Groupe de travail Réseau
Request for Comments : 5026
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

G. Giaretta, éd., Qualcomm
J. Kempf, DoCoMo Labs USA
V. Devarapalli, éd., Azaire Networks
octobre 2007

Amorçage IPv6 mobile dans le scénario partagé

Résumé
Un nœud mobile IPv6 a besoin d'une adresse d'agent de rattachement, d'une adresse de rattachement, et d'associations de sécurité IPsec avec son agent de rattachement avant qu'il puisse commencer à utiliser le service IPv6 mobile. La RFC 3775 exige que certains ou tous soient configurés de façon statique. Le présent document définit comment un nœud IPv6 mobile peut amorcer ces informations à partir d'informations non topologiques et d'accréditifs de sécurité pré-configurés sur le nœud mobile. La solution définie dans le présent document résout le scénario partagé décrit dans la déclaration de problème d'amorçage IPv6 mobile de la RFC 4640. Le scénario partagé se réfère au cas où le service de mobilité du nœud mobile est autorisé par un fournisseur de service différent de l'accès réseau de base. La solution décrite dans ce document est aussi généralement applicable à tout cas d'amorçage, car les autres scénarios sont des réalisations plus spécifiques du scénario partagé.

Table des Matières

1. Introduction

IPv6 mobile [RFC3775] exige du nœud mobile qu'il connaisse l'adresse de son agent de rattachement, sa propre adresse de rattachement, et les matériaux de chiffrement (par exemple, les clés partagées ou les certificats) nécessaires pour établir les associations de sécurité IPsec avec l'agent de rattachement (HA) afin de protéger la signalisation IPv6 mobile. Ceci est généralement appelé le problème de l'amorçage IPv6 mobile [RFC4640].

Le protocole de base IPv6 mobile ne spécifie aucune méthode pour acquérir automatiquement ces informations, ce qui signifie que les administrateurs de réseau sont normalement obligés de régler manuellement les données de configuration sur les nœuds mobiles et les HA. Cependant, dans les déploiements réels, la configuration manuelle ne convient plus lorsque le nombre de nœuds mobiles augmente.

Comme discuté dans la [RFC4640], plusieurs scénarios d'amorçage peuvent être identifiés selon les relations entre l'opérateur de réseau qui authentifie un nœud mobile pour accorder le service d'accès au réseau (ASA, *Access Service Authorizer*) et le fournisseur de service qui autorise le service IPv6 mobile (MSA, *Mobility Service Authorizer*). Le présent document décrit une solution au problème de l'amorçage qui est applicable dans un scénario où le MSA et l'ASA sont des entités différentes (c'est-à-dire, un scénario partagé).

2. Terminologie

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

La terminologie générale de la mobilité se trouve dans la [RFC3753]. Les termes supplémentaires suivants sont utilisés ici :

Autorité de service d'accès (ASA, *Access Service Authorizer*) : opérateur de réseau qui authentifie un nœud mobile et établit l'autorisation du nœud mobile de recevoir le service Internet.

Fournisseur de service d'accès (ASP, *Access Service Provider*) : opérateur de réseau qui assure la transmission directe de paquet IP de et vers l'hôte d'extrémité.

Autorité de service de mobilité (MSA, *Mobility Service Authorizer*) : opérateur de réseau qui autorise le service IPv6 mobile.

Fournisseur du service de mobilité (MSP, *Mobility Service Provider*) : opérateur de réseau qui fournit le service IPv6 mobile. Pour obtenir un tel service, le nœud mobile doit être authentifié et prouver qu'il a l'autorisation d'obtenir le service.

Scénario partagé : scénario où le service de mobilité et le service d'accès au réseau sont autorisés par des entités différentes. Cela implique que la MSA est différente de l'ASA.

3. Scénario partagé

Dans la description de la déclaration du problème [RFC4640], il y a l'hypothèse claire que le service de mobilité et le service d'accès au réseau peuvent être séparés. Cette hypothèse implique que service de mobilité et service d'accès au réseau peuvent être autorisés par des entités différentes. Par exemple, le modèle de service défini dans la [RFC4640] permet à un réseau d'entreprise de déployer un agent de rattachement et d'offrir le service IPv6 mobile à un utilisateur, même si l'utilisateur accède à l'Internet indépendamment de son compte d'entreprise (par exemple, en utilisant son compte personnel d'accès WiFi dans un salon de thé).

Donc, on suppose dans ce document que l'accès réseau et le service de mobilité sont autorisés par des entités différentes, ce qui signifie que l'authentification et l'autorisation pour le service de mobilité et l'accès au réseau vont être considérées séparément. Ce scénario est appelé scénario partagé.

De plus, le modèle défini dans la [RFC4640] sépare l'entité qui fournit le service de l'entité qui authentifie et autorise

l'utilisateur. Ceci est similaire au modèle d'itinérance pour l'accès réseau. Donc, dans le scénario partagé, deux cas différents peuvent être identifiés selon les relations entre l'entité qui fournit le service de mobilité (c'est-à-dire, le fournisseur du service de mobilité, MSP) et l'entité qui authentifie et autorise l'utilisateur (c'est-à-dire, l'autorité de service de mobilité, MSA).

La Figure 1 décrit le scénario partagé quand le MSP et la MSA sont la même entité. Cela signifie que l'opérateur du réseau qui fournit l'agent de rattachement authentifie et autorise l'utilisateur pour le service de mobilité.

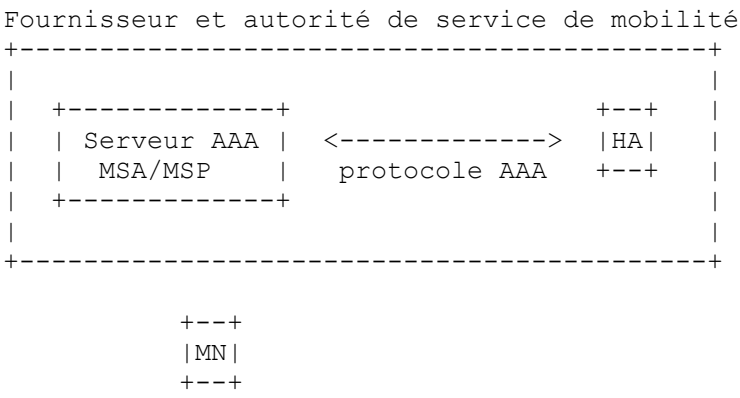


Figure 1 -- Scénario partagé (MSA == MSP)

La Figure 2 montre le scénario partagé dans le cas où la MSA et le MSP sont deux entités différentes. Cela peut arriver si le nœud mobile est loin de son réseau de MSA et est alloué à un HA plus proche pour optimiser l'efficacité ou si la MSA ne peut pas fournir d'agent de rattachement et s'appuie sur un tiers (c'est-à-dire, le MSP) pour accorder le service de mobilité à ses utilisateurs. Noter que le MSP pourrait ou non être aussi l'opérateur du réseau qui fournit l'accès réseau (c'est-à-dire, l'ASP, le fournisseur de service d'accès).

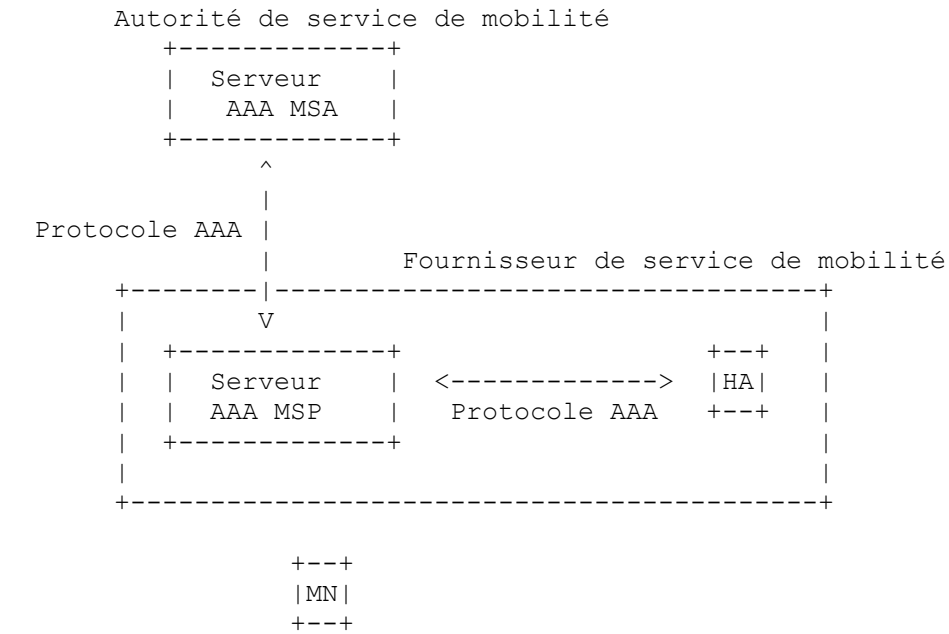


Figure 2 -- Scénario partagé (MSA != MSP)

Noter que les Figures 1 et 2 supposent l'utilisation d'un protocole d'authentification, autorisation, et comptabilité (AAA) pour authentifier et autoriser le nœud mobile pour le service de mobilité. Cependant, comme le protocole d'échange de clé Internet (IKEv2, *Internet Key Exchange version 2*) permet l'authentification d'un client seulement par le protocole d'authentification extensible (EAP, *Extensible Authentication Protocol*) et que l'authentification du serveur doit être effectuée sur la base de certificats ou de clés publiques, le nœud mobile exige potentiellement une vérification de liste de révocation de certificat (CRL, *Certificate Revocation List*) même si un protocole AAA est utilisé pour authentifier et autoriser le nœud mobile au service de mobilité.

Si à la place, une infrastrucure de clé publique (PKI, *Public Key Infrastructure*) est utilisée, le nœud mobile et le HA utilisent des certificats pour s'authentifier l'un l'autre et il n'y a pas de serveur AAA impliqué [RFC4210]. Ceci est conceptuellement similaire à la Figure 1, car le MSP == MSA, sauf que l'agent de rattachement, et potentiellement le nœud mobile, peut exiger une vérification de liste de révocation de certificat auprès de l'autorité de certification (CA, *Certification Authority*). La CA peut être interne ou externe au MSP. La Figure 3 illustre cela.

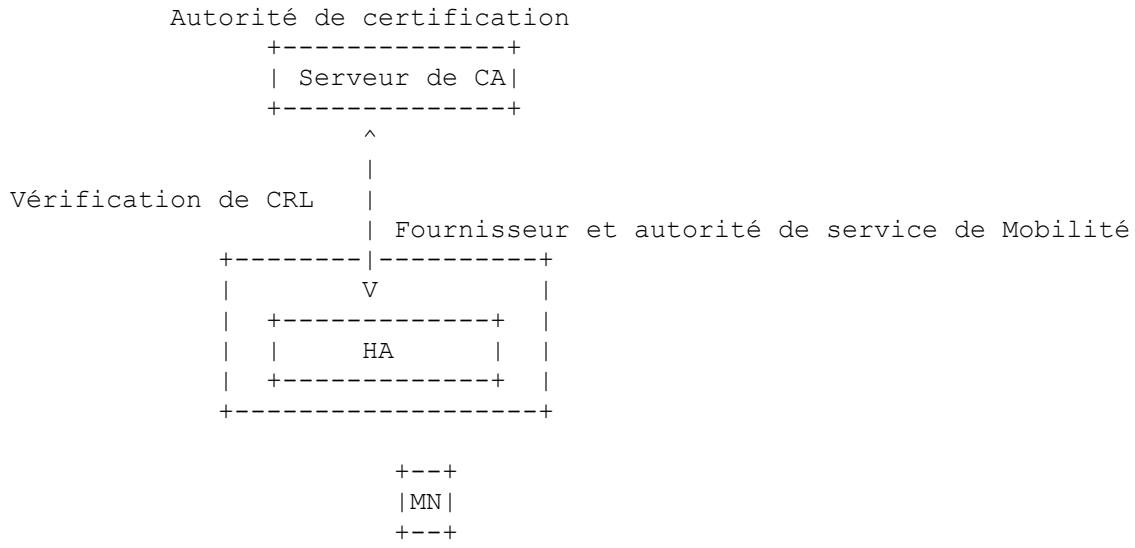


Figure 3 -- Scénario partage avec PKI

Pour plus de détails sur l'utilisation de PKI pour l'authentification IKEv2, se référer aux [RFC4877] et [RFC4945].

Le scénario partagé est le plus simple modèle qui peut être identifié, car aucune hypothèse sur le réseau d'accès n'est faite. Cela implique que le service de mobilité est amorcé indépendamment du protocole d'authentification pour le réseau d'accès utilisé (par exemple, EAP ou même accès ouvert). Pour cette raison, la solution décrite dans ce document et développée pour ce scénario pourrait aussi être appliquée au modèle de déploiement de réseau d'accès intégré [RFC4640], même si il pourrait n'être pas optimisé.

4. Composantes de la solution

Le problème de l'amorçage se compose de différents sous problèmes qui peuvent être résolus indépendamment d'une façon modulaire. Les composants sont identifiés et un bref survol de leur solution suit.

Découverte d'adresse de HA : le nœud mobile a besoin de découvrir l'adresse de son agent de rattachement. Le principal objectif d'une solution d'amorçage est de minimiser les données préconfigurées sur le nœud mobile. Pour cette raison, le DHAAD défini dans la [RFC3775] peut n'être pas applicable dans les déploiements réels car il est exigé que le nœud mobile soit préconfiguré avec le préfixe du réseau de rattachement et il n'est pas permis à un opérateur d'équilibrer la charge en ayant des nœuds mobiles alloués de façon dynamique aux agents de rattachement situés dans les différents sous réseaux. Le présent document définit une solution pour la découverte d'adresse d'agent de rattachement qui se fonde sur le service des noms de domaine (DNS, *Domain Name Service*) introduisant un nouvel enregistrement SRV du DNS [RFC2782]. L'unique information qui doit être préconfigurée sur le nœud mobile est le nom de domaine du MSP.

Établissement d'associations de sécurité IPsec : IPv6 mobile exige qu'un nœud mobile et son agent de rattachement partagent une SA IPsec afin de protéger les mises à jour de liens et autre signalisation IPv6 mobile. Le présent document donne une solution qui se fonde sur IKEv2 et suit ce qui est spécifié dans la [RFC4877]. L'authentification de l'homologue IKEv2 peut être effectuée en utilisant des certificats et en utilisant EAP selon le modèle de déploiement de l'opérateur du réseau.

Allocation d'adresse de rattachement (HoA) : le nœud mobile doit savoir son adresse de rattachement afin d'amorcer le fonctionnement de IPv6 mobile. L'adresse de rattachement est allouée par l'agent de rattachement durant l'échange IKEv2 (comme décrit dans la [RFC4877]). La solution définie dans le présent document permet aussi au nœud mobile

d'autoconfigurer son adresse de rattachement sur la base de l'auto-configuration sans état [RFC4861], des adresses générées cryptographiquement [RFC3972], ou des adresses de confidentialité [RFC4941].

Authentification et autorisation avec MSA : l'utilisateur doit être authentifié afin que le MSP accorde le service. Comme les accréditifs de l'utilisateur ne peuvent être vérifiés que par la MSA, cette étape d'autorisation est effectuée par la MSA. De plus, le service de mobilité doit être explicitement autorisé par la MSA sur la base du profil de l'utilisateur. Ces opérations sont effectuées de différentes façons selon les accréditifs utilisés par le nœud mobile durant l'authentification des homologues IKEv2 et sur l'infrastructure d'extrémité arrière (PKI ou AAA).

Une partie facultative de l'amorçage implique de fournir un moyen pour que le nœud mobile ait son nom de domaine pleinement qualifié (FQDN, *Fully Qualified Domain Name*) mis à jour dans le DNS avec une adresse de rattachement allouée de façon dynamique. Bien que toutes les applications n'exigent pas ce service, de nombreuses applications de réseautage utilisent le FQDN pour obtenir une adresse pour un nœud avant de débuter le trafic IP avec lui. La solution définie dans le présent document spécifie que la mise à jour dynamique du DNS est effectuée par l'agent de rattachement ou à travers l'infrastructure AAA, selon la relation de confiance installée.

5. Opérations du protocole

Cette Section décrit en détails les procédures nécessaires pour effectuer l'amorçage IPv6 mobile sur la base des composants identifiés dans la Section précédente.

5.1 Découverte de l'adresse de l'agent de rattachement

Une fois qu'un nœud mobile a obtenu l'accès au réseau, il peut effectuer l'amorçage IPv6 mobile. À cette fin, le nœud mobile interroge le serveur DNS pour demander des informations sur le service d'agent de rattachement. Comme mentionné précédemment dans ce document, le nœud mobile devrait être préconfiguré avec le nom de domaine du fournisseur du service de mobilité.

Le nœud mobile a besoin d'obtenir l'adresse IP d'un serveur DNS avant qu'il puisse envoyer une demande au DNS. Cela peut être configuré sur le nœud mobile ou obtenu par DHCPv6 sur la liaison visitée [RFC3646]. Dans tous les cas, on supposera qu'il y a un mécanisme pour que le nœud mobile soit configuré avec un serveur DNS car un serveur DNS est nécessaire pour bien d'autres raisons.

Deux options de recherche dans le DNS d'une adresse d'agent de rattachement sont identifiées dans ce document : recherche DNS par nom d'agent de rattachement et recherche DNS par nom de service.

Le présent document ne fournit pas de mécanisme spécifique pour équilibrer la charge des différents nœuds mobiles parmi les agents de rattachement. Il est possible à un MSP de réaliser un équilibrage de charge grossier en mettant à jour de façon dynamique les priorités de RR SRV pour refléter la charge actuelle sur la collection d'agents de rattachement du MSP. Les nœuds mobiles utilisent alors le mécanisme de priorité pour choisir de façon préférentielle le HA le moins chargé. L'efficacité de cette technique dépend de la charge qu'elle fait peser sur les serveurs DNS, en particulier si le DNS dynamique est utilisé pour des mises à jour fréquentes.

Bien que ce document spécifie une solution de découverte d'adresse d'agent de rattachement fondée sur le DNS, quand l'ASP et le MSP sont la même entité, DHCP peut être utilisé. Voir les détails dans la [RFC6611].

5.1.1 Recherche DNS par nom d'agent de rattachement

Dans ce cas, le nœud mobile est configuré avec le nom de domaine pleinement qualifié de l'agent de rattachement. Par exemple, le nœud mobile pourrait être configuré avec le nom "ha1.exemple.com", où "exemple.com" est le nom de domaine du MSP qui accorde le service de mobilité.

Le nœud mobile construit une demande au DNS en établissant le QNAME au nom de l'agent de rattachement. La demande a le QTYPE réglé à "AAAA" afin que le serveur DNS envoie l'adresse IPv6 de l'agent de rattachement. Une fois que le serveur DNS a répondu à l'interrogation, le nœud mobile connaît son adresse d'agent de rattachement et peut faire fonctionner IKEv2 afin de d'établir les SA IPsec et obtenir une adresse de rattachement.

Noter que la configuration du FQDN d'un agent de rattachement sur le nœud mobile peut aussi être étendue pour allouer

dynamiquement un agent de rattachement local à partir du réseau visité. Une telle allocation dynamique serait utile, par exemple, du point de vue de l'amélioration de l'efficacité de l'acheminement en mode de tunnelage bidirectionnel. Les améliorations ou les conventions d'allocation dynamique des agents de rattachement local sortent du domaine d'application de la présente spécification.

5.1.2 Recherche DNS par nom de service

La [RFC2782] définit l'enregistrement de ressource de service (RR SRV, S*ervice Resource Record*) qui permet à un opérateur d'utiliser plusieurs serveurs pour un seul domaine, pour déplacer des services d'hôte à hôte, et pour désigner certains hôtes comme serveur principal pour un service et d'autres comme sauvegarde. Les clients demandent un service/protocole spécifique pour un domaine spécifique et obtiennent en retour les noms de tous les serveurs disponibles.

La [RFC2782] décrit aussi les politiques pour choisir un agent de service sur la base de la préférence et de valeurs de pondération. Le RR SRV du DNS peut contenir les valeurs de préférence et de pondération pour plusieurs agents de rattachement disponibles au nœud mobile en plus des FQDN de l'agent de rattachement. Si plusieurs agents de rattachement sont disponibles dans le RR SRV du DNS, le nœud mobile est alors responsable du traitement des informations selon la politique et de choisir un agent de rattachement. Si l'agent de rattachement choisi ne répond pas aux messages IKE_SA_INIT ou si l'authentification IKEv2 échoue, le nœud mobile DEVRAIT essayer l'agent de rattachement suivant de la liste. Si aucun des agents de rattachement ne répond, le nœud mobile DEVRAIT essayer encore après une période configurable sur le nœud mobile. Si l'authentification IKEv2 échoue avec tous les agents de rattachement, il y a une erreur irrécupérable sur le nœud mobile.

Le nom de service pour le service d'agent de rattachement IPv6 mobile, comme exigé par la RFC 2782, est "mip6" et le nom de protocole est "ipv6". Noter qu'un nom de transport ne peut pas être utilisé ici parce que IPv6 mobile ne fonctionne pas sur un protocole de transport.

Le RR SRV a un code de type DNS de 33. Par exemple, le mobile construit une demande avec le QNAME réglé à "_mip6._ipv6.exemple.com" et le QTYPE à SRV. La réponse contient les FQDN d'un ou plusieurs serveurs qui peuvent alors se résoudre en une transaction DNS séparée aux adresses IP. Cependant, si il y a de la place dans la réponse SRV, il est RECOMMANDÉ que le serveur DNS retourne aussi les adresses IP des agents de rattachement dans les enregistrements AAAA au titre de la section des données supplémentaires (afin d'éviter d'exiger un aller-retour DNS supplémentaire pour résoudre les FQDN).

5.2 Établissement d'associations de sécurité IPsec

Aussitôt que le nœud mobile a découvert l'adresse de l'agent de rattachement, il établit une association de sécurité IPsec avec l'agent de rattachement lui-même avec IKEv2. La description détaillée de cette procédure est donnée dans la [RFC4877]. Si le nœud mobile veut que le HA enregistre l'adresse de rattachement dans le DNS, il DOIT utiliser le FQDN comme identité d'initiateur dans l'étape IKE_AUTH de l'échange IKEv2 (IDi). Ceci est nécessaire parce que le nœud mobile doit prouver qu'il est le propriétaire du FQDN fourni dans la mise à jour d'option DNS suivante. Voir les Sections 6 et 9 pour une analyse plus détaillée de ce problème.

L'authentification du nœud mobile IKEv2 auprès de l'agent de rattachement peut être effectuée en utilisant des signatures de clé publique IKEv2 ou le protocole d'authentification extensible (EAP, *Extensible Authentication Protocol*). Les détails de la façon dont utiliser l'authentification IKEv2 sont décrits dans les [RFC4877] et [RFC4306]. Le choix d'une méthode d'authentification d'homologue IKEv2 dépend du déploiement. Le nœud mobile devrait être configuré avec les informations sur la méthode d'authentification IKEv2 à utiliser. Cependant, IKEv2 restreint l'authentification de l'agent de rattachement au nœud mobile à utiliser l'authentification fondée sur la signature de clé publique.

5.3 Allocation d'adresse de rattachement

L'allocation d'adresse de rattachement est effectuée durant l'échange IKEv2. L'adresse de rattachement peut être allouée directement par l'agent de rattachement ou elle peut être autoconfigurée par le nœud mobile.

5.3.1 Allocation d'adresse de rattachement par l'agent de rattachement

Quand le nœud mobile utilise IKEv2 avec son agent de rattachement, il peut demander une HoA par la charge utile de configuration dans l'échange IKE_AUTH en incluant un attribut INTERNAL_IP6_ADDRESS. Quand l'agent de

rattachement traite le message, il alloue une HoA et lui envoie un message CFG_REPLY. L'agent de rattachement pourrait consulter un serveur DHCP sur la liaison de rattachement pour avoir l'allocation réelle d'adresse de rattachement. Ceci est expliqué en détails dans la [RFC4877].

5.3.2 Auto configuration d'adresse de rattachement par l'agent mobile

Avec le type d'allocation décrit au paragraphe précédent, l'adresse de rattachement ne peut pas être générée sur la base d'adresses générées cryptographiquement (CGA, *Cryptographically Generated Address*) [RFC3972] ou sur la base des extensions de confidentialité pour l'autoconfiguration sans état [RFC4941]. Cependant, le nœud mobile pourrait vouloir avoir une HoA autoconfigurée sur la base de ces mécanismes. Il vaut de mentionner que la procédure d'auto-configuration décrite dans ce paragraphe ne peut pas être utilisée dans certains déploiements possibles, car les agents de rattachement pourraient être provisionnés avec des réservoirs d'adresses de rattachement permises.

Dans le cas le plus simple, le nœud mobile est muni d'un préfixe de rattachement pré-configuré et de la longueur du préfixe de rattachement. Dans ce cas, le nœud mobile crée une adresse de rattachement sur la base du préfixe pré-configuré et l'envoie à l'agent de rattachement, en incluant un attribut INTERNAL_IP6_ADDRESS dans une charge utile de configuration de type CFG_REQUEST. Si l'adresse de rattachement est valide, l'agent de rattachement répond avec une CFG_REPLY, incluant un attribut INTERNAL_IP6_ADDRESS avec la même adresse. Si l'adresse de rattachement fournie par le nœud mobile n'est pas valide, l'agent de rattachement alloue une adresse de rattachement différente incluant un attribut INTERNAL_IP6_ADDRESS avec une nouvelle valeur. Selon la [RFC4306], le nœud mobile DOIT utiliser l'adresse envoyée par l'agent de rattachement. Plus tard, si le nœud mobile veut utiliser une adresse de rattachement auto-configurée (par exemple, fondée sur une CGA) il peut faire une découverte de préfixe mobile, obtenir un préfixe, auto-configurer une nouvelle adresse de rattachement, et ensuite effectuer un nouvel échange CREATE_CHILD_SA.

Si le nœud mobile n'est pas muni d'un préfixe de rattachement pré-configuré, le mobile ne peut pas simplement proposer une HoA auto-configurée dans la charge utile de configuration car le nœud mobile ne connaît pas le préfixe de rattachement avant le début de l'échange IKEv2. Le nœud mobile doit obtenir le préfixe de rattachement et la longueur de préfixe de rattachement avant de pouvoir configurer une adresse de rattachement.

Une solution simple serait que le nœud mobile suppose juste que la longueur de préfixe sur la liaison de rattachement est de 64 bits et qu'il extraie le préfixe de rattachement de l'adresse de l'agent de rattachement. L'inconvénient de cette solution est que le préfixe de rattachement ne peut pas être autre chose que /64. De plus, cela lie le préfixe sur la liaison de rattachement et l'adresse de l'agent de rattachement, mais, en général, un agent de rattachement avec une adresse particulière devrait être capable de servir un certain nombre de préfixes sur la liaison de rattachement, pas juste le préfixe à partir duquel son adresse est configurée.

Une autre solution serait que le nœud mobile suppose que la longueur de préfixe sur la liaison de rattachement est de 64 bits et qu'il envoie son identifiant d'interface à l'agent de rattachement dans l'attribut INTERNAL_IP6_ADDRESS au sein de la charge utile CFG_REQ. Bien que cette approche ne lie pas le préfixe sur la liaison de rattachement et l'adresse de l'agent de rattachement, elle exige quand même que la longueur de préfixe de rattachement soit de 64 bits.

Pour cette raison, le nœud mobile a besoin d'obtenir les préfixes de liaison de rattachement par l'échange IKEv2. Dans la charge utile de configuration durant l'échange IKE_AUTH, le nœud mobile inclut l'attribut MIP6_HOME_PREFIX dans le message CFG_REQUEST. L'agent de rattachement, quand il traite ce message, DOIT inclure dans la charge utile CFG_REPLY les informations de préfixe pour un préfixe sur la liaison de rattachement. Ces informations de préfixe incluent la longueur de préfixe (voir au paragraphe 8.2). Le nœud mobile auto-configure une adresse de rattachement à partir du préfixe retourné dans le message CFG_REPLY et conduit un échange CREATE_CHILD_SA pour créer les associations de sécurité pour la nouvelle adresse de rattachement.

Comme mentionné précédemment dans le présent document, il y a des déploiements où l'auto-configuration de l'adresse de rattachement ne peut pas être utilisée. Dans ce cas, quand l'agent de rattachement reçoit une CFG_REQUEST qui inclut un attribut MIP6_HOME_PREFIX dans la réponse IKE qui suit, il inclut un type de charge utile Notify "USE_ASSIGNED_HoA" et l'adresse de rattachement qui s'y rapporte dans un attribut INTERNAL_IP6_ADDRESS. Si le nœud mobile obtient une charge utile Notify "USE_ASSIGNED_HoA" en réponse à la charge utile de configuration contenant l'attribut MIP6_HOME_PREFIX, il cherche un attribut INTERNAL_IP6_ADDRESS et DOIT utiliser l'adresse qu'il contient dans l'échange CREATE_CHILD_SA qui suit.

Quand l'agent de rattachement reçoit une mise à jour de lien pour le nœud mobile, il effectue une DAD de mandataire pour l'adresse de rattachement auto-configurée. Si la DAD échoue, l'agent de rattachement rejette la mise à jour de lien. Si le nœud mobile reçoit un accusé de réception de lien avec le code d'état 134 (échec de DAD) il DOIT arrêter d'utiliser

l'adresse de rattachement courante, configurer une nouvelle HoA, et ensuite effectuer un échange IKEv2 CREATE_CHILD_SA pour créer les associations de sécurité sur la base de la nouvelle HoA. Le nœud mobile n'a pas besoin de faire à nouveau les échanges IKE_INIT et IKE_AUTH. Une fois que les associations de sécurité nécessaires sont créées, le nœud mobile envoie une mise à jour de lien pour la nouvelle adresse de rattachement.

Il vaut de noter qu'avec ce mécanisme, les informations de préfixe portées dans l'attribut MIP6_HOME_PREFIX incluent seulement un préfixe et ne portent pas toutes les informations qui sont normalement présentes quand elles sont reçues par une annonce de routeur IPv6. La découverte de préfixe mobile, spécifiée dans la RFC 3775, est le mécanisme par lequel le nœud mobile peut obtenir tous les préfixes sur la liaison de rattachement et toutes les informations qui s'y rapportent. Cela signifie que l'attribut MIP6_HOME_PREFIX n'est utilisé que pour l'auto-configuration d'adresse de rattachement et ne remplace pas l'usage de la découverte de préfixe mobile pour les besoins détaillés dans la RFC 3775.

5.4 Autorisation et authentification avec MSA

Dans un scénario où l'agent de rattachement est découvert de façon dynamique par le nœud mobile, il est très probable que l'agent de rattachement ne soit pas capable de vérifier par lui-même les accréditifs fournis par le nœud mobile durant l'échange IKEv2. De plus, le service de mobilité a besoin d'être explicitement autorisé sur la base du profil de l'utilisateur. Par exemple, l'agent de rattachement pourrait ne pas savoir si le service de mobilité peut être accordé à un moment particulier de la journée ou quand le crédit du nœud mobile est sur le point d'expirer.

Pour toutes ces raisons, l'agent de rattachement peut avoir besoin de contacter la MSA afin d'authentifier le nœud mobile et autoriser le service de mobilité. Ceci peut être accompli sur la base d'une infrastructure de clé publique si des certificats sont utilisés et si une PKI est déployée par le MSP et la MSA. Par ailleurs, si le nœud mobile est muni d'autres types d'accréditifs, l'infrastructure AAA doit être utilisée.

La définition de cette communication d'extrémité sort du domaine d'application du présent document. Dans la [RFC5637], une liste de objectifs d'une telle communication est fournie. [17] et la [RFC5778] définissent respectivement les extensions RADIUS et Diameter pour la communication d'extrémité.

6. Enregistrement de l'adresse de rattachement dans le DNS

Pour que le nœud mobile soit accessible par son adresse de rattachement allouée dynamiquement, le DNS doit être mis à jour avec la nouvelle adresse de rattachement. Comme les applications utilisent des recherches dans le DNS sur le FQDN pour trouver un nœud, la mise à jour du DNS est essentielle pour fournir l'accessibilité IP au nœud mobile, ce qui est le principal objet du protocole IPv6 mobile. Le besoin de mise à jour du DNS n'est pas discuté dans la RFC 3775 car elle suppose que le nœud mobile est provisionné avec une adresse de rattachement statique. Cependant, quand une adresse de rattachement dynamique est allouée au nœud mobile, toute entrée du DNS existante devient invalide et le nœud mobile devient injoignable tant qu'une mise à jour du DNS n'est pas effectuée.

Comme la mise à jour du DNS doit être effectuée de façon sécurisée afin d'empêcher des attaques ou modifications provenant de nœuds malveillants, le nœud qui effectue cette mise à jour doit partager une association de sécurité avec le serveur DNS. Avoir tous les nœuds mobiles possibles qui partagent une association de sécurité avec les serveurs DNS du MSP pourrait être embarrassant d'un point de vue administratif. De plus, même si un nœud mobile a une association de sécurité avec un serveur DNS de son MSP, un problème d'autorisation d'adresse vient assombrir le tableau. Une analyse détaillée des menaces possibles contre la mise à jour du DNS est fournie au paragraphe 9.5.

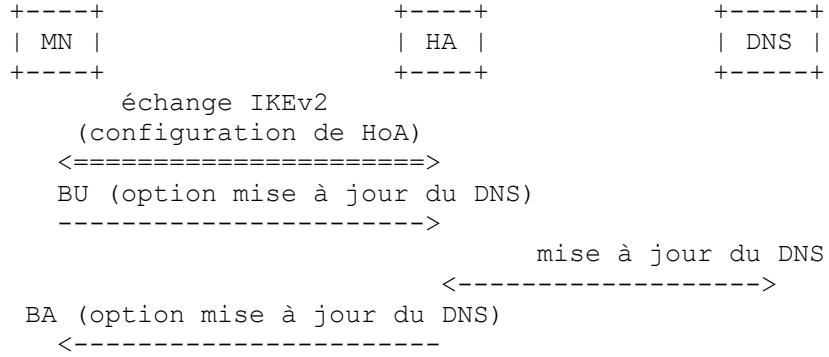
Donc, pour des raisons administrative et de sécurité, il est RECOMMANDÉ que l'agent de rattachement effectue les mises à jour d'entrée du DNS pour le nœud mobile. À cette fin, le nœud mobile PEUT inclure une nouvelle option de mobilité dans la mise à jour de lien, dans l'option de mise à jour du DNS, avec le fanion R réglé à zéro dans l'option. Cette option est définie à la Section 8 et inclut le FQDN qui doit être mis à jour. Après la réception de la mise à jour de lien, l'agent de rattachement DOIT mettre à jour l'entrée du DNS avec l'identifiant fourni par le nœud mobile et l'adresse de rattachement incluse dans l'option Adresse de rattachement. La procédure pour l'envoi d'un message de mise à jour dynamique du DNS est spécifiée dans la [RFC2136]. La mise à jour dynamique du DNS DEVRAIT être effectuée de façon sûre ; pour cette raison, l'usage de TKEY et TSEC ou DNSSEC est recommandé (voir les détails au paragraphe 9.5). Aussitôt que l'agent de rattachement a mis à jour le DNS, il DOIT envoyer un message Accusé de réception de lien au nœud mobile, incluant l'option de mobilité de mise à jour du DNS avec la valeur correcte dans le champ Status (voir le paragraphe 8.1). Cette procédure peut être effectuée directement par l'agent de rattachement si l'agent de rattachement a une association de sécurité avec le domaine spécifié dans le FQDN du nœud mobile.

Par ailleurs, si le nœud mobile veut être accessible par un FQDN qui appartient à la MSA, l'agent de rattachement et le serveur DNS qui doivent être mis à jour appartiennent à des domaines administratifs differents. Dans ce cas, l'agent de rattachement ne peut pas partager une association de sécurité avec le serveur DNS et la mise à jour d'entrée du DNS peut être effectuée par le serveur AAA de la MSA. Pour faire cela, l'agent de rattachement envoie au serveur AAA la paire FQDN-HoA par le protocole AAA. Ce message est relayé par l'infrastructure AAA du MSP et est reçu par le serveur AAA de la MSA. Le serveur AAA de la MSA effectue la mise à jour du DNS sur la base de la [RFC2136]. Noter que même dans ce cas, l'agent de rattachement est toujours obligé d'effectuer une mise à jour du DNS pour l'entrée inverse, car ceci est toujours effectué dans le serveur DNS du MSP. La description détaillée de la communication entre agent de rattachement et AAA sort du domaine d'application du présent document. Les détails sont fournis dans la [RFC5637].

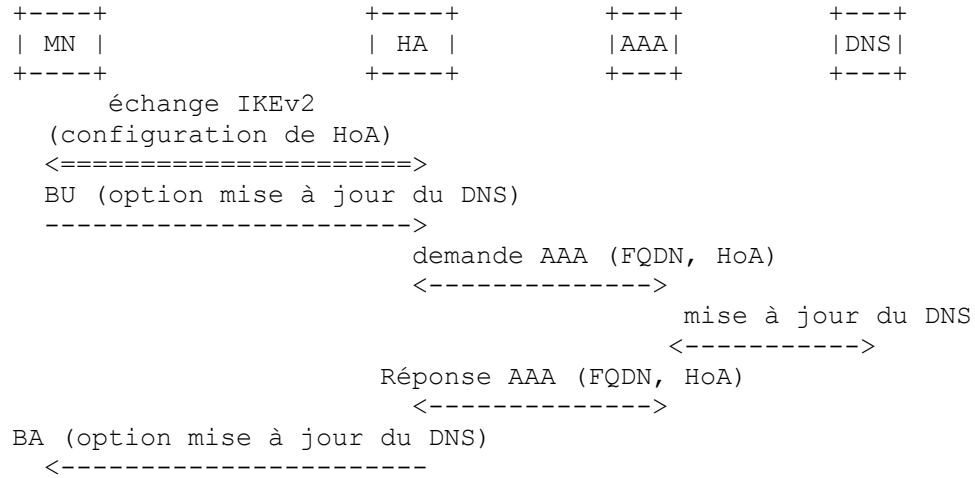
Un mécanisme pour supprimer les entrées périmées du DNS est nécessaire. Une entrée du DNS devient périmée quand l'adresse de rattachement qui s'y rapporte n'est plus utilisée par le nœud mobile. Pour supprimer une entrée du DNS, le nœud mobile inclut dans la mise à jour de lien l'option de mobilité de mise à jour du DNS, avec le fanion R établi dans l'option. Après la réception de la mise à jour de lien, l'agent de rattachement DOIT supprimer l'entrée du DNS identifiée par le FQDN fourni par le nœud mobile et l'adresse de rattachement incluse dans l'option Adresse de rattachement. La procédure d'envoi d'un message de mise à jour dynamique du DNS est spécifiée dans la [RFC2136]. Comme mentionné ci-dessus, la mise à jour dynamique du DNS DEVRAIT être effectuée de façon sûre ; pour cette raison, l'usage de TKEY et TSEC ou DNSSEC est recommandé (voir les détails au paragraphe 9.5). Si il n'y a pas de mise à jour de lien (BU, *Binding Update*) de désenregistrement explicite de la part du nœud mobile, le HA PEUT alors utiliser l'expiration de l'entrée d'antémémoire de lien comme déclencheur pour supprimer l'entrée du DNS.

7. Résumé du flux de protocole d'amorçage

Le flux de messages de la procédure d'amorçage entière quand la mise à jour dynamique du DNS est effectuée par l'agent de rattachement est décrit ci-dessous :



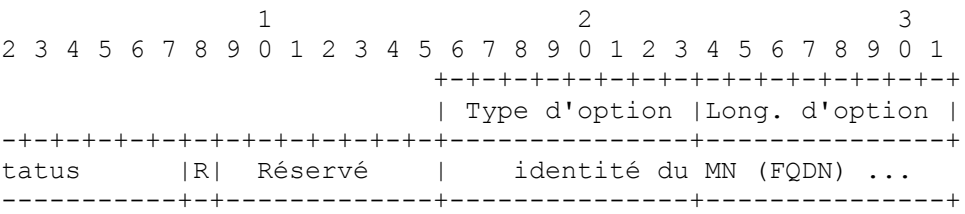
Au contraire, la figure ci-dessous montre le flux de messages de la procédure d'amorçage entière quand la mise à jour dynamique du DNS est effectuée par le serveur AAA de la MSA.



On remarque que même dans ce dernier cas, l'agent de rattachement est toujours obligé d'effectuer une mise à jour du DNS pour l'entrée inverse, car ceci est toujours effectué dans le serveur DNS du MSP. Ceci n'est pas décrit dans la figure.

8. Format d'option et d'attribut

8.1 Option Mobilité de mise à jour du DNS



Type d'option : DNS-UPDATE-TYPE (17)

Longueur d'option : entier non signé de 8 bits indiquant la longueur de l'option en excluant les champs Type et Longueur.

Status : entier non signé de 8 bits indiquant le résultat de la procédure de mise à jour dynamique du DNS. Ce champ DOIT être réglé à 0 et ignoré par le receveur quand l'option Mobilité de mise à jour du DNS est incluse dans un message de mise à jour de lien. Quand l'option Mobilité de mise à jour du DNS est incluse dans le message Accusé de réception de lien, les valeurs dans le champ Status de moins de 128 indiquent que la mise à jour dynamique du DNS a été effectuée avec succès par l'agent de rattachement. Les valeurs supérieures ou égales à 128 indiquent que la mise à jour dynamique du DNS n'a pas été achevée par le HA. Les valeurs suivantes de Status sont actuellement définies :

0 mise à jour du DNS effectuée
128 raison non spécifiée
129 administrativement interdit
130 échec de mise à jour du DNS

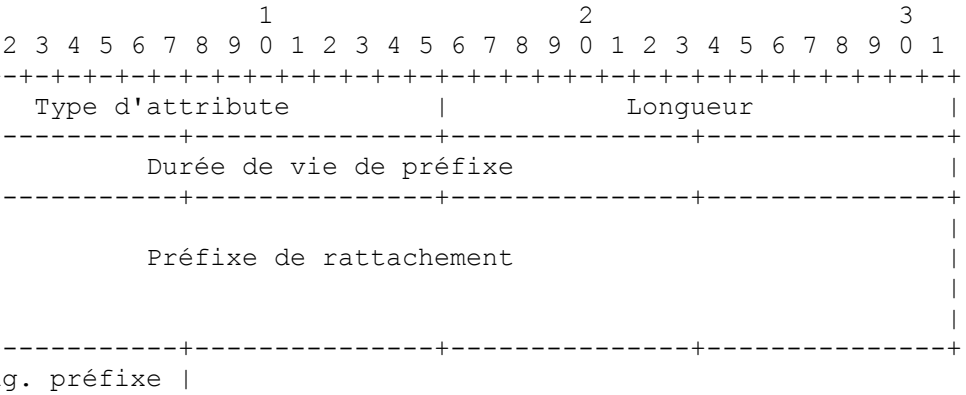
Fanion R : Si il est établi, le nœud mobile demande au HA de supprimer l'entrée du DNS identifiée par le FQDN spécifié dans cette option et la HoA du nœud mobile. Si il est à zéro, le nœud mobile demande au HA de créer ou mettre à jour une entrée du DNS avec sa HoA et le FQDN spécifiés dans l'option.

Réservé : DOIT être réglé à 0.

Identité de MN : identité du nœud mobile en format FQDN à utiliser par l'agent de rattachement pour envoyer une mise à jour dynamique du DNS. C'est un champ de longueur variable.

8.2 Attribut MIP6_HOME_PREFIX

L'attribut MIP6_HOME_PREFIX est porté dans les messages IKEv2 de configuration de charge utile. Cet attribut est utilisé pour porter le préfixe de rattachement à partir duquel le nœud mobile autoconfigure son adresse de rattachement.



Réservé (1 bit) : ce bit DOIT être réglé à zéro et DOIT être ignoré à réception.

Type d'attribut (15 bits) : identifiant unique pour l'attribut MIP6_HOME_PREFIX (16).

Longueur (2 octets) : longueur en octets du champ Valeur (préfixe de rattachement, Durée de vie de préfixe et Longueur de préfixe). Ce peut être 0 ou 21.

Durée de vie de préfixe (4 octets) : la durée de vie du préfixe de rattachement.

Préfixe de rattachement (16 octets) : préfixe de la liaison de rattachement à travers laquelle le nœud mobile peut auto-configurer son adresse de rattachement.

Longueur de préfixe (1 octet) : longueur en bits du préfixe de rattachement spécifié dans le champ Préfixe de rattachement.

Quand l'attribut MIP6_HOME_PREFIX est inclus par le nœud mobile dans la charge utile CFG_REQUEST, la valeur du champ Longueur est 0. Quand l'attribut MIP6_HOME_PREFIX est inclus dans la charge utile CFG_REPLY par l'agent de rattachement, la valeur du champ Longueur est 21 et l'attribut contient aussi les informations de préfixe de rattachement.

9. Considérations sur la sécurité

9.1 Découverte d'adresse de HA

L'utilisation du DNS pour la découverte d'adresse comporte certains risques pour la sécurité. Les transactions du DNS dans l'Internet sont normalement faites sans aucune authentification du serveur DNS par le client ou du client par le serveur. Deux risques sont encourus :

1. Un client légitime obtient une adresse boguée d'agent de rattachement d'un serveur DNS bogué. Ceci est parfois appelé une attaque de "dévoiement" *(pharming)*.

2. Un client attaquant obtient une adresse légitime d'agent de rattachement d'un serveur légitime.

Le risque dans le cas 1 est atténué parce que le nœud mobile est obligé d'effectuer une transaction IKE avec l'agent de rattachement avant d'effectuer une mise à jour de lien pour établir le service IPv6 mobile. Selon la spécification IKEv2 [RFC4306], celui qui répond doit présenter à l'initiateur un certificat valide contenant la clé publique de celui qui répond, et celui qui répond au message IKE_AUTH de l'initiateur doit être protégé par un authentifiant calculé en utilisant la clé publique dans le certificat. Donc, un attaquant devrait établir à la fois un serveur DNS bogué et un agent de rattachement bogué, et provisionner l'agent de rattachement avec un certificat qu'un nœud mobile victime pourrait vérifier. Si le nœud mobile peut détecter que le certificat n'est pas de confiance, l'attaque va être déjouée quand le nœud mobile tentera d'établir la SA IKE.

Le risque dans le cas 2 est limité pour une seule transaction de nœud mobile à agent de rattachement si l'attaquant ne possède pas les accréditifs appropriés pour s'authentifier auprès de l'agent de rattachement. L'établissement de SA IKE va échouer quand le nœud mobile attaquant va tenter de s'authentifier auprès de l'agent de rattachement. Sans considération de si l'agent de rattachement utilise EAP ou des certificats côté hôte pour authentifier le nœud mobile, l'authentification va échouer sauf si le nœud mobile a des accréditifs valides.

Un autre risque existe dans le cas 2 parce que l'attaquant peut tenter de propager une attaque de déni de service (DoS) sur l'agent de rattachement. Dans ce cas, l'attaquant obtient l'adresse de l'agent de rattachement auprès du DNS, puis propage l'adresse à un réseau d'hôtes attaquants qui bombardent l'agent de rattachement avec du trafic. Cette attaque n'est pas particulière à la solution d'amorçage, cependant, il y a actuellement un risque que toute installation d'agent de rattachement IPv6 mobile rencontre. En fait, le risque est encouru par tout service de l'Internet qui distribue une adresse d'envoi individuel d'acheminement mondial à des clients. Comme IPv6 mobile exige que le nœud mobile communique par une adresse d'envoi individuel d'acheminement mondial d'un agent de rattachement, il est possible que l'adresse d'agent de rattachement puisse être propagée à un attaquant par divers moyens (vol du nœud mobile, malgiciel installé sur le nœud mobile, mauvaises intentions du possesseur du nœud mobile lui-même, etc.) même si l'adresse de rattachement est configurée manuellement sur le nœud mobile. Par conséquent, chaque installation d'agent de rattachement IPv6 mobile va probablement être obligée de monter des mesures anti DoS. Ces mesures incluent de surprovisionner les liaisons de et vers les agents de rattachement et les capacités de traitement des agents de rattachement, une surveillance vigilante du trafic sur les réseaux d'agent de rattachement pour détecter quand le volume de trafic augmente de façon anormale, indiquant une

possible attaque de DoS, et des disques de secours *(hot spares)* qui peuvent être rapidement commutés en cas d'attaque montée contre une collection d'agents de rattachement en fonctionnement. Les attaques de DoS d'intensité modérée devraient être déjouées durant la transaction IKEv2. Les mise en œuvres de IKEv2 sont supposées générer leurs mouchards sans aucun état sauvegardé, et temporiser les paramètres de génération de mouchards fréquemment, avec la valeur de fin de temporisation qui augmente si une attaque de DoS est suspectée. Ceci devrait empêcher les attaques en épuisement d'état, et devrait assurer la continuation du service aux clients légitimes jusqu'à ce que les limites pratiques de la bande passante du réseau et la capacité de traitement du réseau de l'agent de rattachement soient atteintes.

Des mesures de sécurité explicites entre le serveur DNS et l'hôte, comme la DNSSEC [RFC4033] ou TSIG/TKEY [RFC2845], [RFC2930], peuvent atténuer le risque de 1) et 2), mais ces mesures de sécurité ne sont pas largement déployées sur les nœuds d'extrémité. Ces mesures de sécurité ne sont cependant pas suffisantes pour protéger l'adresse d'agent de rattachement contre l'attaque de DoS, parce que un nœud qui a une association de sécurité légitime avec le serveur DNS pourrait néanmoins intentionellement ou par inadvertance causer que l'adresse d'agent de rattachement devienne la cible d'une attaque de DoS.

Finalement, on remarquera que l'allocation d'un agent de rattachement provenant du fournisseur d'accès réseau desservant (agent de rattachement local) ou d'un agent de rattachement provenant d'un réseau du voisinage (agent de rattachement du voisinage) peut établir un potentiel de compromission de la confidentialité de la localisation d'un nœud mobile. Une adresse de rattachement ancrée sur un tel agent de rattachement contient des informations sur la localisation topologique du nœud mobile. Par conséquent, un nœud mobile qui exige la confidentialité de sa localisation ne devrait pas divulguer son adresse de rattachement aux nœuds qui ne sont pas autorisés à apprendre la localisation du nœud mobile, par exemple, en mettant à jour le DNS avec la nouvelle adresse de rattachement.

Les considérations de sécurité pour la découverte de HA en utilisant DHCP sont couvertes dans la [RFC6610].

9.2 Allocation d'adresse de rattachement avec IKEv2

L'amorçage IPv6 mobile alloue l'adresse de rattachement à travers une transaction IKEv2. Le nœud mobile peut soit choisir de demander une adresse, de façon similaire à DHCP, soit demander un préfixe sur la liaison de rattachement, puis auto configurer une adresse.

La [RFC3775] exige qu'un agent de rattachement vérifie l'autorisation d'une adresse de rattachement reçue durant une mise à jour de lien. Donc, l'agent de rattachement DOIT autoriser chaque allocation et utilisation d'adresse de rattachement. Cette autorisation est fondée sur la liaison de l'identité du nœud mobile utilisée dans le processus d'authentification IKEv2 et de l'adresse de rattachement. Les agents de rattachement DOIVENT mettre en œuvre au moins les deux modes d'autorisation suivants :

- Les adresses de rattachement configurées pour chaque nœud mobile. Dans ce mode, l'agent de rattachement ou l'infrastructure de nœuds derrière lui sait quelles adresses un nœud mobile spécifique est autorisé à utiliser. Le nœud mobile peut demander ces adresses, ou si le nœud mobile demande n'importe quelle adresse de rattachement, ces adresses lui sont retournées.

- Premier arrivé , premier servi (FCFS, *First-come-first-served*). Dans ce mode, l'agent de rattachement conserve un réservoir d'adresses "utilisées", et permet aux nœuds mobile de demandet toute adresse, pour autant qu'elle n'est pas utilisée par un autre nœud mobile.

Les adresses DOIVENT être marquées comme utilisées pour au moins aussi longtemps que le lien existe, et sont associées à l'identité du nœud mobile qui a fait l'allocation.

De plus, l'agent de rattachement DOIT s'assurer que l'adresse demandée n'est pas l'adresse autorisée d'un autre nœud mobile, c'est-à-dire, si les deux modes FCFS et configuré utilisent le même espace d'adresses.

9.3 Établissement de SA avec EAP par IKEv2

Les considérations sur la sécurité pour l'authentification de la transaction IKE utilisant EAP sont couvertes dans la [RFC4877].

9.4 Sécurité arrière entre le HA et le serveur AAA

Certains déploiement de l'amorçage IPv6 mobile peuvent utiliser un serveur AAA pour traiter l'autorisation du service de mobilité. Ce processus a ses propre exigences de sécurité, mais le protocole d'extrémité pour un agent de rattachement à une interface de serveur AAA n'est pas couvert dans le présent document. Voir dans la [RFC5637] une discussion de cette interface.

9.5. Mise à jour dynamique du DNS

Si un agent de rattachement effectue une mise à jour dynamique du DNS au nom du nœud mobile directement avec le serveur DNS, l'agent de rattachement DOIT avoir une association de sécurité du même type avec le serveur DNS. L'association de sécurité PEUT être établie en utilisant DNSSEC [RFC4033] ou TSIG/TKEY [RFC2845], [RFC2930]. Une association de sécurité est EXIGÉE même si le serveur DNS est dans le même domaine administratif que l'agent de rattachement. L'association de sécurité DEVRAIT être séparée des associations de sécurité utilisées pour d'autres objets, tels que AAA.

Dans le cas où le fournisseur du service de mobilité est différent de l'autorité de service de mobilité, les administrateurs de réseau peuvent vouloir limiter le nombre d'associations de sécurité franchissant des limites de domaine administratif. Si le FQDN du nœud mobile est dans le domaine de l'autorité de service de mobilité, comme une association de sécurité pour la signalisation AAA impliquée dans l'autorisation de service de mobilité est requise dans tous les cas, l'agent de rattachement peut envoyer le FQDN du nœud mobile au serveur AAA sous l'association de sécurité AAA du serveur HA, et le serveur AAA peut effectuer la mise à jour. Dans ce cas, une association de sécurité est requise entre le serveur AAA et le serveur DNS pour la mise à jour dynamique du DNS. Voir dans la [RFC5637] une discussion plus approfondie de l'interface d'agent de rattachement au serveur AAA.

Sans considérer si c'est le serveur AAA ou l'agent de rattachement qui effectue la mise à jour du DNS, l'autorisation du nœud mobile de mettre à jour un FQDN DOIT être vérifiée avant d'effectuer la mise à jour. C'est une question de mise en œuvre de déterminer comment l'autorisation est donnée. Cependant, afin de permettre cette étape d'autorisation, le nœud mobile DOIT utiliser un FQDN comme IDi dans l'étape IKE_AUTH de l'échange IKEv2. Le FQDN DOIT être le même que celui qui va être produit par le nœud mobile dans l'option de mise à jour du DNS.

En cas d'utilisation de EAP sur IKEv2 pour établir la SA IPsec, l'agent de rattachement obtient les informations d'autorisation sur le FQDN du nœud mobile via la communication AAA d'extrémité arrière effectuée durant l'échange IKEv2. Le résultat de cette étape va donner à l'agent de rattachement les informations nécessaires pour autoriser la demande du nœud mobile de mise à jour du DNS. Voir dans la [RFC5637] les détails sur la communication entre le serveur AAA et l'agent de rattachement nécessaires pour effectuer l'autorisation.

En cas d'utilisation de certificats dans IKEv2, les informations d'autorisation sur le FQDN pour la mise à jour du DNS DOIVENT être présentes dans le certificat fourni par le nœud mobile. Comme la spécification IKEv2 n'inclut pas de type de certificat exigé, il n'est pas possible de spécifier précisément comment le FQDN du nœud mobile devrait apparaître dans le certificat. Cependant, par exemple, si le type de certificat est "Certificat - Signature X.509" (un des types recommandés) alors le FQDN peut apparaître dans l'extension d'attribut subjectAltName [RFC3280].

10. Considérations relatives à l'IANA

Le présent document définit une nouvelle option de mobilité et un nouveau type d'attribut de configuration IKEv2.

Les valeurs suivantes ont été allouées :
- o d'après l'espace de noms "Option de mobilité" [RFC3775] : DNS-UPDATE-TYPE, 17 (paragraphe 8.1)
- o d'après l'espace de noms "Types d'attribut de charge utile de configuration IKEv2" [RFC4306] : attribut MIP6_HOME_PREFIX, 16 (paragraphe 8.2)
- o d'après l'espace de noms "Types d'erreur de charge utile Notify IKEv2" [RFC4306] : type d'erreur USE_ASSIGNED_HoA, 42 (paragraphe 5.3.2)

Le présent document crée un nouvel espace de noms "Codes d'état (option Mobilité de mise à jour du DNS)" pour le champ Status dans l'option Mobilité de mise à jour du DNS. Les valeurs actuelles sont décrites au paragraphe 8.1 et sont données ci-dessous :

0 mise à jour du DNS effectuée
128 raison non spécifiée

129 administrativement interdit
130 échec de la mise à jour du DNS

De futures valeurs du champ Status dans l'option Mobilité de mise à jour du DNS peuvent être allouées en utilisant une action de normalisation ou l'approbation de l'IESG.

11. Contributeurs

Cette contribution est un effort conjoint de l'équipe de conception de la solution d'amorçage du groupe de travail MIP6. Les contributeurs sont Basavaraj Patil, Alpesh Patel, Jari Arkko, James Kempf, Yoshihiro Ohba, Gopal Dommety, Alper Yegin, Junghoon Jee, Vijay Devarapalli, Kuntal Chowdury, et Julien Bournelle.

Les membres de l'équipe de conception peuvent être joint à :
Gerardo Giaretta, gerardog@qualcomm.com
Basavaraj Patil, basavaraj.patil@nokia.com
Alpesh Patel, alpesh@cisco.com
Jari Arkko, jari.arkko@kolumbus.fi
James Kempf, kempf@docomolabs-usa.com
Yoshihiro Ohba, yohba@tari.toshiba.com
Gopal Dommety, gdommety@cisco.com
Alper Yegin, alper.yegin@samsung.com
Vijay Devarapalli, vijay.devarapalli@azairenet.com
Kuntal Chowdury, kchowdury@starentnetworks.com
Junghoon Jee, jhjee@etri.re.kr
Julien Bournelle, julien.bournelle@gmail.com

12. Remerciements

Les auteurs tiennent à remercier Rafa Lopez, Francis Dupont, Jari Arkko, Kilian Weniger, Vidya Narayanan, Ryuji Wakikawa, et Michael Ye de leurs précieux commentaires.

13. Références

13.1 Références normatives

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

[RFC2136] P. Vixie, S. Thomson, Y. Rekhter et J. Bound, "Mises à jour dynamiques dans le système de noms de domaine (DNS update)", avril 1997.

[RFC2782] A. Gulbrandsen, P. Vixie et L. Esibov, "Enregistrement de ressource DNS pour la spécification de la localisation des services (DNS SRV)", février 2000.

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

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

[RFC4877] V. Devarapalli, F. Dupont, "Fonctionnement de IPv6 mobile avec IKEv2 et l'architecture IPsec révisée", avril 2007. (*MàJ* RFC3776) *(P.S.)*

13.2 Références pour information

[RFC2845] P. Vixie et autres, "Authentification de transaction de clé secrète pour DNS (TSIG)", mai 20000 (*MàJ par* RFC3645 *; remplacée par* RFC8945 *; P.S.)*

[RFC2930] D. Eastlake 3rd, "Établissement de clés secrètes pour le DNS (TKEY RR)", septembre 2000. *(P.S.)*

[RFC3280] R. Housley, W. Polk, W. Ford et D. Solo, "Profil de certificat d'infrastructure de clé publique X.509 et de liste de révocation de certificat (CRL) pour l'Internet", avril 2002. *(Obsolète, voir* RFC5280)

[RFC3646] R. Droms, éd., "Options de configuration du DNS pour le protocole de configuration dynamique d'hôte pour IPv6 (DHCPv6)", décembre 2003. *(P.S.)*

[RFC3753] J. Manner et M. Kojo, éd., "Terminologie de la mobilité", juin 2004. *(Information)*

[RFC3972] T. Aura, "Adresses générées cryptographiquement (CGA)", mars 2005. (*MàJ par* RFC4581, RFC4982) *(P.S.)*

[RFC4033] R. Arends, et autres, "Introduction et exigences pour la sécurité du DNS", mars 2005.

[RFC4210] C. Adams et autres, "Protocole de gestion de certificat (CMP) d'infrastructure de clé publique X.509 pour l'Internet", septembre 2005. (*MàJ par la* RFC6712) *(P.S.)*

[RFC4640] A. Patel et G. Giaretta, éd., "Position du problème de l'amorçage d'IPv6 mobile (MIPv6)", septembre 2006. *(Info.)*

[RFC4861] T. Narten et autres, "Découverte du voisin pour IP version 6 (IPv6)", septembre 2007. (*Remplace* RFC2461) *(D.S. ; MàJ par* RFC8028, RFC8319, RFC8425, RFC9131)

[RFC4941] T. Narten et autres, "Extensions de confidentialité pour l'auto configuration d'adresse sans état dans IPv6", septembre 2007. (*D.S. ; remplace* RFC3041 ; r*emplacée par* RFC8981*)*

[RFC4945] B. Korver, "Profil Internet de PKI de sécurité IP de IKEv1/ISAKMP, IKEv2, et PKIX", août 2007. *(P.S.)*

[RFC5637] G. Giaretta, I. Guardini, E. Demaria, J. Bournelle, R. Lopez, "Objectifs d'authentification, d'autorisation et de comptabilité (AAA) pour IPv6 Mobile" septembre 2009. *(Information)*

[RFC5778] J. Korhonen, H. Tschofenig, J. Bournelle, G. Giaretta, M. Nakhjiri, "Diameter sur IPv6 mobile : prise en charge de l'interaction du serveur Diameter avec l'agent de rattachement", février 2010. *(P. S.)*

[RFC6610] H. Jang et autres, "Options DHCP pour la découverte des informations de rattachement dans IPv6 mobile (MIPv6)", mai 2012. *(P.S.)*

[RFC6611] K. Chowdhury, A. Yegin, "Amorçage de IPv6 mobile (MIPv6) pour le scénario intégré", mai 2012. *(P.S.)*

[17] Chowdhury, K., "Prise en charge de IPv6 mobile par RADIUS", Travail en cours, mars 2007.

Adresse des auteurs

James Kempf
DoCoMo Labs USA
181 Metro Drive
San Jose, CA 95110
USA
mél : kempf@docomolabs-usa.com

Gerardo Giaretta
Qualcomm
mél : gerardog@qualcomm.com

Vijay Devarapalli
Azaire Networks
3121 Jay Street
Santa Clara, CA 95054
USA
mél : vijay.devarapalli@azairenet.com

Déclaration complète de droits de reproduction

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur le répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf-ipr@ietf.org.

Remerciement

Le financement de la fonction d'édition des RFC est fourni par l'activité de soutien administratif de l'IETF (IASA).