 5.

Les agents étrangers DEVRAIENT prendre en charge l'extension Style de livraison encapsulant.



Type : 130
Longueur : 0

3.4 Nouveaux codes de réponse d'enregistrement

Les réponses d'enregistrement d'agent étranger et de rattachement DOIVENT convoyer l'information de l'échec éventuel de la demande de tunnel inverse. Ces nouveaux codes de réponse sont définis :

Service refusé par l'agent étranger :
- 74 tunnel inverse demandé indisponible
- 75 tunnel inverse obligatoire et le bit 'T' n'est pas établi
- 76 nœud mobile trop distant
- 79 style de livraison non accepté

Note : Le code 79 n'a pas encore été alloué par l'IANA.

Service refusé par l'agent de rattachement :
- 137 tunnel inverse demandé indisponible
- 138 tunnel inverse obligatoire et le bit 'T' n'est pas établi
- 139 encapsulation demandée indisponible

En réponse à une demande d'enregistrement avec le bit 'T' établi, les nœuds mobiles peuvent recevoir (et DOIVENT accepter) le code 70 (demande mal formée) d'un agent étranger et le code 134 (demande mal formée) d'un agent de rattachement. Cependant, les agent étrangers et de rattachement qui prennent en charge l'inversion de tunnel DOIVENT utiliser respectivement les codes 74 et 137.

En plus de l'établissement du bit 'T', le nœud mobile PEUT aussi demander le style de livraison encapsulant en incluant l'extension correspondante. Si un agent étranger ne met pas en œuvre le style de livraison encapsulant, il DOIT répondre au nœud mobile avec le code 79 (style de livraison non accepté). Cela s'applique aussi si l'agent étranger ne prend pas en charge un style de livraison demandé qui pourrait être défini à l'avenir.

L'absence du bit 'T' dans une demande d'enregistrement PEUT traduire un refus avec les codes 75 et 138 chez, respectivement, l'agent étranger et l'agent de rattachement.

Le tunnel vers l'avant et le tunnel inverse sont symétriques, c'est-à-dire, tous deux sont capables d'utiliser les mêmes options de tunnelage négociées à l'enregistrement. Cela implique que l'agent de rattachement DOIT refuser les enregistrements si une forme non acceptée d'enregistrement de tunnelage est demandée (code 139). Noter que IP mobile [RFC2002] définit déjà le code d'échec analogue 72 pour l'usage de l'agent étranger.

4. Changements dans le comportement protocolaire

Sauf spécification contraire, le comportement spécifié par IP mobile [RFC2002] est supposé. En particulier, si une des deux entités partage une association de sécurité de mobilité, elle DOIT utiliser l'extension d'authentification appropriée (extension d'authentification mobile-étranger, étranger-rattachement ou mobile-rattachement) lors de l'échange de datagrammes de protocole d'enregistrement. Une extension d'authentification admissible (par exemple l'extension d'authentification mobile-rattachement) DOIT toujours être présente pour authentifier les messages d'enregistrement entre un nœud mobile et son agent de rattachement.

Le tunnelage inverse impose aux entités mobiles des exigences de traitement de protocole supplémentaires. Les différences dans le comportement de protocole par rapport à IP mobile [RFC2002] sont spécifiées dans les paragraphes qui suivent.

4.1 Considérations sur le nœud mobile

Ce paragraphe décrit comment le nœud mobile traite les enregistrements qui demandent un tunnel inverse.

4.1.1 Envoi des demandes d'enregistrement à l'agent étranger

En plus des considérations de la [RFC2002], un nœud mobile établit le bit 'T' dans sa demande d'enregistrement pour demander un tunnel inverse.

Le nœud mobile DOIT régler le champ TTL de l'en-tête IP à 255. Cela est destiné à limiter l'attaque de capture du tunnel inverse (Section 6).

Le nœud mobile PEUT facultativement inclure une extension Style de livraison encapsulant.

4.1.2 Réception des réponses d'enregistrement provenant de l'agent étranger

Les réponses valides possibles sont :

- Un refus d'enregistrement produit par l'agent de rattachement ou par l'agent étranger :
  a. Le nœud mobile suit les lignes directrices de vérification d'erreur de la [RFC2002], et selon le code de réponse, PEUT essayer de modifier la demande d'enregistrement (par exemple, en éliminant la demande d'autres formes d'encapsulation ou de style de livraison) et en produisant un nouvel enregistrement.
  b. Selon le code de réponse, le nœud mobile PEUT essayer de mettre à zéro le bit 'T', éliminant l'extension Style de livraison encapsulant (si elle était présente) et en produisant un nouvel enregistrement. Noter qu'après avoir fait cela, l'enregistrement peut réussir, mais du fait de l'absence d'un tunnel inverse, le transfert des données peut n'être pas possible.
- L'agent de rattachement retourne une réponse d'enregistrement indiquant que le service sera fourni.

Dans ce dernier cas, le nœud mobile a réussi à établir un tunnel inverse entre son adresse d'entretien et son agent de rattachement. Si le nœud mobile fonctionne avec une adresse d'entretien colocalisée, il PEUT encapsuler les données sortantes car l'adresse de destination de l'en-tête externe est celle de l'agent de rattachement. Cette capacité de tunnelage inverse sélectif des paquets est exposée plus avant au paragraphe 5.4.

Si l'adresse d'entretien appartient à un agent étranger séparé, le nœud mobile DOIT employer le style de livraison qui a été demandé (direct ou encapsulant) et poursuivre comme spécifié à la Section 5.

Une réponse d'enregistrement réussi est une assurance que l'agent étranger et l'agent de rattachement prennent tous deux en charge les formes d'encapsulation de remplacement (autres que IP dans IP) qui ont été demandées. En conséquence, le nœud mobile PEUT les utiliser à discrétion.

4.2 Considérations sur l'agent étranger

Ce paragraphe décrit comment l'agent étranger traite les enregistrements qui demandent un tunnel inverse.

4.2.1 Réception des demandes d'enregistrement provenant du nœud mobile

Un agent étranger qui reçoit une demande d'enregistrement avec le bit 'T' établi traite le paquet comme spécifié dans la [RFC2002], et détermine si il peut s'accommoder de la demande de tunnel vers l'avant. Si il ne le peut pas, il retourne un code approprié. En particulier, si l'agent étranger n'est pas en mesure de prendre en charge la forme d'encapsulation demandée, il DOIT retourner le code 72. Si il ne peut pas prendre en charge la forme demandée de style de livraison, il DOIT retourner le code 79 (style de livraison non accepté).

L'agent étranger PEUT rejeter les demandes d'enregistrement sans le bit 'T' établi en les refusant avec le code 75 (tunnel inverse obligatoire et bit 'T' non établi).

L'agent étranger DOIT vérifier que le champ TTL de l'en-tête IP est réglé à 255. Autrement, il DOIT rejeter l'enregistrement avec le code 76 (nœud mobile trop distant). L'agent étranger DOIT limiter le taux d'envoi de ces réponses d'enregistrement à un maximum de une par seconde.

Comme dernière vérification, l'agent étranger vérifie qu'il peut prendre en charge le tunnel inverse avec la même configuration. Si il ne le peut pas, il DOIT retourner une réponse d'enregistrement refusant la demande avec le code 74 (tunnel inverse demandé indisponible).

4.2.2 Relais des demandes d'enregistrement à l'agent de rattachement

Autrement, l'agent étranger DOIT relayer la demande d'enregistrement à l'agent de rattachement.

À réception d'une réponse d'enregistrement qui satisfait aux vérifications de validité, l'agent étranger DOIT mettre à jour sa liste de visiteurs, incluant l'indication qu'il a été accordé à ce nœud mobile un tunnel inverse et le style de livraison attendu (section 5).

Pendant que cette entrée de liste de visiteurs est en vigueur, l'agent étranger DOIT traiter le trafic entrant conformément au style de livraison, l'encapsuler et le tunneler de l'adresse d'entretien à l'adresse de l'agent de rattachement.

4.3 Considérations sur l'agent de rattachement

Ce paragraphe décrit comment l'agent de rattachement traite les enregistrements qui demandent un tunnel inverse.

4.3.1 Réception des demandes d'enregistrement provenant de l'agent étranger

Un agent de rattachement qui reçoit une demande d'enregistrement avec le bit 'T' établi traite le paquet comme spécifié dans la [RFC2002] et détermine si il peut s'accommoder de la demande de tunnel vers l'avant. Si il ne le peut pas, il retourne un code approprié. En particulier, si l'agent de rattachement n'est pas en mesure de prendre en charge la forme demandée d'encapsulation, il DOIT retourner le code 139 (encapsulation demandée indisponible).

L'agent de rattachement PEUT rejeter les demandes d'enregistrement qui n'ont pas le bit 'T' établi en les refusant avec le code 138 (tunnel inverse obligatoire et bit ' T' non établi).

En dernière vérification, l'agent de rattachement détermine si il peut prendre en charge un tunnel inverse avec la même configuration que le tunnel vers l'avant. Si il ne le peut pas, il DOIT renvoyer un refus d'enregistrement avec le code 137 (tunnel inverse demandé indisponible).

À réception d'une demande d'enregistrement qui satisfait aux vérifications de validité, l'agent de rattachement DOIT mettre à jour sa liste de liens de mobilité pour indiquer qu'il a été accordé à ce nœud mobile un tunnel inverse et le type d'encapsulation attendu.

4.3.2 Envoi des réponses d'enregistrement à l'agent étranger

En réponse à une demande d'enregistrement valide, un agent de rattachement DOIT produire une réponse d'enregistrement au nœud mobile.

Après un enregistrement réussi, l'agent de rattachement peut recevoir des paquets encapsulés adressés à lui-même. La désencapsulation de tels paquets et leur injection aveugle dans le réseau est une faiblesse potentielle de la sécurité (paragraphe 6.1). En conséquence, l'agent de rattachement DOIT mettre en œuvre, et par défaut, DEVRAIT activer les vérifications suivantes pour les paquets encapsulés qui lui sont adressés :

L'agent de rattachement recherche un lien de mobilité dont l'adresse d'entretien est la source de l'en-tête externe, et dont l'adresse de nœud mobile est la source de l'en-tête interne.

Si un tel lien n'est pas trouvé, ou si le paquet utilise un mécanisme d'encapsulation qui n'a pas été négocié à l'enregistrement l'agent de rattachement DOIT éliminer en silence le paquet et DEVRAIT enregistrer l'événement comme exception de sécurité.

Les agents de rattachement qui terminent des tunnels sans relation avec IP mobile (par exemple, des tunnels de diffusion groupée) PEUVENT désactiver la vérification ci-dessus, mais cette pratique est déconseillée pour les raisons susmentionnées.

Pendant que l'enregistrement est en vigueur, un agent de rattachement DOIT traiter chaque paquet de tunnel inverse (comme déterminé par des vérifications comme celle ci-dessus) en le désencapsulant, en récupérant le paquet original, puis en le transmettant au nom de son envoyeur (le nœud mobile) à l'adresse de destination (l'hôte correspondant).

5. Styles de livraison de nœud mobile à agent étranger

Cette section spécifie comment le nœud mobile envoie son trafic de données via l'agent étranger. Dans tous les cas, le nœud mobile apprend l'adresse de couche liaison de l'agent étranger de l'en-tête de couche de liaison dans l'annonce de l'agent.

5.1 Style de livraison directe

Le mécanisme de livraison est très simple à mettre en œuvre au nœud mobile, et utilise de petits paquets (non encapsulés) sur la liaison entre le nœud mobile et l'agent étranger (une liaison potentiellement très lente). Cependant, il ne prend en charge que le tunnelage inverse de paquets en envoi individuel, et ne permet pas l'inversion de tunnel sélective (paragraphe 5.4).

5.1.1 Traitement de paquet

Le nœud mobile DOIT désigner l'agent étranger comme son routeur par défaut. Ne pas le faire ne va pas garantir l'encapsulation de tout le trafic sortant du nœud mobile, et contredit l'objet du tunnel inverse. L'agent étranger DOIT :
- détecter les paquets envoyés par le nœud mobile, et
- modifier sa fonction de transmission pour les encapsuler avant la transmission.

5.1.2 Format et champs d'en-tête de paquet

Ce paragraphe montre le format de l'en-tête de paquet utilisé par le style de livraison directe. Les formats indiqués supposent l'encapsulation de IP dans IP [RFC2003].

Format de paquet reçu par l'agent étranger (style de livraison directe) :
Champs IP :
Adresse de source = adresse de rattachement du nœud mobile
Adresse de destination = adresse du protocole de couche supérieure de l'hôte correspondant

Format de paquet transmis par l'agent étranger (style de livraison directe) :
Champs IP (en-tête encapsulant) :
Adresse de source = adresse d'entretien de l'agent étranger
Adresse de destination = adresse de l'agent de rattachement
Champ Protocole : 4 (IP dans IP)
Champs IP (en-tête d'origine) :
Adresse de sources = adresse de rattachement du nœud mobile
Adresse de destination = adresse du protocole de couche supérieure de l'hôte correspondant

Ces champs de l'en-tête encapsulant DOIVENT être choisis comme suit :

Adresse IP de source	Copiée du champ Adresse d'entretien dans la demande d'enregistrement.
Adresse IP de destination	Copiée du champ Agent de rattachement au sein de la plus récente réponse d'enregistrement réussie
Champ Protocole IP	Par défaut, 4 (IP dans IP [RFC2003]), mais d'autres méthodes d'encapsulation PEUVENT être utilisées comme négocié au moment de l'enregistrement.

5.2 Style de livraison encapsulant

Ce mécanisme exige que le nœud mobile mette en œuvre l'encapsulation, et dirige explicitement les paquets sur l'agent étranger en le désignant comme l'adresse de destination dans un nouvel en-tête le plus externe. Les nœuds mobiles qui souhaitent envoyer des paquets en diffusion ou en diffusion groupée DOIVENT utiliser le style de livraison encapsulant.

5.2.1 Traitement de paquet

L'agent étranger ne modifie pas sa fonction de transmission. Il reçoit plutôt un paquet encapsulé et après avoir vérifié qu'il a été envoyé par le nœud mobile :
- il le désencapsule pour récupérer le paquet interne,
- il le réencapsule, et l'envoie à l'agent de rattachement.

Si un agent étranger reçoit un paquet non encapsulé d'un nœud mobile qui avait explicitement demandé le style de livraison encapsulant, l'agent étranger NE DOIT PAS alors faire un tunnel inverse pour un tel paquet et DOIT plutôt le transmettre en utilisant les mécanismes d'acheminement IP standard.

5.2.2 Format et champs d'en-tête de paquet

Ce paragraphe montre le format des en-têtes de paquet utilisés par le style de livraison encapsulant. Les formats montrés supposent l'encapsulation IP dans IP [RFC2003].

Format de paquet reçu par l'agent étranger (style de livraison encapsulant) :
Champs IP (en-tête encapsulant) :
Adresse de source = adresse de rattachement du nœud mobile
Adresse de destination = adresse de l'agent étranger
Champ Protocole : 4 (IP dans IP)
Champs IP (en-tête d'origine) :
Adresse de source = adresse de rattachement du nœud mobile
Adresse de destination = adresse de protocole de couche supérieure de l'hôte correspondant

Les champs de l'en-tête IP encapsulant DOIVENT être choisis comme suit :
Adresse IP de source = adresse de rattachement du nœud mobile
Adresse IP de destination = adresse de l'agent telle qu'apprise de l'adresse IP de source de la plus récente réponse d'enregistrement réussie de l'agent.
Champ Protocole IP = Par défaut, 4 (IP dans IP [RFC2003]), mais d'autres méthodes d'encapsulation PEUVENT être utilisées comme négocié au moment de l'enregistrement.

Format de paquet transmis par l'agent étranger (style de livraison encapsulant) :
Champs IP (en-tête encapsulant) :
Adresse de source = adresse d'entretien de l'agent étranger
Adresse de destination = adresse de l'agent de rattachement
Champ Protocole : 4 (IP dans IP)
Champs IP (en-tête d'origine) :
Adresse de source = adresse de rattachement du nœud mobile
Adresse de destination = adresse de protocole de couche supérieure de l'hôte correspondant

Ces champs de l'en-tête IP encapsulant DOIVENT être choisis comme suit :
Adresse IP de source : Copiée du champ Adresse d'entretien dans la demande d'enregistrement.
Adresse IP de destination : Copiée du champ Agent de rattachement dans la plus récente réponse d'enregistrement réussi.
Champ Protocole IP : par défaut, 4 (IP dans IP [RFC2003]), mais d'autres méthodes d'encapsulation PEUVENT être utilisées comme négocié au moment de l'enregistrement.

5.3 Prise en charge des datagrammes de diffusion et diffusion groupée

Si un nœud mobile fonctionne avec une adresse d'entretien colocalisée, les datagrammes de diffusion et diffusion groupée sont traités conformément aux paragraphes 4.3 et 4.4 de la [RFC2002]. Les nœuds mobiles qui utilisent une adresse d'entretien d'agent étranger PEUVENT avoir leurs datagrammes en diffusion et diffusion groupée tunnelés en inverse par l'agent étranger. Cependant, tout nœud mobile qui fait ainsi DOIT utiliser le style de livraison encapsulant.

Cela livre le datagramme au seul agent étranger. Celui-ci le désencapsule et le traite ensuite comme tout autre paquet provenant du nœud mobile,à savoir en le transmettant par tunnel inverse à l'agent de rattachement.

5.4 Tunnelage inverse sélectif

Les paquets destinés à des ressources locales (par exemple, une imprimante du voisinage) peuvent n'être pas affectés par le filtrage d'entrée. Un nœud mobile avec une adresse d'entretien colocalisée PEUT optimiser la livraison de ces paquets en ne leur faisant pas subir le tunnel inverse. D'un autre côté, un nœud mobile qui utilise l'adresse d'entretien d'un agent étranger PEUT utiliser cette capacité de tunnel inverse sélectif en demandant le style de livraison encapsulant, et en suivant ces lignes directrices :
Paquets NON destinés à passer par le tunnel inverse :
Envoyés en utilisant le style de livraison direct. L'agent étranger DOIT traiter ces paquets comme du trafic régulier : il PEUT les transmettre mais NE DOIT PAS les envoyer par tunnel inverse à l'agent de rattachement.
Paquets destinées à passer par le tunnel inverse :
Envoyés en utilisant le style de livraison encapsulant. L'agent étranger DOIT traiter ces paquets comme spécifié au paragraphe 5.2 : ils DOIVENT être transmis par tunnel inverse à l'agent de rattachement.

6. Considérations sur la sécurité

Les extensions présentées dans ce document sont soumises aux considérations sur la sécurité exposées dans la spécification IP mobile [RFC2002]. Essentiellement, la création des deux tunnels, vers l'avant, et inverse, implique une procédure d'authentification, qui réduit les risques d'attaques.

6.1 Capture de tunnel inverse et attaques de déni de service

Une fois le tunnel établi, un nœud malveillant pourrait le capturer pour injecter des paquets dans le réseau. Les tunnels inverses pourraient exacerber ce problème, parce que lorsque ils atteignent le point de sortie du tunnel, les paquets sont transmis au delà du réseau local. Ce problème est aussi présent dans la spécification IP mobile, car il impose déjà l'utilisation des tunnels inverses pour certaines applications.

Les échanges non authentifiés qui impliquent l'agent étranger permettent à un nœud malveillant de se faire passer pour un nœud mobile valide et de rediriger un tunnel inverse existant sur un autre agent de rattachement, peut-être un autre nœud malveillant. Le meilleur moyen pour se protéger contre ces attaques est d'employer les extensions d'authentification mobile-étranger et étranger-rattachement définies dans la [RFC2002].

Si les associations de sécurité de mobilité nécessaires ne sont pas disponibles, le présent document introduit un mécanisme pour réduire la gamme et l'efficacité des attaques. Le nœud mobile DOIT régler à 255 la valeur du TTL dans les en-têtes IP des demandes d'enregistrement envoyées à l'agent étranger. Cela empêche les nœuds malveillants qui sont éloignés de plus d'un bond de se faire passer pour des nœuds mobiles valides. Des codes supplémentaires à utiliser pour les refus d'enregistrement rendent les attaques qui surviennent plus faciles à retracer.

Avec l'objectif de réduire encore les attaques, le groupe de travail IP mobile a examiné d'autres mécanismes impliquant l'utilisation de l'état non authentifié. Cependant, cela introduit des possibilités d'attaques de déni de service. Le consensus a été que ce compromis allait trop loin sur des mécanismes qui ne garantissent rien de plus qu'une faible protection (non cryptographique) contre les attaques.

6.2 Filtrage d'entrée

On s'est interrogé sur l'efficacité à long terme des tunnels inverses en présence de filtrages d'entrée. La conjecture est que les administrateurs de réseau vont cibler les paquets qui font l'objet de tunnelage inverse (les paquets encapsulés IP dans IP) pour le filtrage. La recommandation sur le filtrage d'entrée explique pourquoi ce n'est pas le cas [RFC2267] : "Retracer la source d'une attaque est plus simple lorsque la source est très probablement "valide"."

6.3 Tunnelage inverse pour espaces d'adresses disparates

Des implications pour la sécurité découlent de l'utilisation par l'agent étranger des informations de couche liaison pour choisir le tunnel inverse approprié pour les paquets d'un nœud mobile (paragraphe A.3). Les couches de liaison non authentifiées permettent à un nœud mobile malveillant de faire un mauvais usage du tunnel inverse existant d'un autre, et d'injecter des paquets dans le réseau.

Pour que cette solution soit viable, la couche de liaison DOIT authentifier en toute sécurité le trafic reçu par l'agent étranger en provenance des nœuds mobiles. Les technologies de couche de liaison non authentifiée (par exemple, l'ethernet partagé) ne sont pas recommandées pour mettre en œuvre la prise en charge d'adresses disparates.

7. Considérations relatives à l'IANA

L'extension Style de livraison encapsulant défini au paragraphe 3.3 est une extension d'enregistrement IP mobile telle que définie dans la [RFC2002]. L'IANA a alloué la valeur 130 à cette fin au moment de la publication de la [RFC2344].

Les valeurs de code définies au paragraphe 3.4 sont des codes d'erreur comme défini dans la [RFC2002]. Ils correspondent aux valeurs d'erreur associées au rejet par les agents de rattachement et étrangers. Au moment de la publication de la [RFC2344], l'IANA a alloué les codes 74 à 76 pour les rejets d'agent étranger et les codes 137 à 139 pour les rejets d'agent de rattachement. Le code pour 'style de livraison non accepté' a reçu la valeur de 79 de l'IANA.

8. Remerciements

Le style de livraison encapsulant a été proposé par Charlie Perkins. Jim Solomon a été l'instrument de formatage du présent document sous sa forme actuelle. Merci à Samita Chakrabarti pour ses précieux commentaires sur la prise en charge de l'espace d'adresses disparate, et pour la plus grande partie du texte du paragraphe A.4.

Références

[CERT] Computer Emergency Response Team (CERT), "IP Spoofing Attacks and Hijacked Terminal Connections", CA-95:01, janvier 1995. Disponible via ftp anonyme à info.cert.org dans /pub/cert_advisories.

[RFC1918] Y. Rekhter et autres, "Allocation d'adresse pour les internets privés", BCP 5, février 1996.

[RFC2002] C. Perkins, éd., "Prise en charge de la mobilité sur IP", octobre 1996. (*Obsolète, voirr* RFC5944) *(P.S.)*

[RFC2003] C. Perkins, "Encapsulation de IP dans IP", RFC 2003, octobre 1996.

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

[RFC2267] P. Ferguson, D. Senie, "Filtrage d'entrée de réseau : combattre les attaques de déni de service qui utilisent le déguisement d'adresse de source IP", janvier 1998. (*Obsolète, voir* RFC2827) *(Information)*

[RFC2402] S. Kent et R. Atkinson, "En-tête d'authentification IP", novembre 1998. (*Obsolète, voir* RFC4302, 4305)

[RFC2406] S. Kent et R. Atkinson, "Encapsulation de charge utile de sécurité IP (ESP)", novembre 1998. *(Obsolète, voir* RFC4303)

[RFC2486] B. Aboba, M. Beadles, "Identifiant d'accès réseau", janvier 1999. (*Obsolète, voir* RFC7542) *(P.S.)*

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

[RFC2890] G. Dommety, "Extensions de clé et de numéro de séquence à GRE", septembre 2000. *(P.S.)*

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

[5] Manuel Rodriguez, communication privée, août 1995. *(extêmement intéressante !)*

Adresse de l'éditeur et du président

Les questions sur le présent document peuvent être adressées à :

Gabriel E. Montenegro
Sun Microsystems
Laboratories, Europe
29, chemin du Vieux Chene
38240 Meylan
FRANCE
téléphone : +33 476 18 80 45
mél : gab@sun.com

Le groupe de travail peut être contacté via l'actuel président :

Basavaraj Patil
Nokia Networks
6000 Connection Drive
Irving, TX 75039
USA

téléphone : +1 972-894-6709
Fax : +1 972-894-5349
mél : Raj.Patil@nokia.com

Phil Roberts
Motorola
1501 West Shure Drive
Arlington Heights, IL 60004
USA
téléphone : +1 847-632-3148
mél : QA3445@email.mot.com

Appendice A : Prise en charge d'espace d'adresses disparates

IP mobile [RFC2002] suppose que toutes les entités impliquées (nœud mobile, agent étranger et agent de rattachement) ont des adresses dans le même espace d'adresse à acheminement mondial. Dans de nombreux scénarios de déploiement, lorsque un nœud mobile quitte son réseau de rattachement il peut errer dans une région où son adresse de rattachement n'est pas acheminable ou connue par le système d'acheminement local. De même, les adresses IP de l'agent étranger et de l'agent de rattachement peuvent appartenir à des espaces d'adresses disparates, ce qui empêche leurs échanges directs de messages de protocole d'enregistrement. Ces problèmes sont particulièrement possibles si les entités impliquées utilisent des adresses dans les gammes spécifiées dans la [RFC1918] pour la prise en charge de réseaux privés.

Pour parler précisément, l'utilisation d'adresses privées n'est pas la seule cause. Cela peut, en fait, être très courant, mais la racine du problème est dans l'utilisation d'espaces d'adresses disparates. Par exemple, des entreprises ont souvent plusieurs gammes d'adresses correctement allouées. Elles annoncent normalement l'accessibilité à seulement un sous-ensemble de ces gammes, laissant les autres pour l'usage exclusif du réseau d'entreprise. Comme ces gammes ne sont pas acheminables dans l'Internet général, leur utilisation conduit aux mêmes problèmes que ceux rencontrés avec les adresses "privées", même si elles ne sont pas prises dans les gammes spécifiées dans la RFC1918.

Même si le nœud mobile, l'agent de rattachement, et l'agent étranger, résident tous au sein du même espace d'adresses, des problèmes peuvent survenir si le nœud correspondant ne le fait pas. Cependant, ce problème n'est pas spécifique de IP mobile, et sort du domaine d'application du présent document. Le paragraphe suivant limite encore plus la portée des problèmes qui relèvent de ce document. Un paragraphe suivant explique comment l'inversion de tunnel peut être utilisée pour y faire face.

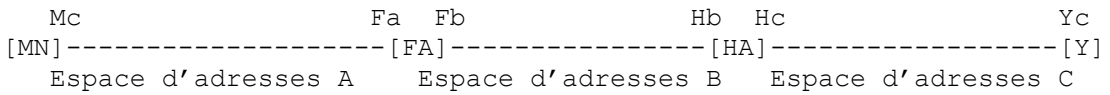
A.1 Portée de la solution de tunnelage inverse

Le tunnelage inverse (comme défini par le présent document) peut être utilisé pour s'arranger des espaces d'adresses disparates, sous les contraintes suivantes :

- Il n'existe aucune disposition pour résoudre le cas dans lequel le nœud correspondant et le nœud mobile sont dans des espaces d'adresses disparates. Cela limite la portée du problème aux seules questions spécifiques de IP mobile.
- L'agent étranger et l'agent de rattachement sont directement joignables de l'un à l'autre par le fait qu'ils résident dans le même espace d'adresses. Cela limite la portée du problème aux seuls cas les plus simples. Cela implique aussi que le protocole d'enregistrement lui-même a un chemin direct entre l'agent étranger et l'agent de rattachement, et, à cet égard, qu'il n'est pas affecté par des espaces d'adresses disparates. Cette restriction s'applique aussi aux nœuds mobiles qui fonctionnent avec une adresse d'entretien colocalisée. Dans ce cas, l'inversion de tunnel est une solution complète et élégante.
- Il n'y a pas d'élément de protocole supplémentaire au delà de ceux définis par IP mobile [RFC2002] et l'inversion de tunnel. En particulier, des extensions supplémentaires aux demandes ou réponses d'enregistrement, ou des bits supplémentaires dans l'en-tête – bien que potentiellement utiles – sortent du domaine d'application de ce document.

En dépit de ces limitations, l'inversion de tunnel peut être utilisée pour résoudre les problèmes les plus courants. La gamme des problèmes qui peuvent être résolus est mieux comprise en examinant quelques diagrammes simples :

Figure A1 : Paquets non acheminables dans des espaces d'adresses disparates



Dans ce diagramme, il y a trois espaces d'adresses disparates : A, B et C. L'agent de rattachement (HA) a une adresse sur chaque espaces d'adresses B et C, et l'agent étranger (FA), sur les espaces d'adresses A et B. Le nœud mobile (MN) a une

adresse permanente, Mc, au sein de l'espace d'adresses C.

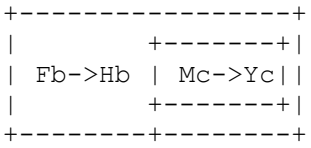
Dans le cas le plus courant, A et C sont tous deux des espaces d'adresses "privés", et B est l'Internet public.

Supposons que MN envoie un paquet au nœud correspondant (Y) dans son réseau de rattachement. Vraisemblablement, MN n'a pas de difficulté à livrer ce paquet au FA, parce que il le fait en utilisant les mécanismes de couche 2. D'une façon ou d'une autre, le FA doit réaliser que ce paquet doit être transmis en tunnel inverse, et il doit aller chercher le lien approprié pour ce faire. Les mécanismes possibles sont décrits au paragraphe A.3.

Cependant, une fois que le paquet est dans l'espace d'adresses B, il devient non acheminable. Noter que le filtrage d'entrée exacerbe le problème, parce qu'il ajoute une exigence de signification topologique à l'adresse IP de source en plus de celle de l'adresse de destination. Avec le mûrissement de IP mobile, d'autres entités pourront être définies (par exemple, des serveurs AAA). Leur ajout fait peser encore plus d'exigences sur les espaces d'adresses utilisés.

Le tunnelage inverse ajoute un en-tête IP à signification topologique au paquet (adresse IP de source de Fb, destination de Hb) durant son transit au sein de l'espace d'adresses B. En supposant une encapsulation IP dans IP (bien que d'autres, comme GRE soient aussi possibles) voila à quoi va ressembler le paquet :

Figure A2 : Paquet IP dans IP en tunnel inversé de Fa à HA



HA reçoit ce paquet, récupère le paquet d'origine, et comme il connaît l'espace d'adresses C, le livre à l'interface appropriée.

Bien sûr, pour que cela se produise, l'adresse d'entretien enregistrée par le MN n'est pas le Fa usuel, mais Fb. Comment cela se produit sort du domaine d'application de ce document. Des mécanismes possibles sont :

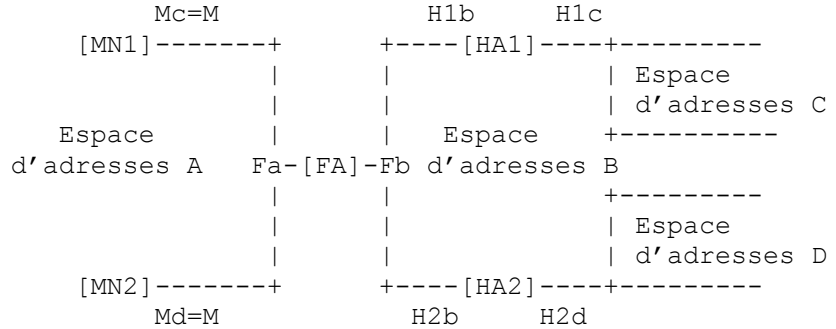
- FA reconnaît les nœuds mobiles dont les adresses rentrent dans les gammes d'adresses privées spécifiées par la RFC1918. Dans ce cas, l'agent étranger pourrait forcer l'utilisation de Fb comme adresse d'entretien, peut-être en rejetant la demande d'enregistrement initiale avec un message d'erreur approprié et des informations complémentaires.
- FA pourrait être configuré à toujours annoncer Fb tant que H->Fb et Fb->H sont garantis d'être respectivement des tunnels vers l'avant et inverse valides, pour toutes les valeurs de H. Ici, H est l'adresse de tout agent de rattachement dont les nœuds mobiles peuvent s'enregistrer via FA.
- FA pourrait indiquer qu'il prend en charge les espaces d'adresses disparates via un bit 'P' actuellement indéfini dans ses annonces, et une indication de l'espace d'adresses pertinent pour une ou toutes ses adresses d'entretien en incluant un Nature de l'indicateur d'adresse (NAI, *Nature of Address Indicator*) [RFC2486] ou un indicateur de domaine (peut-être comme variante du NAI). Autrement, les nœuds mobiles configurés ainsi pourraient solliciter le NAI ou des informations d'indicateur de domaine en réponse aux annonces avec le bit 'P' établi.

De plus, le nœud mobile a besoin de fournir l'adresse appropriée pour son agent de rattachement : Hb au lieu du Hc usuel. Comment cela se fait sort du domaine d'application de ce document. Des mécanismes possibles sont :

- cette détermination pourrait être déclanchée en réponse à l'utilisation du Fb de l'agent étranger comme adresse d'entretien ;
- le nœud mobile pourrait toujours utiliser Hb comme son adresse d'agent de rattachement, spécialement (1) si Hb est acheminable au sein de l'espace d'adresses C, ou (2) si MN est certain de ne jamais être à son réseau de rattachement (dans certaines configurations, les nœuds mobiles sont toujours en itinérance) ;
- le nœud mobile pourrait être configuré avec différentes adresses d'agent de rattachement et leurs espaces d'adresses correspondants (peut-être indiqués via un NAI [RFC2486] ou une de ses variantes).

Un autre question majeure introduite par les adresses privées est que deux nœuds mobiles ou plus, peuvent avoir la même adresse numérique IP :

Figure A3 : Nœuds mobiles avec un conflit d'adresses



Supposons qu'il y ait deux espaces d'adresses A et B, et un agent étranger (FA) avec des interfaces sur les deux. Il y a deux agents de rattachement (HA1 et HA2) dans l'espace d'adresses B, avec les adresses H1b et H2b, respectivement. Chacun des agents de rattachement a une interface dans un espace d'adresses privé en plus de l'espace d'adresses B : HA1 a H1c sur C, et HA2 a H2d sur D. MN1 et MN2 sont deux nœuds mobiles avec les adresses de rattachement Mc et Md, correspondant à l'espace d'adresses C et D, respectivement.

Si Mc et Md sont des adresses privées comme défini dans la RFC1918, elles peuvent être numériquement équivalentes (toutes deux égales à M). À cause de cela, l'agent étranger ne peut plus s'appuyer seulement sur l'adresse de rattachement des nœuds mobiles pour différencier ses différents liens.

A.2 Terminaison des tunnels vers l'avant chez l'agent étranger

Dans la figure A1, supposons que le nœud correspondant Y envoie un paquet au nœud mobile à l'adresse Mc. Le paquet est intercepté par l'agent de rattachement à Hc et tunnelé vers le nœud mobile via l'adresse Fb.

Une fois que le paquet atteint FA (via l'adresse Fb) l'agent étranger doit identifier lequel de ses nœuds mobiles enregistré est la destination ultime du paquet interne. Afin de le faire, il a besoin d'identifier le lien approprié via un tuplet dont l'unicité est garantie parmi tous ses nœuds mobiles.

Le tuplet unique suffisant pour démultiplexer les paquets IP dans IP [IPIP] (protocole 4) est :
- adresse IP de destination de l'en-tête encapsulé (interne)
  C'est l'adresse de rattachement du nœud mobile MN (Mc dans l'exemple ci-dessus). À première vue, elle semble unique parmi tous les nœuds mobiles, mais comme on l'a mentionné plus haut, avec les adresses privées, un autre mobile peut avoir une adresse Md numériquement équivalente à Mc.
- adresse IP de source de l'en-tête externe
  C'est l'extrémité distante du tunnel, Hb dans l'exemple ci-dessus.
- adresse IP de destination de l'en-tête externe
  C'est l'extrémité locale du tunnel, Fb dans l'exemple ci-dessus.

Les trois valeurs ci-dessus sont apprises d'un enregistrement réussi et ce sont l'adresse de rattachement du nœud mobile, l'adresse de l'agent de rattachement et l'adresse d'entretien. Donc, il est possible d'identifier le bon lien. Une fois que le FA a identifié la destination ultime du paquet, Mc, il livre le paquet interne en utilisant les mécanismes de couche de liaison.

Les paquets GRE [RFC2784] (protocole 47) ne sont traités que si leur champ Type de protocole a une valeur de 0x800 (les autres valeurs sortent du domaine d'application de ce document) et sont démultiplexés sur la base du même tuplet que les paquets IP dans IP. Dans la terminologie GRE, le tuplet est :
- adresse IP de destination du paquet de charge utile (interne)
- adresse IP de source du paquet de livraison (externe)
- adresse IP de destination du paquet de livraison (externe).

Noter que les champs Routing, Sequence Number, Strict Source Route et Key ont été déconseillés pour GRE [RFC2784]. Cependant, un document séparé spécifie leur utilisation [RFC2890].

Les tuplets ci-dessus fonctionnent pour l'encapsulation IP dans IP ou GRE, et supposent que le paquet interne est en clair. Les encapsulations qui chiffrent l'en-tête de paquet interne sortent du domaine d'application de ce document.

A.3 Initiation des tunnels inverses chez l'agent étranger

Dans la figure A3, on suppose que le nœud mobile M1 envoie un paquet au nœud correspondant dans son espace d'adresse de rattachement, C, et que le nœud mobile M2 envoie un paquet à un nœud correspondant dans son espace d'adresse de rattachement, D.

Au FA, les adresses de source pour les deux paquets vont être vues comme M, donc, cette information n'est pas suffisante. Le tuplet unique requis pour identifier le bon lien est :
- informations de couche liaison relatives au MN
  Elles peuvent être sous la forme d'une adresse MAC, d'une session PPP (ou une interface d'entrée) ou un codage de canal pour un service cellulaire numérique. Des identifiants d'appareil peuvent aussi être utilisés dans ce contexte.
- adresse IP de source de l'en-tête IP.
  Comme on l'a souligné, il n'est pas garanti qu'elle soit par elle-même unique.

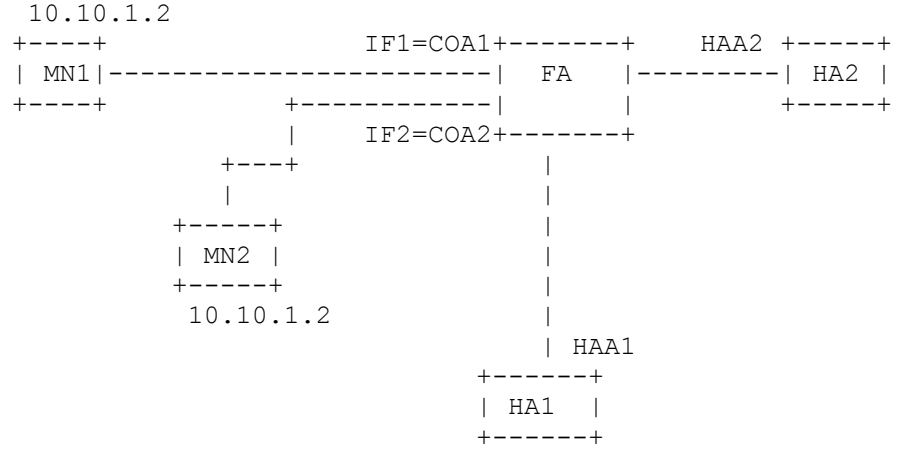
Ces informations doivent être établies et mémorisées au moment de l'enregistrement. Les éléments ci-dessus sont suffisants pour que l'agent étranger choisisse le bon lien à utiliser. Ceci produit à son tour l'adresse de l'agent de rattachement, et les options de tunnel inverse négociées durant le processus d'enregistrement. L'agent étranger peut maintenant procéder au tunnel inverse.

A.4 Scénario d'adresse privée limitée

Le scénario de l'adresse privée limitée (LPAS, *Limited Private Address Scenario*) a beaucoup retenu l'attention de l'industrie du cellulaire sans fil, de sorte qu'il est utile de le définir et de préciser ses exigences.

LPAS est un sous ensemble du scénario de l'espace d'adresses disparate exposé dans cet appendice. Ce paragraphe explique comment LPAS pourrait être déployé étant donné l'état actuel des spécifications IP mobile.

Figure A4 : Exemple de scénario d'adresse privée



La figure ci-dessus présente un scénario très simple dans lequel des adresses privées sont utilisées. Ici, les "adresses privées" sont strictement celles définies dans la [RFC1918]. Dans ce scénario de déploiement, les seules entités qui ont des adresses privées sont les nœuds mobiles. Les adresses d'agent étranger et d'agent de rattachement sont acheminables publiquement sur l'Internet général. Plus précisément, les adresses d'entretien annoncées par les agents étrangers (COA1 et COA2 à la Figure A4) et les adresses d'agent de rattachement utilisées par les nœuds mobiles dans les demandes d'enregistrement (HAA1 et HAA2 dans la Figure A4) sont acheminables publiquement sur l'Internet général. Par conséquent, tout tunnel IP mobile peut être établi entre toute adresse de rattachement d'agent de rattachement et toute adresse d'entretien d'agent étranger.

On notera aussi que deux nœuds mobiles différents (MN1 et MN2) avec la même adresse privée (10.10.1.2) visitent le même agent étranger FA. Ceci est accepté tant que MN1 et MN2 sont desservis par des agents de rattachement différents. Donc, du point de vue d'un agent de rattachement, chaque nœud mobile a une adresse IP unique, même si elle se trouve être une adresse privée selon la [RFC1918].

Le fonctionnement en présence d'optimisation de chemin [RFC3775] sort du domaine d'application de ce document.

Exigences pour le scénario d'adresse privée ci-dessus :

Exigences du nœud mobile :
Les nœuds mobiles qui ont l'intention d'utiliser des adresses privées avec IP mobile DOIVENT établir le bit 'T' et employer l'inversion de tunnel. Les adresses privées de nœud mobile au sein d'un certain espace d'adresses DOIVENT être uniques. Donc, deux nœuds mobiles appartenant à un seul agent de rattachement ne peuvent pas avoir la même adresse privée. Donc, lors de la réception ou de l'envoi de trafic tunnelé pour un nœud mobile, les points d'extrémité de tunnel sont utilisés pour faire la distinction entre des adresses de nœud mobile en conflit. Si le nœud mobile se trouve s'enregistrer simultanément auprès de plusieurs agents de rattachement à travers le même agent étranger, il doit y avoir des informations de couche de liaison qui sont distinctes pour chaque nœud mobile. Si de telles informations distinctes de couche de liaison ne sont pas disponibles, les nœuds mobiles DOIVENT utiliser des adresses uniques.

Exigences pour l'agent étranger :
Toutes les interfaces d'annonces de l'agent étranger DOIVENT avoir une adresse d'entretien publiquement acheminable. Donc, un nœud mobile avec une adresse privée ne visite l'agent étranger que dans son réseau publiquement acheminable. Les agents étrangers DOIVENT prendre en charge l'inversion de tunnel afin de prendre en charge les nœuds mobiles à adresse

privée. Si un agent étranger reçoit une demande d'enregistrement d'un nœud mobile à adresse privée, et si le nœud mobile n'a pas établi le bit 'T', l'agent étranger DEVRAIT la rejeter.
Lors de la livraison à, ou réception de paquets de nœuds mobiles, les agents étrangers DOIVENT différencier entre nœuds mobiles avec adresses privées conflictuelles en utilisant des informations de couche de liaison comme mentionné précédemment (paragraphes A.2 et A.3). Un agent étranger en l'absence d'optimisation de chemin, devrait s'assurer que deux nœuds mobiles qui visitent le même agent étranger correspondent l'un avec l'autre à travers de leurs agents de rattachement respectifs. Si un agent étranger prend en charge l'inversion de tunnel, il DOIT alors prendre en charge le scénario simple de prise en charge d'adresse privée décrit ici.

Exigences de l'agent de rattachement :
Toute adresse d'agent de rattachement utilisée par des nœuds mobiles dans des demandes d'enregistrement DOIT être une adresse à acheminement public. Les agents de rattachement n'accepteront pas de chevauchement d'adresses de rattachement privées, donc chaque adresse de rattachement privée d'un nœud mobile enregistré auprès d'un agent de rattachement est unique. Lorsque le bit 'T' est établi dans la demande d'enregistrement provenant du nœud mobile, l'agent de rattachement DOIT reconnaître et accepter la demande d'enregistrement des nœuds mobiles qui ont des adresses privées. Aussi, l'agent de rattachement DEVRAIT être capable d'allouer des adresses privées hors de son réservoir d'adresses aux nœuds mobiles pour les utiliser comme adresses de rattachement. Ceci ne contredit pas le traitement d'agent de rattachement du paragraphe 3.8 de la [RFC2002].

Appendice B Changements par rapport à la RFC2344

Cette section fait la liste des changements par rapport à la précédente version de ce document (RFC2344).

- Ajout de l'Appendice A sur la prise en charge des espaces d'adresses disparates et des adresses privées.

- Ajout du paragraphe correspondant (6.3) sous les 'Considérations sur la sécurité'.

- La prise en charge de la livraison encapsulante a été rendue facultative par la transformation de DOIT en DEVRAIT. Cela exige aussi la définition d'un nouveau code d'erreur 79 (alloué par l'IANA).

- Mention de la possibilité d'une extension d'authentification admissible qui peut être différente de l'extension d'authentification Mobile-rattachement.

- Une section considérations relatives à l'IANA a été ajoutée.

Déclaration complète de droits de reproduction

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