http://livre.g6.asso.fr/index.php/Mobilit%C3%A9_dans_IPv6

Mobilité dans IPv6

Comparaison entre VPN IPsec et VPN SSL | Table des matières | La gestion de la mobilité IPv6

Ce chapitre a pour objectif de décrire comment la mobilité a tiré partie d'IPv6 pour améliorer les mécanismes définis dans IPv4. Il introduit la vision IETF de la mobilité et les différents éléments du réseau qui en découlent. Sur la base de scénario, il décrit les flux de signalisation et de données, échangés lors des épisodes de mobilité. Afin de ne pas trop alourdir la présentation, tout en donnant une idée précise du protocole, seuls quelques formats de paquets sont donnés en exemple. Les mécanismes de sécurité mis en oeuvre dans l'optimisation de la signalisation sont également décrits. Le chapitre aborde ensuite des sujets encore à l'étude comme certaines améliorations de performances et la mobilité des réseaux eux-même. Il s'achève sur la présentation d'une implémentation expérimentale de la mobilité.

Introduction

Depuis quelques années déjà les terminaux informatiques deviennent moins encombrants et par conséquent plus mobiles. Par ailleurs les possibilités de se connecter à l'Internet se multiplient. Il s'en suit une mobilité induite par l'utilisation de plusieurs technologies d'accès (Ethernet, Wi-Fi, GPRS,...) sur un même terminal dans la même journée. Les études actuellement conduites par les constructeurs et les opérateurs pour fournir des infrastructures mobiles utilisant de nouvelles technologies radio, Wi-Fi et WiMax notamment, ont pour objet d'offrir la continuité des services en cours de déplacement, comme le permet le GSM dans le cas de la téléphonie mobile. Cela nécessite que les applications ne soient pas interrompues lors des épisodes de mobilité.

Enfin, les sociétés de transport désirant offrir un service de connexion à leurs clients en déplacement et les fabricants de véhicules, qui interconnectent de plus en plus d'équipements à bord, envisagent la question de la mobilité d'un réseau entier et non plus uniquement celle d'équipements isolés.

Le problème de la mobilité dans IP peut se décomposer en trois sous-problèmes distincts :

- pouvoir communiquer ;
- être joignable ;
- conserver les communications en cours lors des déplacements.

Le premier problème est élégamment résolu par le mécanisme d'auto configuration d'IPv6, en effet, dès que le terminal a réussi à construire une adresse IPv6 globale, il est capable de communiquer avec toute autre station sur l'Internet. Mobile IPv6 (MIPv6) modifie très peu ces mécanismes. Il ne requiert que de nouvelles directives de configuration permettant d'accélérer le processus. Le délai d'acquisition d'une adresse globale routable est en effet critique dans les situations de mobilité.

Le second problème est résolu pour les postes IP fixes par le DNS qui établit la relation entre un nom logique connu de tous et une adresse IP (Nommage). Dans le contexte de la mobilité, la fréquence d'attribution d'une nouvelle adresse est incompatible avec la mise à jour du DNS distribué. D'autres mécanismes ont été proposés.

Le troisième problème est plus difficile à résoudre. Il a pour origine la dualité des fonctions d'une adresse IPv6. Elle identifie de manière unique sur l'Internet un terminal, ou pour être plus précis une interface réseau d'un terminal. Elle permet aussi de localiser un noeud dans la topologie de l'Internet. Ainsi chaque fois qu'un noeud se déplace, ce dernier doit changer d'adresse pour que la nouvelle adresse corresponde à sa nouvelle localisation (fonction de localisation). Malheureusement son identification change aussi ce qui pose des problèmes aux couches supérieures. En effet, TCP utilise le quintuplé : Adresse IPv6 source, Adresse IPv6 destination, Port source, Port destination et numéro de protocole pour identifier une connexion. Lorsqu'un de ces éléments change, il ne s'agit plus pour lui de la même session et les communications en cours sont interrompues.

Dès 1998, l'IETF a standardisé une solution de mobilité IP pour IPv4 [RFC 3344]. Les contraintes liées à la modification d'un protocole très largement déployé ont limité le travail à la modification du comportement du mobile lui-même (sans implication du correspondant pour qui la mobilité devait être transparente) et à l'ajout de nouvelles entités dans le réseau. IPv6 offrait l'opportunité du déploiement d'un nouveau protocole intégrant dès l'origine la mobilité. Les correspondants peuvent ainsi être mis à contribution pour des traitements liés à la mobilité. De plus la conception plus moderne d'IPv6 permet d'alléger les mécanismes d'encapsulation et de profiter des mécanismes d'auto configuration.

Des désaccords concernant la sécurisation de Mobile IPv6 (c.f. Les risques induits par la mobilité et leur limitation) et les différentes optimisations possibles, ont rendu la standardisation de Mobile IPv6 longue et laborieuse, les RFCs n'ayant été publiés qu'en juin 2004. La gestion de la mobilité dans IPv6 est maintenant définie dans le RFC 3775 pour ses aspects fonctionnels. Le RFC 3776 traite pour sa part des aspects liés à la sécurité de la signalisation de la mobilité.

Si les travaux dans le domaine de la mobilité IP se sont dans un premier temps exclusivement consacrés au support des stations mobiles, le besoin de fournir un accès Internet permanent aux routeurs mobiles et aux stations situées dans un réseau en mouvement (réseau mobile) est aujourd'hui clairement identifié. Les problèmes spécifiques posés par ce type de mobilité sont traités à l'IETF au sein du groupe de travail NEMO (NEtwork MObility) récemment créé. Ces travaux ont abouti à l'édition du RFC 3963 qui spécifie des fonctionnalités semblables à celles de MIPv6 dédiées aux routeurs mobiles.

La gestion de la mobilité IPv6

Mobilité dans IPv6 Table des matières Déplacements des mobiles

Contents

Le choix de l'IETF

Plusieurs alternatives sont possibles pour résoudre les problèmes introduits par la mobilité. La première d'entre-elles consiste à changer le fonctionnement même d'IP en modifiant les principes de l'adressage. Des propositions existent pour définir deux espaces d'adressage. Le premier serait dédié à la localisation et le second à l'identification. Mais il s'agit là d'un travail de très longue haleine. La seconde d'entre-elles consiste à ne rien changer au niveau d'IP et à laisser les couches supérieures gérer le problème. Il serait par exemple possible de modifier TCP pour gérer la mobilité (c'est-à-dire le changement d'adresse) au niveau transport. Malheureusement cela ne peut se faire qu'en modifiant la pile TCP ce qui est impensable étant donné le nombre de stations concernées. Par contre des propositions existent pour SCTP qui est un nouveau protocole de transport et n'est donc pas encore déployé à grande échelle. Le niveau applicatif peut aussi prendre en charge la mobilité en gérant la rupture et le ré-établissement automatique des connexions interrompues lors des handovers (épisodes de mobilité).

Toutes ces solutions supposent d'importants travaux de développement et sont difficiles à mettre en oeuvre. Dans la mesure ou le développement d'IPv6 ne s'accompagne pas nécessairement de la modification en profondeur des niveaux protocolaires supérieurs, l'IETF a eu la volonté de gérer la mobilité au niveau de la pile IP et de la rendre transparente aux niveaux supérieurs utilisant le service IP.

Le groupe de travail Mobile IP s'est donc appuyé sur une solution basée sur deux adresses IP et sur le routage « normal » des paquets pour assurer la gestion de la mobilité des noeuds. Des améliorations apportées par la version 6 d'IP et des éléments spécifiques à MIPv6 ont été utilisés pour assurer au mieux la transparence des déplacements. MIPv6 utilise ou définit l'emploi des éléments suivants :

- les en-têtes d'extension protocolaire (protocole 135) ;
- les en-têtes de routage (nouveau type 2) ;
- les en-têtes destination ;
- les mécanismes d'annonce des routeurs (ICMPv6) ;
- la gestion de l'obsolescence des adresses ;
- la sécurisation des paquets (IPsec).

Vue générale de la gestion de la mobilité IPv6

Les mécanismes d'IPv6 vus dans les chapitres précédents offrent une très bonne base à la gestion de la mobilité. En effet, ils résolvent un certain nombre de problèmes qu'avaient à résoudre les solutions de mobilité IPv4. Ainsi, le mécanisme de configuration sans état permet au terminal mobile (MN : *Mobile Node*) en déplacement d'acquérir une adresse IPv6 globale topologiquement valide. Il peut dès lors communiquer sans contrainte. Le mécanisme d'annonce des routeurs facilite quant à lui la détection du mouvement qui est essentielle à la gestion de la mobilité.

Le principe à la base de la mobilité IPv6 est de séparer les fonctions d'identification et de localisation toutes deux traditionnellement assurées par l'adresse IP. Il s'en suit que lorsque le mobile se déplace, il doit changer d'adresse IP puisque celle-ci le localise dans le réseau. De ce fait, il perd son identité et n'est plus directement joignable à l'adresse connue de ses correspondants et du service de nom. Il est toujours possible d'enregistrer la nouvelle adresse dans un service de nom dynamique (DDNS) mais cela induit un délai très important et ne résout qu'une partie du problème. En effet, l'adresse IP est aussi utilisée par les couches transport (UDP et TCP) pour identifier une connexion. Lorsque l'adresse IP du mobile change, les connexions TCP en cours sont donc rompues.

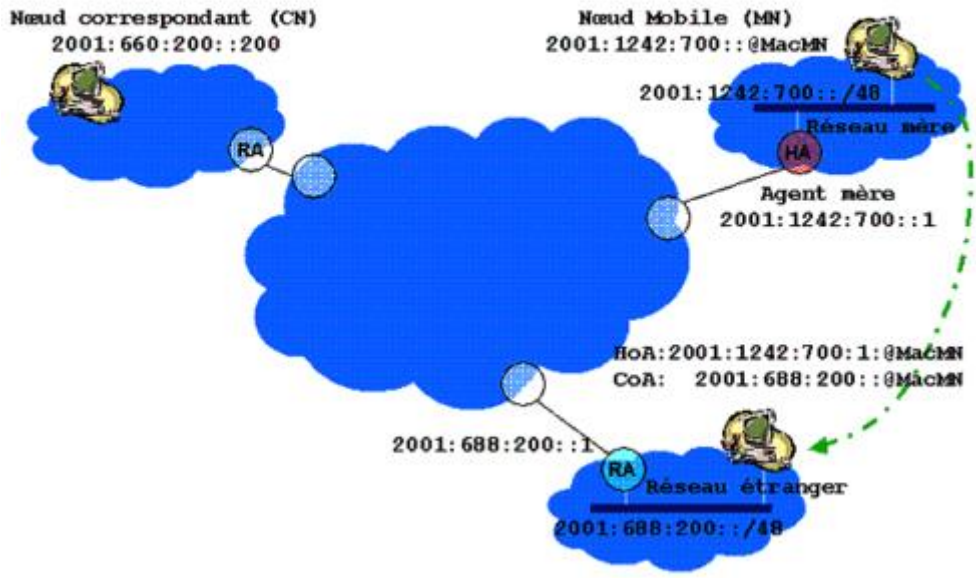

Figure 13-1 *Différentes adresses utilisées dans la mobilité IPv6*

Pour éviter cela, mobile IP permet au mobile de conserver l'adresse utilisée dans son réseau d'attachement. A des fins d'identification, on parle de home address (HoA) ou adresse mère et de home network ou réseau mère. Ainsi, du point de vue des couches supérieures, le mobile conserve son adresse mère (HoA) quelle que soit sa localisation. Par ailleurs, il acquiert une adresse nouvelle temporaire appelée care-of address (CoA) ou adresse temporaire, locale celle-ci, dans chacun des réseaux qu'il visite, dits réseaux étrangers. Ce second type d'adresses est utilisé à des fins de localisation. Du point de vue de la pile IPv6 le noeud mobile

communique toujours avec l'adresse temporaire sauf lorsqu'il est attaché à son réseau mère. Du point de vue des couches protocolaires supérieures le mobile communique toujours avec son adresse mère (cf. figure Différentes adresses utilisées dans la mobilité IPv6).

Une nouvelle entité, le home agent (HA) ou agent mère, localisé dans le réseau mère est chargé d'assurer la correspondance entre la HoA et la CoA du mobile lorsque celui-ci est attaché à un réseau étranger. Cet agent est également chargé de ré-acheminer les paquets IP à destination de l'adresse mère du mobile vers son adresse temporaire dans son réseau visité.

Le mobile dans son réseau mère.

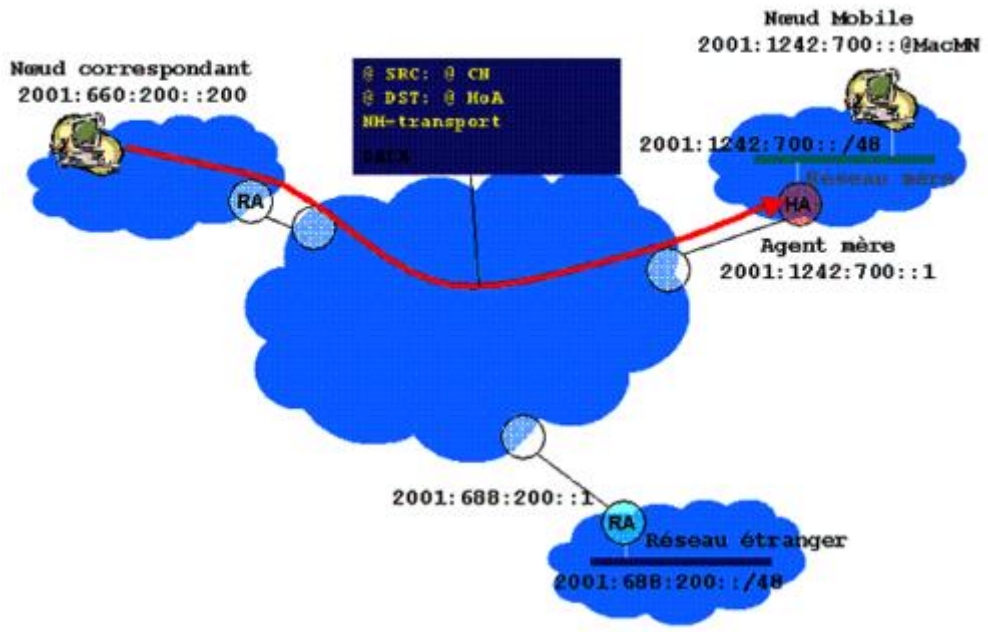

Figure 13-2 *Envoi de paquets à un mobile situé dans son réseau mère*

Lorsque le mobile est attaché au réseau mère (cf. figure Envoi de paquets à un mobile situé dans son réseau mère), il dispose de son adresse mère et communique normalement en utilisant sa HoA comme adresse source. Les paquets qui lui sont destinés comprennent l'adresse mère comme adresse destination et sont routés en fonction du préfixe du réseau mère. L'agent mère est inactif. Il n'y a pas de problème de sécurité supplémentaire induit par la gestion de la mobilité puisque le mobile communique de la même manière que n'importe quel noeud IPv6 sur l'Internet.

Le réseau mère n'est pas nécessairement un réseau sur lequel le mobile peut s'attacher, son rôle principal étant d'accueillir le home agent et les adresses mères des mobiles qu'il gère. Il y a toutefois une relation administrative forte entre le mobile et son réseau mère.

Le mobile dans un réseau étranger

Lorsque le mobile est attaché à un réseau étranger, il dispose, en plus de son adresse mère, d'une ou plusieurs adresses temporaires routables acquises par les mécanismes d'auto-configuration avec ou sans états. Une de ces adresses est choisie comme adresse temporaire

primaire et est transmise à l'agent mère pour créer une association entre la HoA et cette CoA primaire.

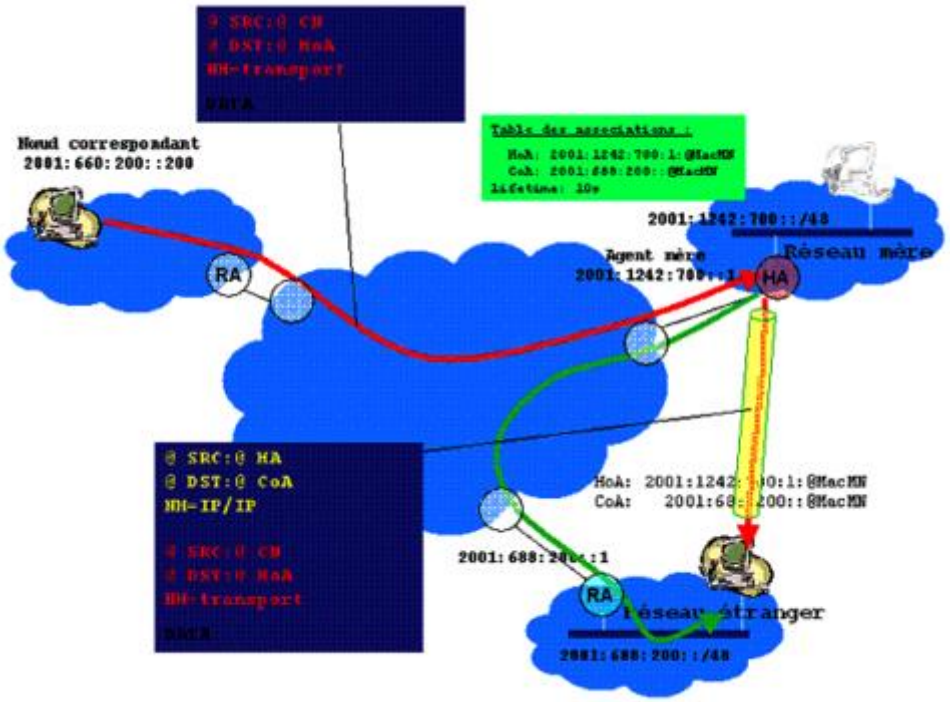

Figure 13-3 *Envoi de paquets à un mobile situé hors de son réseau mère - tunnelage*

L'agent mère maintient une "table des associations" contenant les associations de tous les mobiles qu'il gère et qui sont en visite dans un réseau étranger (cf. figure Envoi de paquets à un mobile situé hors de son réseau mère - tunnelage). Grâce à ces informations, il peut faire suivre les paquets à destination de la HoA d'un des mobiles vers la CoA primaire de ce dernier. Il encapsule pour cela les paquets en utilisant l'extension d'en-tête IP-IP d'IPv6. Les paquets ainsi tunnelés sont protégés par IPsec.

Le paquet IP retransmis vers le mobile comporte comme adresse source celle du HA et comme adresse destination la CoA primaire du mobile. Le paquet atteint le réseau étranger puisque la CoA primaire a pour préfixe un de ceux du réseau étranger. Le mobile réceptionne ce paquet et découvre l'extension d'en-tête IP dans IP. Il supprime l'en-tête extérieur et remet le paquet aux couches supérieures comme si le mobile avait réceptionné le paquet dans son réseau mère. Ce paquet à donc pour adresse destination l'adresse mère du mobile et pour adresse source l'adresse IPv6 du correspondant émetteur du message. Le quintuplé TCP d'identification d'une session n'est pas modifié. La communication n'est plus rompue lors d'un épisode de mobilité sans qu'il ait été nécessaire de modifier le protocole TCP.

Les paquets issus du mobile dans un réseau étranger et à destination du correspondant utilisent un principe similaire. Cependant dans le cas présent les paquets sont reverse tunnelés via le HA. le paquet IP ainsi transmis comporte comme adresse source la CoA primaire du mobile et comme adresse destination l'adresse du HA. le paquet IP encapsulé comporte comme adresse source la Home Address et comme adresse destination celle du correspondant. Les paquets ainsi transmis sont protégés par IPSEC, traversent les routeurs jusqu'au HA qui supprime l'en-tête extérieur et forwarde le paquet résultant au correspondant.

De cette manière le correspondant voit la communication comme venant directement du réseau mère du mobile. Pour effectuer ce traitement, le correspondant ne maintient aucun état spécifique aux mobiles avec qui il communique. Ainsi un mobile peut communiquer avec des correspondants ayant un support minimum de la mobilité. Ce support minimum de la mobilité ne monopolise aucune ressource particulière au niveau du correspondant, et n'induit pas de nouveaux problèmes de sécurité ou de performances.

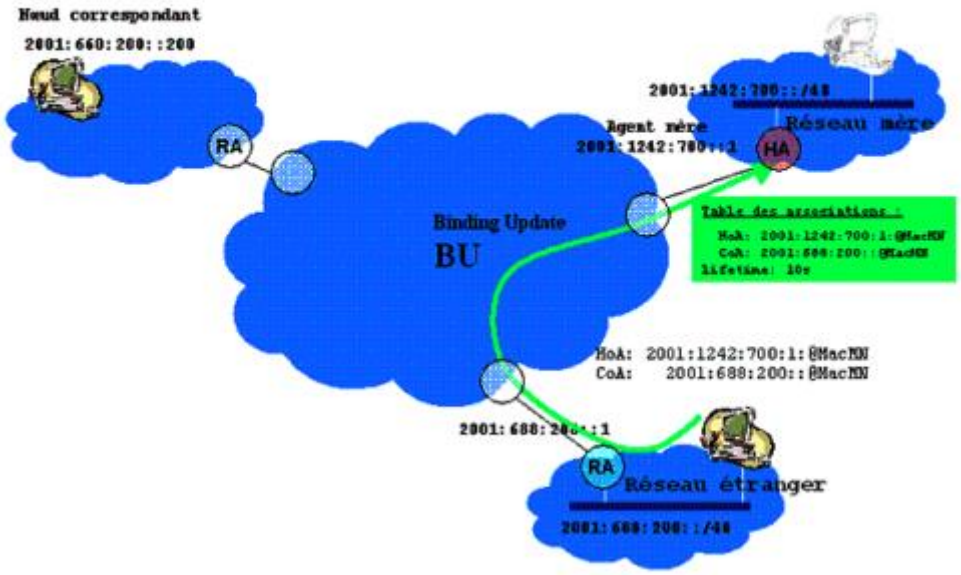

Figure 13-4 *Mise à jour d'association entre le mobile et l'agent mère*

Pour créer une association, ou la mettre à jour lorsqu'il change de réseau étranger, un mobile utilise une signalisation propre à la mobilité IPv6 appelée Binding Update (BU) ou mise à jour d'association. Cette signalisation utilise un nouveau protocole (135) basé sur les extensions d'en-tête IPv6 (cf. figure Mise à jour d'association entre le mobile et l'agent mère).

Toutefois, même avec ce mécanisme très simple, les applications, ou les utilisateurs, n'ont pas conscience de la mobilité et par conséquent du fait que le terminal n'est pas dans son réseau mère. Si bien, qu'elles peuvent faire confiance à un environnement réseau connu entre le correspondant et le noeud mobile, par exemple entre deux bâtiments d'un même campus. Le fait de se trouver dans un réseau visité à l'insu des applications peut donc causer des problèmes de sécurité puisque les paquets vont circuler sur une portion de réseau inconnu et potentiellement non sûr. Pour éviter cela, il est possible d'utiliser le tunnel sécurisé entre le mobile et le "home agent" dans les deux sens. La sécurité est ainsi assurée sans que le correspondant local n'ait à supporter la mobilité.

Optimisation dans le cas du mobile dans un réseau étranger

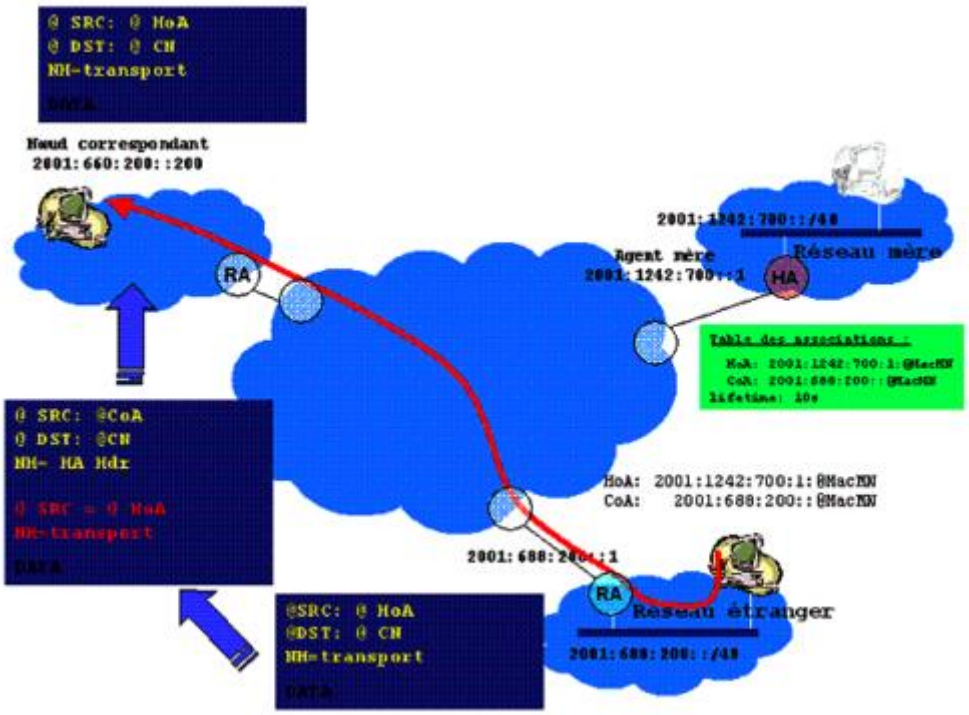

Figure 13-5 *Envoi de paquets par un mobile situé hors de son réseau mère*

Le routage systématique par l'agent mère du mobile est simple à mettre en oeuvre et très sûr puisque la communication entre l'agent mère et le mobile est sécurisée par IPsec (cf. figure Envoi de paquets à un mobile situé dans son réseau mère - tunnelage inverse). Par contre, elle est particulièrement inefficace au niveau du routage. En effet, si le mobile est en déplacement loin de son réseau mère et qu'il communique avec un serveur proche de lui, il est plus efficace de communiquer directement que de passer par l'agent mère (cf. figure Envoi de paquets par un mobile situé hors de son réseau mère). Cela permet d'économiser des ressources dans l'Internet et au niveau du réseau mère qui pourrait avoir des difficultés à monter en charge si les communications de tous les mobiles passent par lui. C'est pourquoi, l'optimisation de routage, qui était une option de mobile IPv4, a été intégrée à Mobile IPv6.

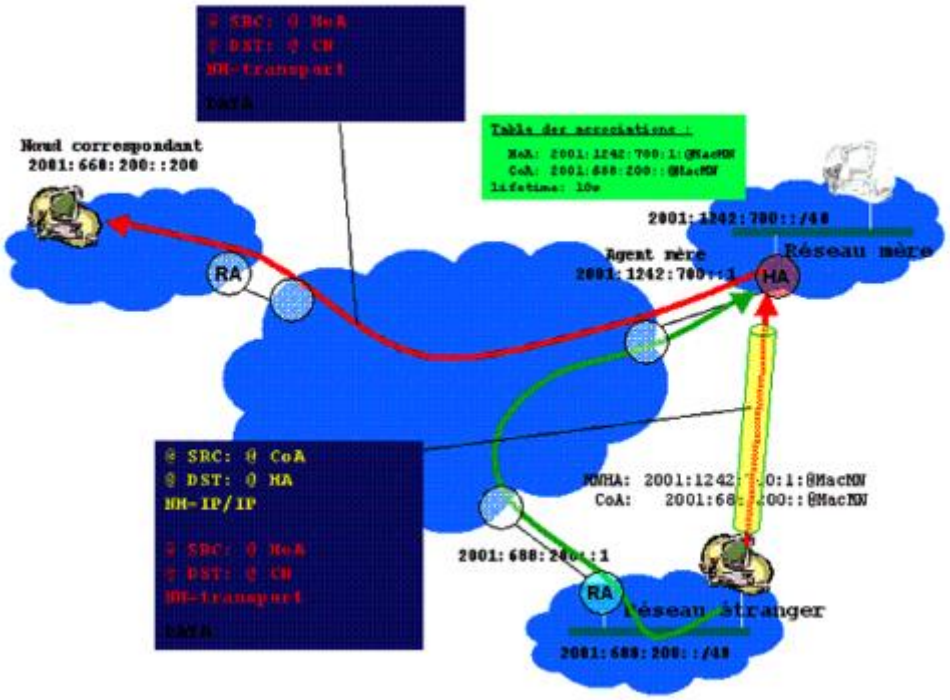

Figure 13-6 *Envoi de paquets à un mobile situé dans son réseau mère - tunnelage inverse*

L'optimisation de routage de Mobile IPv6 profite du fait que IPv6 est un nouveau protocole et que des mécanismes liés à la mobilité peuvent lui être intégrés lors de son déploiement. Ainsi pour supporter l'optimisation de routage les noeuds correspondants doivent intégrer des fonctions spécifiques liées à la mobilité.

Lorsqu'un correspondant supporte l'optimisation de routage, il maintient comme l'agent mère une table des associations pour tous les mobiles utilisant l'optimisation de routage avec lesquels il est en communication. Le mobile met à jour l'association qui le concerne en envoyant un message de mise à jour d'association (BU : Binding Update) au correspondant sitôt après qu'il a informé l'agent mère de sa nouvelle localisation. Il doit pour cela maintenir une table des mises à jour d'associations contenant toutes les associations qu'il doit entretenir auprès des correspondants et de l'agent mère. Cet entretien se fait à chaque déplacement et lorsqu'une mise à jour d'association arrive à échéance en échangeant des message de type BU (cf. figure Mise à jour d'association entre le mobile et le correspondant - route optimisée).

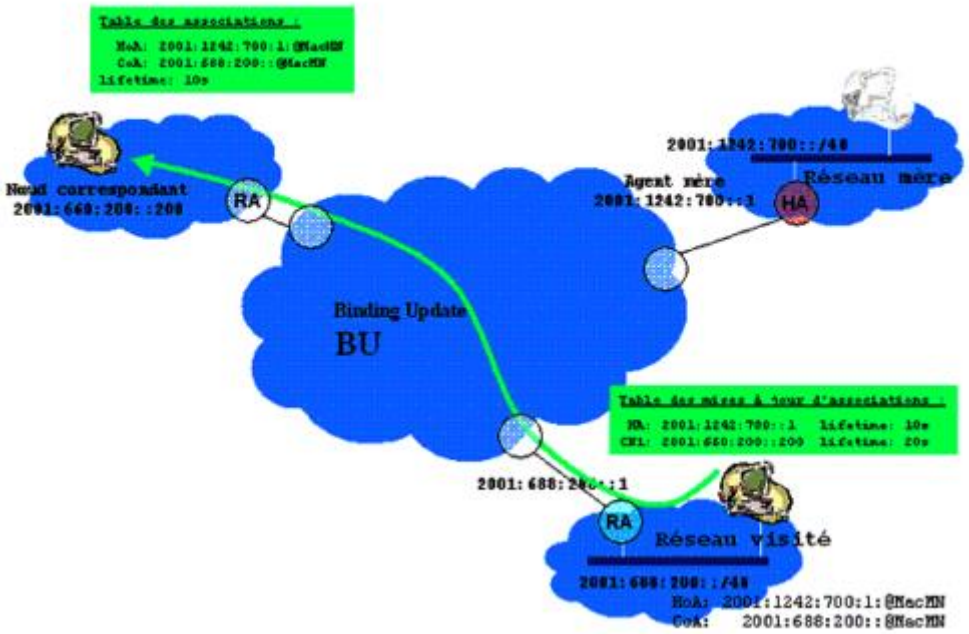

Figure 13-7 *Mise à jour d'association entre le mobile et le correspondant - route optimisée*

Le correspondant qui émet un paquet à destination d'un mobile et qui utilise l'optimisation de routage, trouve dans sa table des associations une association entre la HoA et une CoA. Il remplace alors l'adresse de destination par la CoA et ajoute une extension d'en-tête de routage particulière (de type 2) contenant la HoA du mobile comme adresse de destination finale (cf. figure Envoi de paquets à un mobile situé hors de son réseau mère - route optimisée).

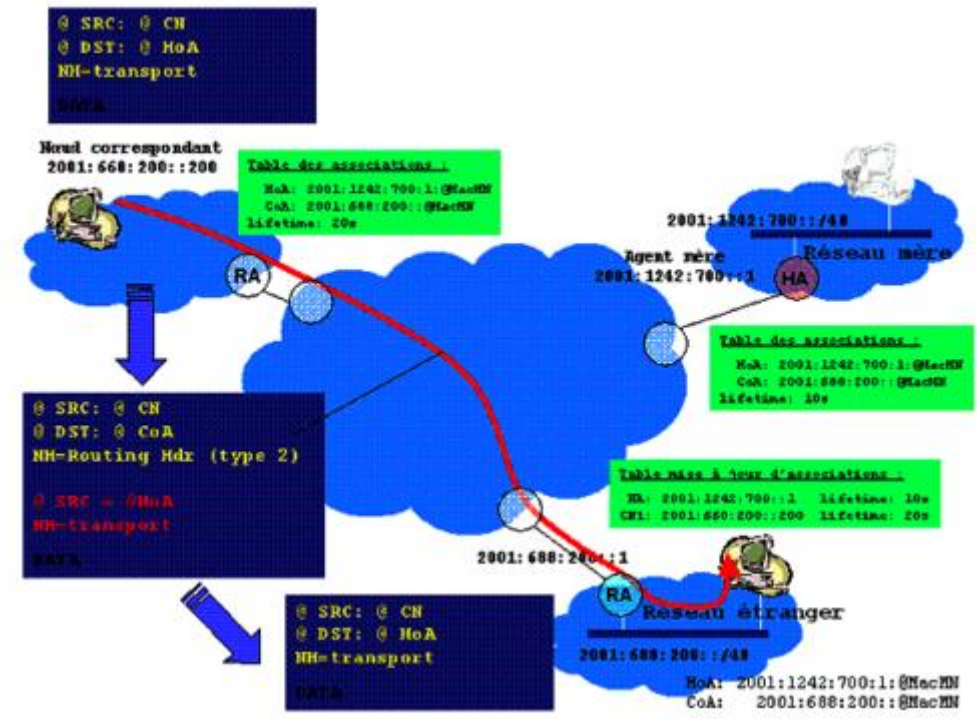

Figure 13-8 *Mise à jour d'association entre le mobile et le correspondant - route optimisée*

Les extensions d'en-tête de routage peuvent être filtrées pour des raisons de sécurité et pour qu'elles ne soient pas utilisées pour contourner les politiques de sécurité. Le type de l'extension d'en-tête de routage utilisé par Mobile IPv6 est différent pour permettre aux passerelles de sécurité d'appliquer des règles spécifiques aux paquets contenant un en-tête de routage liés à la gestion de la mobilité.

Tous les correspondants IPv6 potentiels ne supportent pas forcément l'optimisation de routage. Dans ce cas, un correspondant répond qu'il ne comprend pas la mise à jour d'association et les communications continuent à passer à travers l'agent mère. Pour, ce faire il utilise un message ICMPv6 spécifique qui informe le noeud mobile.

Lorsque le mobile veut envoyer un paquet à un correspondant, il vérifie au préalable si une optimisation de route a été initialisée. Dans ce cas précis uniquement, il émet les paquets à destination du correspondant en utilisant sa CoA et en ajoutant une extension d'en-tête spéciale appelée HoA. Cette extension d'en-tête est ajoutée de façon transparente aux couches supérieures pour qui la communication est toujours entre le correspondant et la HoA du mobile. Elle comprend la HoA du mobile, la CoA du mobile étant utilisée normalement pour émettre le paquet. Ainsi l'adresse source du paquet dispose d'un préfixe valide dans le réseau étranger et les paquets ne seront pas filtrés par le routeur de sortie. Lorsqu'il reçoit ce paquet, le correspondant supprime l'extension d'en-tête "home address" et remplace l'adresse source du paquet par la HoA trouvée dans l'extension. Il remet ensuite le paquet aux couches supérieures qui le considèrent comme venant directement du réseau mère du mobile.

Le mécanisme de mise à jour d'association pose d'importants problèmes de sécurité. En effet, il est aisé de protégé les échanges de signalisation entre le mobile et l'agent mère du fait de la relation administrative qui permet par exemple l'utilisation d'un secret partagé. C'est beaucoup plus compliqué en ce qui concerne les correspondants et pourtant la sécurité des mises à jour d'association est vitale. Sans protection, il serait possible de détourner les communications d'un mobile en redirigeant le trafic pour l'espionner ou de mener une attaque par déni de service. C'est pourquoi une procédure appelée "test de routage retour" est spécifiée (voir Sécurisation de la signalisation avec les noeuds correspondants).

Traitement du multicast

Pour la gestion du multicast, il faut considérer séparement les différents types de groupes multicast auxquels un noeud mobile adhère : il y a d'une part les groupes multicast auxquels toute station IPv6 adhère (par exemple le groupe multicast de sollicitation) et ceux auxquels une station adhère pour des besoins applicatifs spécifiques. Enfin il faut considérer la portée des groupes multicast qui peut être globale, locale ou correspondre à un site donné.

Pour ce qui est de la portée, le problème est relativement simple, les paquets multicast de portée locale ne doivent pas être retransmis à un noeud mobile qui se trouve dans un réseau visité et d'une manière générale, ceux qui n'ont pas une portée globale ne devraient pas l'être.

Lorsqu'un noeud mobile se trouve dans son réseau d'origine (réseau mère) il se comporte comme toute station IPv6 et traite normalement les paquets multicast. Par contre lorsqu'il se trouve dans un réseau étranger, il y a deux manières de gérer les flux multicast :

- soit l'agent mère retransmet vers le mobile les paquets à destination des groupes auxquels ce dernier a adhéré,
- soit le mobile ré-adhère aux groupes multicasts qui l'intéressent à chaque fois qu'il se déplace.

La première méthode suppose que l'agent mère dispose de la plupart des fonctions d'un routeur multicast. Il doit pouvoir comprendre et initier les échanges concernant l'appartenance du noeud mobile aux différents groupes et lui retransmettre les paquets à travers le mécanisme de tunneling.

Dans le second cas, l'agent mère n'assure pas le relayage des paquets multicast et le mobile qui souhaite écouter un groupe après un changement de réseau IPv6 doit se réabonner au groupe en question. Cette solution suppose que l'application prenne en compte la mobilité pour relancer la procédure d'adhésion avec la nouvelle CoA. Ceci constitue un des problèmes que MIPv6 souhaite éviter. Une autre difficulté vient de ce que l'interruption dans la réception d'un flux multicast entre le changement de réseau et la réception du premier paquet multicast à la nouvelle localisation peut être très longue du fait de la procédure d'adhésion.

Lorsque l'agent mère assure la gestion du multicast, le noeud mobile peut choisir pour chaque groupe multicast auquel il adhère, s'il passe par l'agent mère ou par une adhésion directe. Dans ce cas l'agent mère doit supporter le protocole de gestion des groupes multicast (i.e. MLD). De son côté, le mobile qui veut pouvoir profiter de cette fonctionnalité, doit implémenter la partie du protocole de gestion des groupes qui concerne l'hôte et être capable de traiter les paquets multicast encapsulés par l'agent mère.

Lorsque le mobile souhaite recevoir les paquets multicast destiné à un groupe particulier, il émet un paquet MLD d'adhésion au groupe avec pour destination l'adresse multicast des routeurs MLD et pour portée la valeur 1. Ce paquet est transmis à l'agent mère par l'intermédiaire du tunnel inverse entre le mobile et l'agent mère. De la même manière lorsqu'il ne souhaite plus recevoir les paquets de ce groupe, il informe l'agent mère qu'il quitte le groupe par le même moyen. De son côté, l'agent mère agit comme un routeur multicast standard et interroge régulièrement les mobiles en visite sur leur appartenance à des groupes multicast, en utilisant des messages MLD transmis dans les tunnels vers les mobiles.

Ce paquet est transmis à l'agent mère par l'intermédiaire du tunnel inverse entre le mobile et l'agent mère. De la même manière lorsqu'il ne souhaite plus recevoir les paquets de ce groupe, il informe l'agent mère qu'il quitte le groupe par le même moyen. De son côté, l'agent mère agit comme un routeur multicast standard et interroge régulièrement les mobiles qui sont dans des réseaux visités sur leur appartenance à des groupes multicast en utilisant des messages MLD transmis dans les tunnels vers les mobiles. De cette manière, il maintient, pour chaque mobile, une vue à jour des groupes multicast auxquels il appartient et lui fait suivre les paquets multicast par l'intermédiaire du tunnel.

Pour l'émission de paquet multicast, le mobile possède également deux solutions lorsqu'il est hors de son réseau mère :

- Emission des paquets en utilisant le routeur multicast local (celui du réseau visité). Dans ce cas le mobile utilise l'adresse temporaire locale (CoA) comme adresse source et ne doit pas utiliser l'option home address dans les paquets multicast. Dans ce cas, cela implique que l'application doit gérer l'existence d'une adresse locale.

- Utilisation du tunnel pour émettre les paquets à partir du réseau d'origine du mobile à travers l'agent mère. Dans ce cas les déplacements restent transparents aux applications émettant du trafic multicast au niveau du mobile.

La première alternative pose des problèmes insolubles aux protocoles de routage multicast chargés de construire les arbres de diffusion dans le réseau. En effet, à chaque fois que le mobile change de localisation dans l'Internet, les arbres de diffusion déjà construits sont soit inutilisables soit ne correspondent plus au meilleur choix possible. De plus les membres du groupe adhèrent souvent à un groupe et à une source spécifique, ce qui suppose qu'à chaque changement de localisation du mobile, tout le processus d'adhésion recommence avec une nouvelle adresse de source et que l'arbre de diffusion spécifique à la source soit reconstruit.

La gestion du multicast pose d'importantes difficultés pour la réception aussi. Elle suppose un important travail de la part de l'agent mère qui doit déjà assurer le transfert des paquets unicasts lorsque l'optimisation de routage n'est pas utilisée. En effet, lorsque l'agent mère transformé pour l'occasion en routeur multicast IPv6 doit émettre une requête de demande d'appartenance aux groupes, il ne peut pas la transmettre en multicast comme un routeur multicast IPv6 normal, il doit au contraire envoyer une copie de la requête dans chacun des tunnels correspondant aux mobiles qui se sont enregistrés auprès de lui. De la même manière, il va devoir traiter autant de réponses qu'il y a de mobiles et ceux-ci ne peuvent pas utiliser les mécanismes de MLD qui permettent de limiter le trafic de signalisation.

Déplacements des mobiles

La gestion de la mobilité IPv6 Table des matières Les en-têtes de mobilité

La raison d'être de Mobile IPv6 est de gérer les déplacements des mobiles. Pour cela il faut être capable de détecter les changements de réseau, d'obtenir une nouvelle CoA, et informer l'agent mère et les correspondants du changement de localisation (i.e. de CoA). L'ensemble de ces opérations sont regroupées dans le "handover".

Contents

Détection du changement de réseau

La phase de détection de mouvement est cruciale. Elle représente une bonne part du délai d'interruption observé lors des changements de réseau. Le mobile utilise la gestion de voisinage pour détecter qu'un voisin, en l'occurrence son routeur par défaut, n'est plus accessible. Le défaut de ce mécanisme est que le mobile ne détecte la perte du routeur par défaut que lorsqu'il a des données à transmettre, ce qui retarde la détection du changement de réseau et augmente d'autant la durée des interruptions.

Une solution alternative suppose la coopération du routeur IPv6 qui ajoute dans les annonces de routeur une option indiquant le délai entre deux annonces. Le mobile qui écoute en permanence les annonces émises peut alors déduire de la perte de plusieurs annonces successives qu'il vient probablement de changer de réseau. Une autre adaptation demandée au routeur IPv6 concerne la réduction du délai entre deux annonces successives pour améliorer encore la vitesse de détection, ainsi il est conseillé d'émettre une annonce de routeur non sollicité toutes les 50 ms en moyenne (au lieu de 3s). Évidemment une telle configuration induit un trafic non négligeable pour certains types de réseau (réseau locaux sans fil).

Il est important de réduire le nombre de *handover* car ceux-ci induisent une rupture temporaire des communications et une signalisation importante dans le réseau. Le mobile peut utiliser d'autres informations pour décider de la nécessité d'effectuer un handover, mais il doit le faire prudemment. Par exemple, le mobile ne peut pas utiliser la découverte d'un nouveau réseau (une annonce de routeur avec un nouveau préfixe) pour décider qu'il a perdu l'accès à son ancien réseau. Il est, en effet, possible de recevoir simultanément des annonces en provenance de plusieurs routeurs annonçant des préfixes différents sur un même réseau.

Lorsqu'il reçoit une annonce de routeur, le mobile doit prendre en compte le préfixe annoncé et non l'adresse source des annonces de routeur pour détecter un changement, car des routeurs appartenant à des réseaux différents peuvent utiliser la même adresse lien-local. Dans ce cas, le bit `R` qui permet d'indiquer une adresse globale du routeur peut lever l'ambiguïté.

Notons que les mécanismes de détection de changement de réseau décrits sont complètement indépendants du niveau liaison. Il est possible de prendre en compte les informations connues du niveau liaison, comme le fait que le mobile vient de perdre ou d'acquérir un nouveau réseau sans-fils ou une nouvelle interface, pour déclencher la procédure du handover IPv6. Emettre une sollicitation de routeur aussitôt qu'un changement de réseau d'accès est soupçonné, permet de gagner un temps important mais suppose une implémentation plus complexe, puisque dépendante d'un niveau liaison particulier. En contrepartie, il est possible d'éviter l'envoi fréquent d'annonces de routeur non sollicitées.

Configuration de l'adresse temporaire

Une fois que le mobile a détecté la perte du routeur par défaut, il doit acquérir une nouvelle adresse en sollicitant un routeur. A réception d'une annonce de routeur sur le nouveau réseau il peut découvrir le préfixe du réseau et configurer une adresse globale appartenant à ce préfixe qui sera la nouvelle adresse temporaire (CoA). Lors de cette configuration, le mobile doit effectuer une procédure de détection d'adresse dupliquée (DAD) pour la nouvelle adresse. Sous certaines conditions, on cherchera à réduire la durée de cette procédure en émettant la sollicitation de voisin sans attendre le délai aléatoire habituel. D'autres proposition ont été faites pour ne pas attendre la seconde réglementaire qu'une éventuelle station défendant l'adresse réponde à la sollicitation de voisin.

Notons que le mobile peut configurer une adresse pour chaque préfixe annoncé sur le lien local. Toutes ces adresses seront des care-of address. Mais il devra choisir l'une d'entres-elles pour mettre à jour les associations au niveau du HA et des correspondants. Elle sera dite primary care-of address ou adresse temporaire primaire.

Avertissement de l'agent mère

Dès que le mobile a changé de care-of address principale, il doit en informer l'agent mère en envoyant une mise à jour d'association (*binding update*). Cette mise à jour peut être la première, dans ce cas, l'agent mère crée l'association. Dans le cas contraire, il met à jour l'association courante. Une mise à jour d'association, sera par la suite envoyée régulièrement, avant le délai d'expiration, pour maintenir l'association.

Lorsqu'il crée une nouvelle association, l'agent mère effectue la procédure de détection de duplication d'adresse (DAD) pour la home address avant d'acquitter l'association au mobile. Si un autre mobile ou une station sur le réseau mère possède cette adresse il répond au mobile que l'adresse est déjà utilisés et ce dernier doit essayer une autre adresse.

Découverte dynamique de l'agent mère

Il peut arriver que le mobile ne connaisse pas l'adresse d'un agent mère sur son réseau mère ou que l'agent mère qu'il connaissait ne réponde plus. Dans ce cas, le mobile doit tenter de découvrir l'adresse d'un agent mère apte à assumer ce rôle pour lui. Il envoie pour cela un paquet ICMP à l'adresse anycast des "Agents mère IPv6" pour le préfixe de son réseau mère.

Lorsque le mobile reçoit une réponse celle-ci contient une liste ordonnée des adresses globales des HAs du réseau mère. Il essaye ensuite dans l'ordre les adresses des agents mère de la liste jusqu'à recevoir un acquittement positif à sa demande de mise à jour d'association.

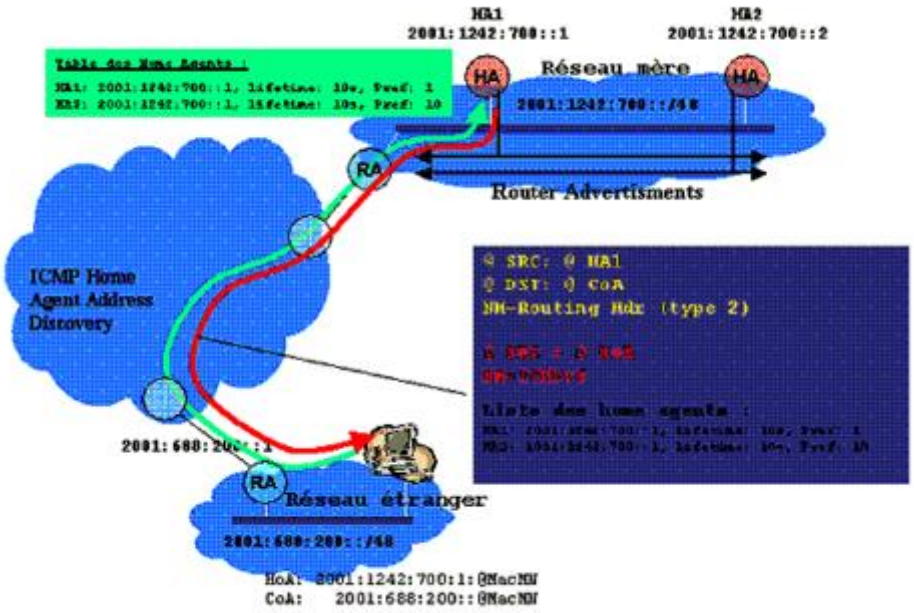

Figure 13-9 *Découverte dynamique de l'agent mère*

Pour supporter ce service, chaque HA doit être capable de découvrir les autres HAs sur le réseau mère pour en maintenir la liste. Il écoute pour cela les annonces de routeur émises sur le lien. Celles qui annoncent offrir le service d'agent mère (bit H : *Home Agent* validé) sont ajoutées à la liste. L'annonce de HA peut contenir d'autres informations utiles dans l'option home agent advertisement option : le délai de validité (*lifetime*), une adresse globale et une préférence. Cette dernière est utilisée pour ordonner la liste transmise au mobile.

Dans l'exemple, figure Découverte dynamique de l'agent mère, la requête ICMP du mobile atteint l'agent mère 1 mais ce denier renvoie une liste indiquant que l'agent mère 2 est plus prioritaire. Le mobile continuera donc la procédure en demandant à l'agent mère 2 d'enregistrer l'association.

Ce mécanisme pourra être implémenté pour distribuer la fonction d'agent mère sur plusieurs serveurs et pour répartir dynamiquement la charge entre les différents serveurs. La charge des agents mère est un point très critique de la mobilité IP et il est nécessaire de trouver des solutions permettant de résister au facteur d'échelle.

Interception des paquets par l'agent mère

L'agent mère doit assurer l'interception des paquets à destination du mobile dès qu'il dispose d'une association entre l'adresse mère (HoA) et une adresse temporaire (CoA) valide. Pour cela il diffuse une annonce de voisin non sollicitée sur le réseau mère. Cette annonce indique aussi que toutes les tables de voisinage doivent être mise à jour pour associer la HoA du

mobile avec l'adresse de niveau 2 de l'agent mère. Comme le multicast n'est pas fiabilisé ce message est généralement émis plusieurs fois.

Ensuite, à chaque fois qu'une sollicitation de voisin concerne la HoA d'un mobile qu'il gère, le HA répond en lieu et place du mobile, pour associer la HoA du mobile avec son adresse de niveau 2. Il assure ainsi la défense de la HoA enregistrée dans l'association lors des procédures de détection de duplication d'adresse. Il répondra qu'il possède l'adresse si un autre mobile ou une autre station du réseau mère tente de la configurer.

Lorsque le HA a des paquets à transmettre au mobile, il doit agir comme un correspondant. Il utilise donc un en-tête de routage de type 2. Si par contre il s'agit de paquet qu'il intercepte pour le compte du mobile, ils sont encapsulés en utilisant l'encapsulation IP dans IP et envoyés à destination de l'adresse temporaire du mobile. Ce dernier traite ces paquets comme tout paquet disposant d'un en-tête de tunnelage. C'est-à-dire qu'il supprime l'en-tête externe et traite le paquet IP contenu comme s'il était arrivé directement.

L'agent mère ne fait pas suivre les paquets émis à destination de l'adresse lien local du mobile. Ceux-ci sont détruits et un message ICMP annonçant l'indisponibilité du mobile est envoyé à la source, sauf dans le cas du multicast ou le paquet est silencieusement écarté.

Information des correspondants

En acquittant la mise à jour d'association l'agent mère informe le mobile qu'il possède une association en règle et ce dernier peut informer ses correspondants. Pour cela il effectue la procédure RR (Return Routability Procedure - Procédure de test de Routage Retour) qui sera vue plus loin puis la mise à jour d'association. Il doit le faire pour tous les correspondants qui sont dans la liste des associations qu'il maintient.

Gestion de l'adresse mère

La validité de l'adresse mère, comme celle des autres adresses IPv6, est limitée dans le temps. La limite vient de la durée de validité annoncée dans l'annonce de routeur contenant le préfixe. Lorsqu'une adresse mère approche de sa date de péremption, le mobile ne peut pas envoyer tout simplement de sollicitation de routeur s'il n'est pas dans le réseau mère. Dans ce cas il émet un message appelé "sollicitation de préfixe mobile", directement vers l'agent mère. Ce message est semblable à une sollicitation de routeur, mais il contient l'option d'en-tête destination home address. Il doit être protégé par IPsec comme la plupart des échanges entre le mobile et l'agent mère. Ce dernier répond à la sollicitation par une annonce de préfixe mobile ressemblant à une annonce de routeur et dont les éléments seront traités par le mobile comme si l'annonce avait été reçue sur le réseau mère. En particulier le préfixe du réseau mère permet de mettre à jour la durée de validité de l'adresse mère.

Ce mécanisme permet de supporter la renumérotation du réseau mère. En effet, lorsque le mobile reçoit un nouveau préfixe, il peut configurer une nouvelle adresse mère en utilisant les mécanismes habituels d'auto configuration sans état.

Retour dans le réseau mère

Lorsqu'il détecte qu'il est de retour dans le réseau mère, le mobile doit en informer l'agent mère pour que ce dernier cesse de faire suivre les paquets à l'ancienne localisation du mobile.

Il utilise pour détecter son retour dans le réseau mère une annonce de routeur contenant le préfixe de sa home address.

Pour envoyer la mise à jour d'association à l'agent mère, le mobile doit connaître l'adresse de niveau 2 de l'agent mère ce qui peut être déduit de l'annonce de routeur. Toutefois, il peut y avoir plusieurs agents mère sur le réseau. Dans ce cas le mobile doit découvrir l'adresse de niveau 2 de l'agent mère sans utiliser sa home address puisque l'agent mère est configuré pour la défendre dans les procédures de détection d'adresse dupliquée. Il demande donc l'adresse de niveau 2 de l'agent mère en émettant une sollicitation de voisin avec comme adresse source l'adresse non définie (::). Par contre il doit utiliser la home address comme adresse source de la mise à jour d'association et être en mesure de recevoir l'acquittement qui sera transmis par l'agent mère à cette adresse. Il doit donc configurer préalablement son interface avec la home address sans effectuer de procédure de détection d'adresse dupliquée.

Dès que la procédure de mise à jour d'association est terminée le mobile peut diffuser une annonce de voisin indiquant qu'il reprend possession de sa home address à toutes les autres stations sur le réseau local. Le bit indiquant la sollicitation devra être à zéro, tandis que celui indiquant que toutes les stations doivent mettre à jour leur cache avec la nouvelle association sera mis à 1. Ce message sera émis plusieurs fois pour prévenir les pertes éventuelles sur le réseau local. Une fois cette procédure terminée il doit supprimer les associations maintenues par les correspondants pour toutes les associations qu'il maintient.

Les en-têtes de mobilité

Déplacements des mobiles | Table des matières | Les risques induits par la mobilité et leur limitation

Format général du paquet

Nous avons vu que les en-têtes de mobilité sont utilisés pour transporter la signalisation de la gestion des associations de mobilité entre le noeud mobile, son agent mère et le noeud correspondant.

Un en-tête de mobilité ne doit jamais être utilisé en même temps qu'un en-tête de routage de type 2, excepté dans le seul cas du transport d'un acquittement d'une demande de BU. Il ne doit jamais non plus être utilisé en même temps qu'une extension de destination, sauf dans certains cas de Binding Update avec l'agent mère ainsi qu'avec des noeuds correspondants déjà identifiés.

Le format général d'un en-tête de mobilité est donné figure Format de l'extension de mobilité :

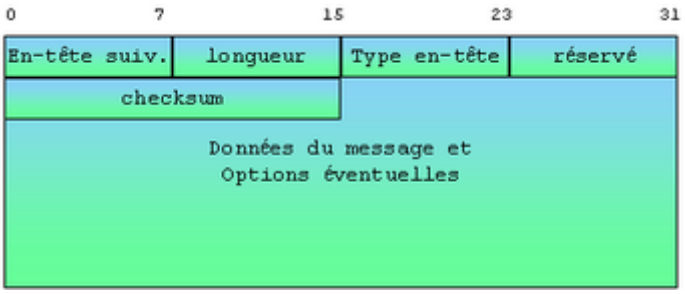

Figure 13-10 *Format de l'extension de mobilité*

- Le champ en-tête suivant est pris dans le même espace de numérotation que les en-têtes d'extension d'IPv6 (cf. Valeurs du champ en-tête suivant). Dans le cas de la signalisation de mobilité, il doit valoir 59 (pas d'en-tête suivant).
- Le champ longueur de l'en-tête, en octets, ne prend pas en compte les 8 premiers octets de l'en-tête.
- Le champ type d'en-tête décrit les messages de signalisation donné au tableau Type des en-têtes de mobilité.

Type des en-têtes de mobilité	
0	Demande de rafraîchissement émise par le noeud correspondant
1	Initialisation de test d'adresse mère (HoTI)
2	Initialisation de test d'adresse temporaire (CoTI)

3	Test d'adresse mère (HoT)
4	Test d'adresse temporaire (CoT)
5	Mise à jour d'association (émise depuis le noeud mobile)
6	Acquittement de mise à jour d'association
7	Erreur de mise à jour d'association

La structure et la longueur du message varient en fonction du numéro de l'en-tête. De plus, MIPv6 définit également des options de mobilité associées à ces messages. Comme la longueur des messages associés à chaque numéro d'en-tête est connue, la présence d'une option est déduite d'une longueur de l'en-tête plus grande que ce qui est suffisant pour le message. Elle se trouve forcément à la suite du message.

Comme toutes les en-tête IPv6, ces en-têtes de mobilité doivent être alignés sur des frontières de 8 octets. Des champs réservés seront éventuellement insérés pour respecter cette contrainte. Un noeud ne sachant pas interpréter une option doit l'ignorer. Actuellement MIPv6 ne définit d'option que pour les messages de BU (type 5) et leur acquittement (type 6).

Format des messages et options des différents types d'en-têtes

Figure 13-11 *Format de l'extension de mobilité rafraîchissement d'association*

La demande de rafraîchissement d'association ne requiert aucune information spécifique. Le message est vide, il n'y a pas d'option. (cf. figure Format de l'extension de mobilité rafraîchissement d'association).

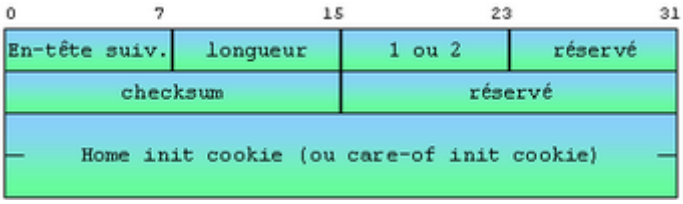

Figure 13-12 *Format de l'extension de mobilité HoTI ou CoTI*

Les messages HoTI, CoTI ne contiennent que le nombre aléatoire émis par le noeud mobile. Il ne contient pas d'option. (cf. figure Format de l'extension de mobilité HoTI ou CoTI).

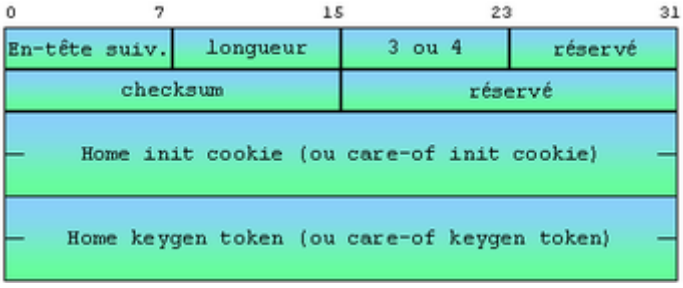

Figure 13-13 *Format de l'extension de mobilité HoT ou CoT*

Les messages HoT, CoT contiennent, l'index du nombre aléatoire (nonce) choisi par le noeud correspondant, le nombre aléatoire émis par le noeud mobile (*cookie*), (pour le test home address ou care-of address) et le jeton chiffré (`keygen token`) émis par le noeud correspondant. Il ne contient pas d'option (cf. figure Format de l'extension de mobilité HoT ou CoT).

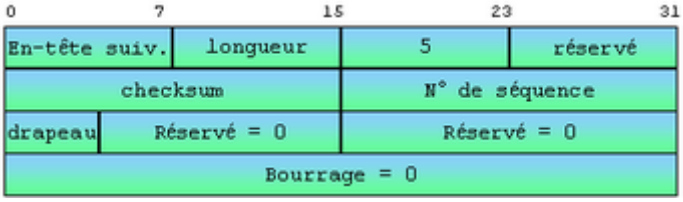

Figure 13-14 *Format de l'extension de mobilité mise à jour d'association*

Les messages de notification de mise à jour d'association, émis par le noeud mobile, peuvent contenir des options mobiles. Si elles ne sont pas présentes, le paquet doit se terminer par 4 octets de bourrage. (cf. figure Format de l'extension de mobilité mise à jour d'association)

Les options possibles sont :

- Les données d'autorisation de mise à jour d'association. L'option est obligatoire pour les mises à jour émises vers le noeud correspondant puisqu'elles ne sont pas protégées par IPsec.
- L'indice du "nonce" choisi par le noeud correspondant.
- Une "care-of address" alternative.

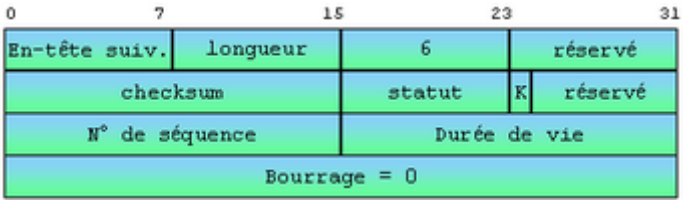

Figure 13-15 *Format de l'extension de mobilité acquittement de mise à jour d'association*

Les message d'acquittement de mise à jour d'association peut contenir des options mobiles. Si elles ne sont pas présentes, le paquet doit être terminé par 4 octets de bourrage. (cf. figure Format de l'extension de mobilité acquittement de mise à jour d'association) :

- Une valeur du champ statut inférieure à 128 indique un acquittement, et une valeur supérieure un rejet. Le motif du rejet est codé par la valeur du statut.

- Le bit K = 1 indique que l'association de sécurité IPsec suivra les mouvements du noeud mobile. Le noeud correspondant doit le positionner à 0.
- Les options possibles sont :
    - Les données d'autorisation de mise à jour d'association.
    - Les informations de fréquence de rafraîchissement des associations.

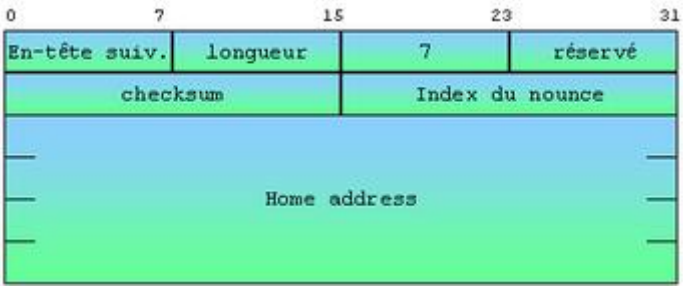

Figure 13-16 *Format de l'extension de mobilité message d'erreur*

Les messages d'erreur de mise à jour d'association contiennent un statut sur 8 bits codant l'erreur, ainsi que la home address de la mise à jour en erreur pour le cas où le noeud mobile aurait établi plusieurs associations avec le noeud correspondant (cf. figure Format de l'extension de mobilité message d'erreur).

Déplacements des mobiles | Table des matières | Les risques induits par la mobilité et leur limitation

Les risques induits par la mobilité et leur limitation

Les en-têtes de mobilité | Table des matières | Sécurisation de la signalisation avec les noeuds correspondants

La mobilité doit satisfaire les deux contraintes de sécurité suivantes :

- L'introduction de la mobilité dans IP ne doit pas introduire de nouvelles vulnérabilités dans le réseau,
- Une communication dans un contexte mobile ne doit pas être plus risquée que dans un contexte fixe.

La sécurisation de MIPv6 est prévue dans le cadre standard de l'Internet où l'infrastructure de routage est réputée correcte, c'est-à-dire où un paquet destiné à un noeud A est effectivement acheminé vers ce noeud A. Cette sécurisation vise à obtenir un niveau de confiance des communications mobiles, égal à ou proche de celui offert aux communications fixes.

Les risques pour le noeud mobile

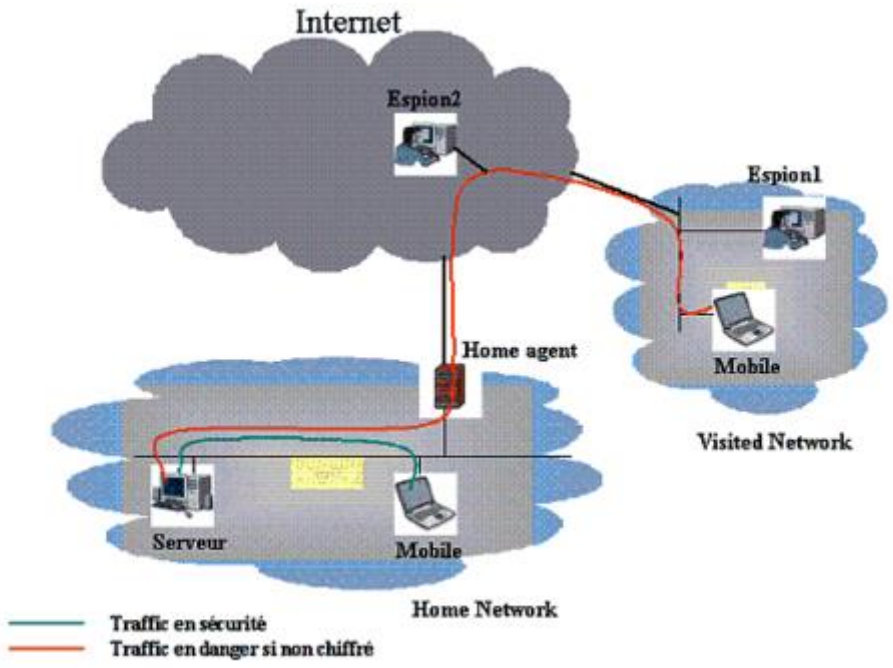

Figure 13-17 *Chiffrement nécessaire des données*

Un noeud dans son réseau mère (*home network* dans les figures) considère généralement son environnement comme amical, surtout lorsqu'il communique avec des correspondants également situés dans son réseau mère. En visite dans un autre réseau il doit se montrer plus circonspect. En particulier, il devra assurer la confidentialité des données transmises, par

exemple en utilisant IPsec, afin d'éviter qu'elles ne soient épiées, au niveau du réseau visité, mais également sur le chemin entre le réseau visité et son réseau mère (cf. figure Chiffrement nécessaire des données).

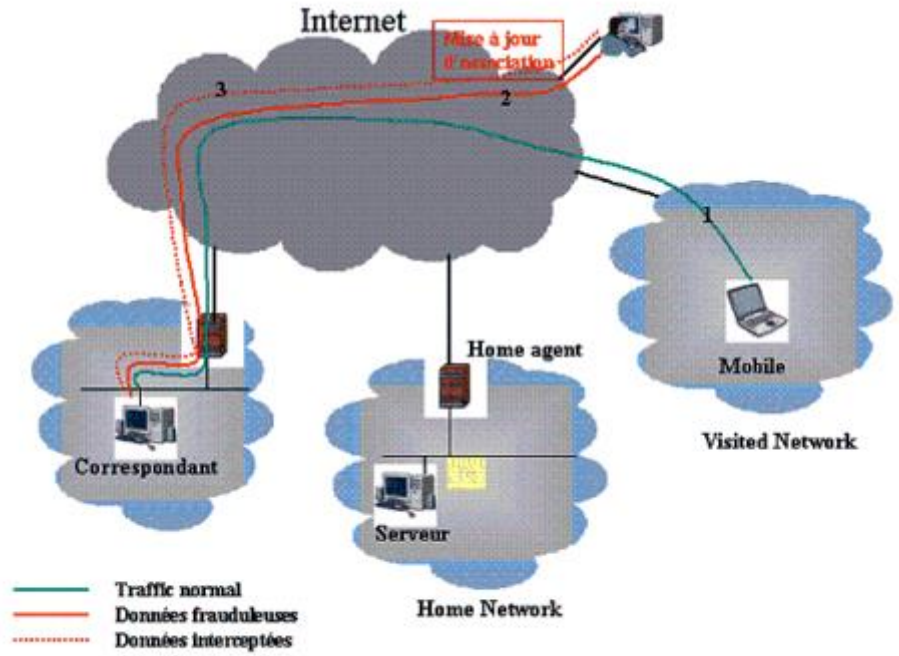

Figure 13-18 *Détournement de trafic*

Un noeud mobile peut également souffrir de déni de service si les mises à jour d'association avec son agent mère sont falsifiées. Un noeud hostile dans le réseau visité, ou partout ailleurs dans le réseau, pourrait envoyer une fausse demande de mise à jour d'association afin de détourner le trafic de son véritable destinataire. Il est donc important pour le noeud mobile de sécuriser ces mises à jour (cf. figure Détournement de trafic).

L'IETF a décidé d'utiliser IPsec pour la signalisation entre le mobile et son agent mère, spécifiée dans le RFC 3776.

.

Les risques pour les autres noeuds

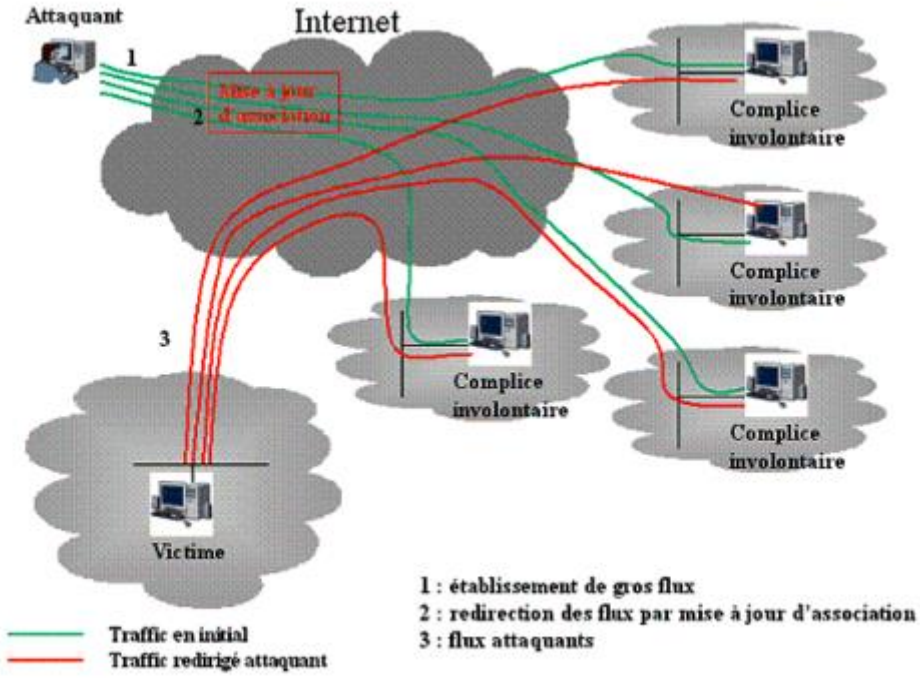

Figure 13-19 *Déni de service envers un noeud tiers*

Un noeud malveillant peut utiliser des messages de mise à jour d'association frauduleux pour détourner de ses clients légitimes les flux d'un serveur mettant en oeuvre la mobilité. Ce cas est similaire au cas du détournement du trafic destiné à un noeud mobile. Un noeud malveillant peut également utiliser des noeuds mettant en oeuvre la mobilité pour inonder un autre noeud, de trafic non sollicité, de façon à engorger ses liens de communication, ceci sans même que la victime ne mette en oeuvre la mobilité (cf. figure Déni de service envers un noeud tiers).

On notera que ces risques sont exclusivement liés à la mise en oeuvre de l'optimisation du routage. Afin de les diminuer jusqu'à un niveau acceptable, sans pénaliser les performances du protocole, MIPv6 prévoit la procédure de test de "routage retour" entre le noeud mobile et son correspondant. Cette procédure est décrite au paragraphe suivant et spécifiée dans le RFC 3775.

Les en-têtes de mobilité | Table des matières | Sécurisation de la signalisation avec les noeuds correspondants

Sécurisation de la signalisation avec les noeuds correspondants

Les risques induits par la mobilité et leur limitation | Table des matières | Protection de la signalisation par le protocole IPsec

La procédure de test de routage retour

Les mises à jour d'association étant fréquentes, il est important que cette procédure soit la plus légère possible. Un noeud mobile et un noeud correspondant ne se connaissent pas à priori. Ils ne partagent donc pas de secret susceptible de chiffrer leurs échanges lors des différentes mises à jour d'association nécessaires pendant toute la durée de la communication. L'utilisation d'IPsec et d'une procédure d'échange sécurisé des clefs aurait été trop lourde. La procédure choisie a pour premier but de générer ce secret partagé.

Afin d'éviter l'attaque en déni de service à l'encontre d'un noeud tiers, elle garantit au noeud correspondant que, pour une certaine adresse temporaire et pour une certaine adresse mère, il y a effectivement un noeud mobile prêt à recevoir un paquet.

La procédure est conçue de façon à ce que le noeud correspondant ne puisse pas subir lui-même une attaque en déni de service par la simple exécution répétée de la procédure. A cette fin, elle consomme peu de ressources de calcul, et les ressources mémoires nécessaires ne dépendent pas du nombre de demande d'association. Enfin, pour ne pas surcharger le réseau, le noeud correspondant n'émet pas plus de paquets qu'il n'en reçoit.

La procédure est constituée de deux phases préliminaires, dont l'une teste la home address et l'autre teste la care-of address. Ensuite toute demande de mise à jour, ou de destruction d'association sera assujettie à l'exécution correcte des ces deux phases préliminaires.

Les deux phases sont menées parallèlement l'une de l'autre, à l'initiative du noeud mobile. Le noeud correspondant répond à leurs requêtes indépendamment l'une de l'autre. Il demeure sans état jusqu'à ce qu'une association soit établie. Les messages doivent donc être autosuffisants pour que la procédure puisse se dérouler.

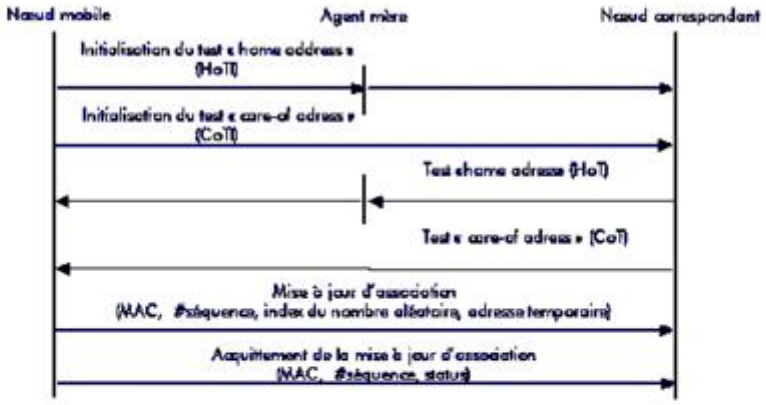

Figure 13-20 *Routage retour*

La procédure (cf. figure Routage retour) nécessite que le noeud mobile dispose d'un ensemble de nombres aléatoires secrets (*nonces*), tels que l'index d'un de ces nombres suffise à le retrouver dans cet ensemble. Elle nécessite également que le noeud correspondant dispose d'une clef secrète notée `Kcn`.

Un message HoTI, émis depuis la home address du noeud mobile vers le noeud correspondant (donc via l'agent mère), contient une valeur aléatoire sur 64 bits, le *home init cookie* identifiant cette home address.

Un message HoT, émis par le noeud correspondant en réponse au message HoTI à destination de la home address du mobile, donc toujours via l'agent mère contient trois valeurs :

- le *home init cookie* obtenu dans le message HoTI,
- l'index sur 16 bits d'un nonce, choisi par le noeud correspondant,
- le home keygen token, calculé par le noeud correspondant :

```
premiers (64, HMAC_SHA1 (Kcn, (home address | nonce | 0 )))
```

Un message CoTI, émis depuis la care-of address du noeud mobile, directement vers le noeud correspondant, contient une seconde valeur aléatoire sur 64 bits, le *care-of init cookie* identifiant cette care-of address.

Un message CoT, émis par le noeud correspondant en réponse au message CoTI du noeud mobile, directement vers le noeud mobile contient trois valeurs :

- le *care-of init cookie* obtenu dans le message CoTI,
- l'index sur 16 bits d'un second nonce, choisi par le noeud correspondant,

- le care-of keygen token, calculé par le noeud correspondant :

```
premiers (64, HMAC_SHA1 (Kcn, (care-of address| nonce | 1 )))
```

Lorsque le noeud mobile a reçu les messages HoT et CoT, la procédure de test du routage retour est terminée. Arrivé à ce point, le noeud mobile calcule `Kbm`, la clef de gestion des associations (*key binding management*) telle que :

```
Kbm = SHA1 ( "home keygen token" | "care-of keygen token")
```

pour la mise à jour d'une association, ou

```
Kbm = SHA1 ( "home keygen token")
```

pour sa destruction.

Pour demander une nouvelle association, le noeud mobile envoie, depuis sa care-of address courante, à destination du noeud correspondant, une demande d'association contenant cinq informations :

- Sa home address
- Un numéro de séquence d'association
- Les deux index des home et care-of nonces
- Une valeur chiffrée
- `Premier( 96, HMAC_SHA1(Kbm , ("home address" | adresse du noeud correspondant | donnée de la mise jour d'association)))`

On notera que puisque les indexes des nombres aléatoires secrets sont fournis par le noeud mobile, le noeud correspondant peut recalculer `Kbm`. `Kbm` est donc bien une clef partagée utilisable dans une procédure `HMAC_SHA1` pour vérifier la légalité d'une demande de mise à jour d'association.

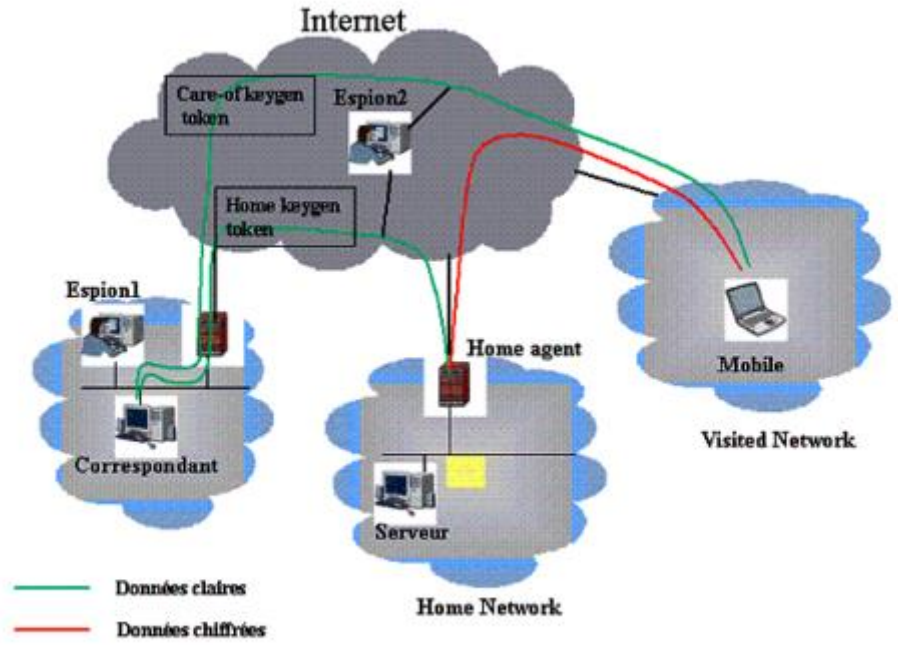

Figure 13-21 *Attaque contre le routage retour*

La correction de la procédure repose sur l'hypothèse qu'aucun intrus ne peut écouter à la fois les messages home test et care-of test ni connaître `Kbm`. Ces messages utilisant deux chemins différents pour joindre le noeud correspondant (cf. figure Attaque contre le routage retour), il faudrait donc que l'intrus se trouve dans le réseau du noeud correspondant. Dans ce cas, la mobilité n'introduit pas plus de risque que IP fixe lui-même.

Par contre, si un noeud malveillant obtient les deux home et care-of keygen tokens, il pourra par la suite envoyer de fausses demandes de mise à jour d'association. Pour cela, ce noeud doit écouter des données circulant en clair sur les 2 chemins conduisant du noeud mobile au noeud correspondant, directement et via l'agent mère. La probabilité que cette écoute soit possible augmente si le noeud malveillant est proche du noeud correspondant. L'écoute est définitivement possible lorsque l'on est connecté au réseau du noeud correspondant.

Les message HoTI, CoTI, HoT et CoT sont transportés dans des en-têtes d'extension de mobilité (numéro de protocole 135). Chacun possède un numéro de type d'en-tête de message particulier (respectivement 1,2,3,4).

La procédure conduit au partage d'un secret entre les noeuds mobile et correspondant. Il est nécessaire de rafraîchir régulièrement ce secret. Le rafraîchissement est laissé à l'initiative du noeud correspondant. Il est mise en oeuvre en expirant la validité du nonce utilisé dans la clef `Kbm`. Une demande de modification d'association arrivant avec un nonce expiré sera refusée via le message d'acquittement. Le noeud mobile relancera alors la procédure pour obtenir une nouvelle `Kbm` basée sur un nonce valide.

La clef `Kcn` doit elle même être régulièrement régénérée. Elle le sera en particulier à chaque redémarrage du noeud correspondant et préférablement lors de chaque régénération de nonce.

Il est en effet nécessaire que chaque nonce soit associé à la bonne `Kcn` dans la vérification de la clef `Kbm` d'une demande de mise à jour d'association.

La vérification par le noeud correspondant d'une clef `Kbm` s'effectue en vérifiant que :

- Les nonces HoA et CoA ne sont pas expirés,
- Le re-calcul de `Kbm`, sur la base des indices des nonces et de la `Kcn` associée, est cohérent avec la valeur `Kbm` contenue dans la demande d'association.

Un message d'erreur est envoyé en cas d'expiration d'une au moins des nonces. Aucun message d'erreur n'est émis dans le cas ou le re-calcul de la `Kbm` échoue. Dans le cas de nonce expiré, il est nécessaire de procéder au re-calcul sur la base d'une éventuelle ancienne valeur de `Kcn` pour n'envoyer de message d'expiration que si la `Kbm` est valide par rapport à l'ancienne `Kcn`.

Seul le noeud mobile maintient l'état des données de sécurité de chaque association. Les informations home init cookie et care-of init cookie peuvent être supprimées dès réceptions des nonces et keygen tokens. Les demandes de création d'association sont à l'initiative du noeud mobile. Il n'est donc pas sujet à une attaque en déni de service par consommation excessive de ressources mémoire.

Le noeud correspondant maintient un état de sécurité indépendant du nombre d'associations en cours. Il n'est donc pas sujet non plus à une attaque en déni de service par consommation excessive de ressources mémoire.