

Groupe de travail Réseau  
**Request for Comments : 3543**  
 Catégorie : En cours de normalisation  
 Traduction Claude Brière de L'Isle

S. Glass, Sun Microsystems  
 M. Chandra, Cisco Systems  
 août 2003

## Révocation d'enregistrement dans IPv4 mobile

### Statut de ce mémoire

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

### Notice de copyright

Copyright (C) The Internet Society (2003). Tous droits réservés

### Résumé

Le présent document définit un mécanisme de révocation d'enregistrements IPv4 mobile par lequel un agent de mobilité impliqué dans la fourniture de services IP mobile à un nœud mobile peut notifier aux autres agents de mobilité fournissant des services IP mobile au même nœud mobile que son enregistrement est terminé. Le mécanisme est aussi utilisable par un agent de rattachement pour notifier à un nœud mobile colocalisé la terminaison de son lien. De plus, le mécanisme prévoit l'accusé de réception de cette notification. Un mécanisme de signalisation déjà défini dans le protocole IPv4 mobile est utilisé comme moyen pour informer un nœud mobile de la révocation de son lien.

## Table des Matières

1. Introduction et applicabilité.....	2
2. Terminologie.....	2
3. Extensions et messages de révocation d'enregistrement.....	3
3.1 Prise en charge de l'annonce de révocation d'enregistrement.....	3
3.2 Extension de prise en charge de révocation.....	4
3.3 Messages de révocation d'enregistrement.....	5
3.4 Message d'accusé de réception de révocation d'enregistrement.....	6
3.5 Protection contre la répétition.....	7
4. Vue d'ensemble de la révocation d'enregistrement.....	8
4.1 Notification du nœud mobile.....	8
4.2 Mécanisme de révocation d'enregistrement – Notification d'agent.....	9
4.3 Bits d'enregistrement IP mobile dans le processus de révocation.....	12
5. Codes d'erreur.....	13
6. Considérations sur la sécurité.....	13
6.1 Annonces d'agent.....	13
6.2 Messages de révocation.....	14
7. Considérations relatives à l'IANA.....	15
7.1 Nouveaux types de message.....	15
7.2 Nouvelles valeurs d'extension.....	15
7.3 Nouveaux codes d'erreur.....	15
8. Références.....	15
8.1 Références normatives.....	15
8.2 Références pour information.....	15
Appendice A Exemple des messages de révocation utilisés.....	16
A.1 Phase d'enregistrement.....	16
A.2 Phase de révocation.....	16
Appendice B Adresse disparate, et considérations de receveur.....	17
Remerciements.....	17
Adresses des auteurs.....	17
Déclaration complète de droits de reproduction.....	18

## 1. Introduction et applicabilité

IP mobile [RFC3344] définit l'enregistrement d'une localisation d'un nœud mobile pour fournir la connectivité entre le nœud mobile et son domaine de rattachement, facilitant la communication entre les nœuds mobiles et tout nœud correspondant. À tout moment, l'agent de rattachement ou l'agent étranger peut souhaiter cesser de desservir un nœud mobile, ou pour des raisons administratives, peut n'avoir plus besoin de desservir un nœud mobile.

Le présent document définit un mécanisme général de révocation d'enregistrement pour IPv4 mobile, par lequel un agent de mobilité peut notifier à un autre agent de mobilité (ou un nœud mobile co-localisé 'direct') la fin du lien de mobilité. Un agent de mobilité qui reçoit une notification de révocation n'a plus à fournir de services au nœud mobile dont l'enregistrement a été révoqué. Un mécanisme de signalisation déjà défini par le protocole IPv4 mobile [RFC3344] sert de moyen pour informer un nœud mobile de la révocation de son lien.

Le protocole de révocation d'enregistrement procure les avantages suivants :

1. La libération à temps des ressources de IP mobile. Les ressources qui sont consommées pour fournir les services IP mobile à un nœud mobile qui a cessé de recevoir les services IP mobile d'un agent, peuvent être réclamées par l'autre agent d'une façon plus rapide que si il devait attendre l'expiration du lien. Cela s'applique aussi au cas dans lequel un nœud mobile quitte un agent étranger pour un autre. La notification de l'agent étranger précédent lui permettra de réclamer les ressources.
2. Une comptabilité précise. Cela a un impact favorable sur la résolution des questions de comptabilité à l'égard de la longueur des liens de mobilité dans les deux domaines, car la fin réelle de l'enregistrement est relayée.
3. Une adoption plus précoce des changements de politique de domaine par rapport aux services offerts/exigés d'un lien IP mobile. Par exemple, le domaine de rattachement peut maintenant exiger des tunnels inverses [RFC3024], bien qu'il y ait des liens existants qui ne les utilisent pas. Sans un mécanisme de révocation, les nouveaux services ne peuvent être mis en place ou retirés que lorsque les liens sont réenregistrés.
4. Une notification à temps à un nœud mobile qu'il ne reçoit plus les services de mobilité, raccourcissant par là de façon significative toute période de 'trou noir' pour faciliter une récupération plus robuste.

Le protocole de révocation est un mécanisme actif, et non obstructif, qui permet une communication plus serrée entre les trois entités IP mobile dans les divers domaines administratifs. Comme de nombreux nœuds mobiles peuvent ne pas comprendre le concept de révocation, on a pris soin d'assurer la rétro compatibilité avec la [RFC3344].

Le protocole de révocation d'enregistrement ne remplace pas les méthodes décrites dans la [RFC3344] pour le désenregistrement IP mobile, car l'objet de ces mécanismes est fondamentalement différent. Les messages de désenregistrement sont utilisés par un nœud mobile pour informer son agent de rattachement qu'il est, par exemple, revenu à son sous-réseau de rattachement, tandis que les messages de révocation sont utilisés entre les agents de mobilité pour signaler la fin des liens de mobilité. Plus précisément, le message de révocation défini ici N'EST PAS à utiliser par les nœuds mobiles colocalisés 'directs' qui terminent leur enregistrement car les messages de désenregistrement sont suffisants pour cela. Un nœud mobile colocalisé 'direct' peut cependant souhaiter traiter les messages de révocation car c'est un mécanisme utile pour déclencher la renégociation des services demandés à partir du domaine de rattachement.

## 2. Terminologie

On suppose que le lecteur est familiarisé avec la terminologie utilisée dans la [RFC3344]. De plus, les termes suivants sont définis :

Nœud mobile colocalisé 'direct' : nœud mobile enregistré directement auprès de son agent de rattachement, avec le bit 'D' établi dans sa demande d'enregistrement, et qui NE s'enregistre PAS par un agent étranger.

Ressources IP mobile : divers éléments fonctionnels alloués par un agent de mobilité pour prendre en charge un lien IP mobile, par exemple, mémoire.

Services IP mobile : diverses responsabilités d'un agent de mobilité pour la prise en charge d'un nœud mobile comme défini dans la [RFC3344], par exemple, encapsulation de paquets adressés à un nœud mobile par un agent de rattachement, désencapsulation de ces paquets par un agent étranger pour livraison à un nœud mobile, etc.

Agent de mobilité : l'agent de rattachement ou l'agent étranger comme spécifié dans la [RFC3344].

Révocation : terminaison prématurée d'un lien de mobilité.

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 la [RFC2119].

### 3. Extensions et messages de révocation d'enregistrement

La révocation d'enregistrement dans IPv4 mobile est accomplie via ce qui suit :

- Annoncer la prise en charge de la révocation d'enregistrement (paragraphe 3.1) :
  - o un fanion dans l'extension Annonce d'agent a été réservé pour que les agents annoncent leur prise en charge des messages de révocation.
- Extension Prise en charge de la révocation (paragraphe 3.2) :
  - o cette extension est ajoutée à une demande d'enregistrement ou à une réponse d'enregistrement par un agent de mobilité pour indiquer qu'il prend en charge la révocation d'enregistrement.
  - o cette extension est ajoutée à une demande d'enregistrement par un nœud mobile colocalisé 'direct' pour indiquer qu'il comprend les messages de révocation.
- Message de révocation d'enregistrement (paragraphe 3.3) :
  - o message envoyé par un agent de mobilité pour informer un autre agent de mobilité, ou un nœud mobile colocalisé 'direct', qu'il a révoqué le lien d'un nœud mobile.
- Message Accusé de réception de révocation d'enregistrement (paragraphe 3.4) :
  - o message envoyé par des agents de mobilité ou des nœuds mobiles colocalisés 'directs' pour indiquer la réception d'un message de révocation.

Les considérations sur la sécurité relatives aux messages et extensions ci-dessus sont couvertes dans la Section 6.

#### 3.1 Prise en charge de l'annonce de révocation d'enregistrement

Les agents de mobilité peuvent annoncer leur prise en charge de la révocation d'enregistrement avec une modification à l'extension Annonce d'agent de mobilité décrite dans la [RFC3344]. Un bit 'X' est introduit pour indiquer la prise en charge par un agent de la révocation d'enregistrement.

```

      0          1          2          3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|           Type           |      Longueur      |   Numéro de séquence   |
+-----+-----+-----+-----+-----+-----+-----+
| Durée de vie d'enregistrement |R|B|H|F|M|G|r|T|U|X| réservés |
+-----+-----+-----+-----+-----+-----+
|           zéro, un ou plusieurs adresses d'entretien           |
|           ...           |
+-----+-----+-----+-----+-----+-----+

```

X : L'agent de mobilité prend en charge la révocation d'enregistrement

Un agent étranger qui établit le bit 'X' dans une extension d'annonce d'agent DOIT prendre en charge les messages de révocation d'enregistrement sur cette liaison, précisément l'extension Prise en charge de révocation (paragraphe 3.2.) les messages Révocation (paragraphe 3.3.) et Accusé de réception de révocation (paragraphe 3.4). Il n'est pas obligatoire que tous les agents annoncent sur la même liaison la prise en charge de la révocation d'enregistrement, ni qu'un agent annonce cette prise en charge sur toutes ses liaisons.

Noter qu'en utilisant cette information, un nœud mobile peut choisir un agent étranger qui prend en charge la révocation d'enregistrement. Si un nœud mobile ne comprend pas ce bit, il l'ignore conformément à la [RFC3344].

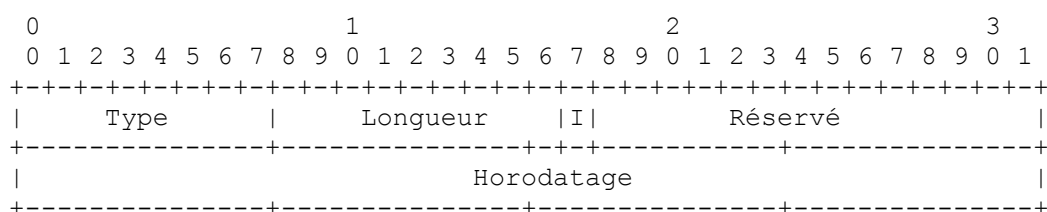
En tant que bit dans l'annonce d'agent, l'utilisation du bit 'X' n'a pas d'impact sur les autres messages, comme par exemple, mise en cause-réponse [RFC3012].

### 3.2 Extension de prise en charge de révocation

L'extension IP mobile de prise en charge de la révocation indique la prise en charge de la révocation d'enregistrement, et DOIT donc être rattachée à une demande d'enregistrement ou une réponse d'enregistrement par toute entité qui veut recevoir les messages de révocation. Normalement, c'est soit un agent étranger, soit un agent de rattachement. Cependant un nœud mobile colocalisé 'direct' PEUT aussi inclure une extension de prise en charge de la révocation dans sa demande d'enregistrement. Un nœud mobile qui n'est pas colocalisé NE DOIT PAS inclure une extension Prise en charge de la révocation dans son enregistrement.

Un agent étranger qui annonce le bit 'X' sur la liaison sur laquelle la demande d'enregistrement a été reçue, et qui a une relation de sécurité avec l'agent de rattachement identifié dans la même demande d'enregistrement, DOIT attacher une extension de prise en charge de la révocation à la demande d'enregistrement transmise. Un agent de rattachement qui reçoit une demande d'enregistrement qui ne contient pas d'extension de révocation NE DEVRAIT PAS inclure une extension de prise en charge de la révocation dans la réponse d'enregistrement associée.

Le format de l'extension de prise en charge de la révocation se fonde sur le format d'extension Type-Longueur-Valeur donné dans la [RFC3344] et est défini comme suit :



Type : 137

Longueur : Longueur (en octets, actuellement 6). Elle n'inclut PAS les champs Type et Longueur (conformément au paragraphe 1.9 de la [RFC3344]). Cela permet une plus grande longueur d'extension si plus de bits étaient nécessaires à l'avenir.

Horodatage : horodatage courant sur 4 octets de l'agent de mobilité ou du nœud mobile colocalisé 'direct'. C'est utilisé pour identifier l'ordre d'enregistrement des paquets transmis, comment ils se rapportent à l'envoi de tout message de révocation, et pour identifier le décalage approximatif entre les horloges des agents de mobilité qui prennent en charge ce lien ou entre un nœud mobile colocalisé 'direct' et son agent de rattachement.

'T' Bit : ce bit est réglé à '1' par un agent de mobilité pour indiquer qu'il prend en charge l'utilisation du bit 'T' dans les messages de révocation (paragraphe 3.3.)

Lorsque il est envoyé par un agent étranger dans une demande d'enregistrement :

si il est réglé à 1, l'agent étranger veut que l'agent de rattachement utilise le bit 'T' dans le processus de révocation pour déterminer si le nœud mobile devrait être informé ou non de la révocation ;

si il est réglé à 0, il indique à l'agent de rattachement que l'agent étranger va suivre sa propre politique à l'égard de l'information du nœud mobile en cas de révocation.

Lorsque envoyé par un agent de rattachement en réponse à une extension de révocation dans laquelle le bit 'T' était réglé à '1' :

si il est réglé à 1, l'agent de rattachement est d'accord pour utiliser le bit 'T' dans le processus de révocation pour indiquer à l'agent étranger si le nœud mobile devrait ou non être informé ;

si il est réglé à 0, l'agent de rattachement ne va pas utiliser le bit 'T' dans le processus de révocation, donnant par là à l'agent étranger le comportement par défaut par rapport à l'information du nœud mobile.

Pour préserver la robustesse du protocole, le comportement par défaut recommandé pour un agent étranger est d'informer le nœud mobile de sa révocation comme décrit au paragraphe 4.1.

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

Lorsque elle apparaît dans une demande d'enregistrement, ou une réponse d'enregistrement, l'extension IP mobile de prise en charge de la révocation DOIT être protégée soit par une extension d'authentification étrangère-de rattachement, une extension d'authentification mobile-de rattachement, ou tout autre mécanisme équivalent [RFC3344], par exemple, via AAA [RFC2977], [RFC2989], ou peut-être IPsec. Si l'extension apparaissant dans l'un de ces messages d'enregistrement n'est pas protégée, l'action appropriée décrite dans la [RFC3344] (paragraphe 3.8.2.1 et 3.7.3.1) DOIT être effectuée.

La prise en charge du bit 'T' est FACULTATIVE. Si un agent de mobilité ne prend pas en charge la fonction spécifiée, il DOIT régler le bit 'T' à zéro. Noter que l'agent de rattachement qui règle le bit 'T' à '1' en réponse à une extension de révocation

provenant de l'agent étranger dans laquelle le bit 'I' était réglé à '0' est indéfini, et NE DEVRAIT PAS être fait.

La prise en charge du bit 'I' a été négociée lorsque les deux agents ont réglé le bit 'I' à '1' dans leur extension de prise en charge de la révocation.

Il est important de noter que cette extension peut être sautée (c'est-à-dire, si l'agent de mobilité receveur ne comprend pas cette extension, il DOIT la sauter, et continuer le traitement du reste de la demande d'enregistrement).

### 3.3 Messages de révocation d'enregistrement

Un message de révocation est envoyé par un agent de mobilité pour informer un autre agent de mobilité, ou un nœud mobile colocalisé 'direct', qu'il révoque le lien d'un nœud mobile.

Champs IP :

Adresse de source : dans le cas de l'agent de rattachement qui produit la révocation d'enregistrement, c'est l'adresse enregistrée auprès de l'adresse d'entretien comme celle de l'agent de rattachement (c'est l'adresse identifiée comme adresse de rattachement de ce lien). Dans le cas de l'agent étranger qui produit la révocation d'enregistrement, c'est l'adresse enregistrée auprès de l'agent de rattachement comme adresse d'entretien.

Adresse de destination : dans le cas de l'agent de rattachement qui produit la révocation d'enregistrement, c'est l'adresse de source de la dernière demande d'enregistrement approuvée pour ce lien, c'est-à-dire, l'adresse de destination de la dernière réponse d'enregistrement indiquant le succès pour ce lien. Dans le cas de l'agent étranger qui produit la révocation d'enregistrement, c'est l'adresse enregistrée comme celle de l'agent de rattachement par le nœud mobile dont l'enregistrement est en cours de révocation.

Champs UDP :

Accès de source : variable

Accès de destination : 434

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

```

      0           1           2           3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|      Type      |  Réserve  |  A  I  |      Réserve  |
+-----+-----+-----+-----+-----+-----+
|                               Adresse de rattachement                               |
+-----+-----+-----+-----+-----+-----+
|                               Adresse du domaine de rattachement                               |
+-----+-----+-----+-----+-----+-----+
|                               Adresse de domaine étranger                               |
+-----+-----+-----+-----+-----+-----+
|                               Identifiant de révocation                               |
+-----+-----+-----+-----+-----+-----+
|  Extensions...  |
+-----+-----+
|  Authentifiant...  |
+-----+-----+

```

Type : 7

Réserve : DOIT être envoyé à 0, et ignoré à réception.

A : bit Agent (bit de 'direction').

Ce bit identifie le rôle de l'agent qui envoie la révocation, c'est à dire la 'direction' du message de révocation. Il est utile pour détecter les attaques en réflexion, particulièrement lorsque un chiffrement symétrique est utilisé.

Réglé à '0' si l'agent qui révoque sert ce lien comme agent étranger.

Réglé à '1' si l'agent qui révoque sert ce lien comme agent de rattachement.

I : bit Informe.

Ce bit NE DOIT être réglé à '1' que si la prise en charge du bit 'I' a été négociée dans les messages d'extension de révocation échangés dans le processus d'enregistrement, autrement, le résultat peut être imprévisible.

Lorsque envoyé par l'agent de rattachement à un agent étranger :

réglé à '0' pour demander que le nœud mobile NE soit PAS être informé de la révocation, ou parce que l'utilisation du bit 'I' n'a pas fait l'objet d'un accord ;

réglé à '1' pour demander que le nœud mobile soit informé de la révocation.

Lors de l'envoi d'un message de révocation à un nœud mobile colocalisé 'direct', ce bit est essentiellement non pertinent, mais DEVRAIT être réglé à '1'.

Lorsque envoyé par l'agent étranger : réglé à '0' pour indiquer que l'agent étranger utilise la politique du domaine étranger quant à la question de savoir si le nœud mobile devrait ou non être informé de la révocation, ou parce que la prise en charge du bit 'I' n'a pas fait l'objet d'un accord.

Réglé à '1' pour demander à l'agent de rattachement si le nœud mobile devrait être informé de la révocation.

Réservé : DOIT être à 0 à l'envoi, et ignoré à réception.

Adresse de rattachement : adresse IP de rattachement du nœud mobile dont l'enregistrement est révoqué.

Adresse de domaine étranger : c'est l'adresse IP pertinente dans le domaine étranger pour identifier quel lien est révoqué. C'est une des suivantes : l'adresse IP de l'agent étranger, ou l'adresse d'entretien colocalisée.

Adresse du domaine de rattachement : c'est l'adresse de l'agent de rattachement pour identifier quel lien est révoqué.

Identifiant de révocation : il protège contre les attaques en répétition. L'agent qui révoque DOIT insérer son horodatage actuel de 4 octets provenant de la même horloge que celle qu'il utilise pour remplir le champ horodatage dans son extension de révocation. Voir au paragraphe 3.5.

Un message de révocation d'enregistrement DOIT être protégé soit par un authentifiant valide comme spécifié dans la [RFC3344], à savoir un authentifiant rattachement-étranger, si la communication est entre un agent de rattachement et un agent étranger, soit un authentifiant mobile-rattachement si la communication est envoyée d'un agent de rattachement à un nœud mobile colocalisé 'direct', ou un autre mécanisme de sécurité au moins aussi sûr, et accepté par les domaines de rattachement et étranger, par exemple, IPsec. Si un agent, ou un nœud mobile colocalisé 'direct', reçoit un message de révocation d'enregistrement qui ne contient pas un authentifiant valide, et n'est pas protégé de façon adéquate, le message de révocation DOIT être ignoré, et éliminé en silence.

Un message de révocation NE DOIT PAS être envoyé pour un enregistrement qui est arrivé à expiration, et PEUT seulement être envoyé avant l'expiration de l'enregistrement du nœud mobile. Noter cependant que du fait de la nature de la livraison des datagrammes, cela ne garantit pas que ces messages vont arriver avant l'expiration naturelle d'un lien.

Un agent NE DOIT PAS envoyer plus d'un message de révocation ou d'enregistrement par seconde pour le même lien. Noter que cela met à jour la [RFC3344] en incluant les messages de révocation dans la limite de débit spécifiée dans la [RFC3344], c'est-à-dire, qu'un agent NE DOIT PAS envoyer plus d'un message d'enregistrement par seconde pour le même lien.

Un exemple d'utilisation des messages de révocation est donné à l'Appendice A.

### 3.4 Message d'accusé de réception de révocation d'enregistrement

Un message d'accusé de réception de révocation est envoyé par les agents de mobilité ou les nœuds mobiles colocalisés 'directs' pour indiquer la réception réussie d'un message de révocation.

Champs IP :

Adresse de source : copiée de l'adresse de destination du message de révocation d'enregistrement reçu pour lequel cet accusé de réception de révocation d'enregistrement est généré.

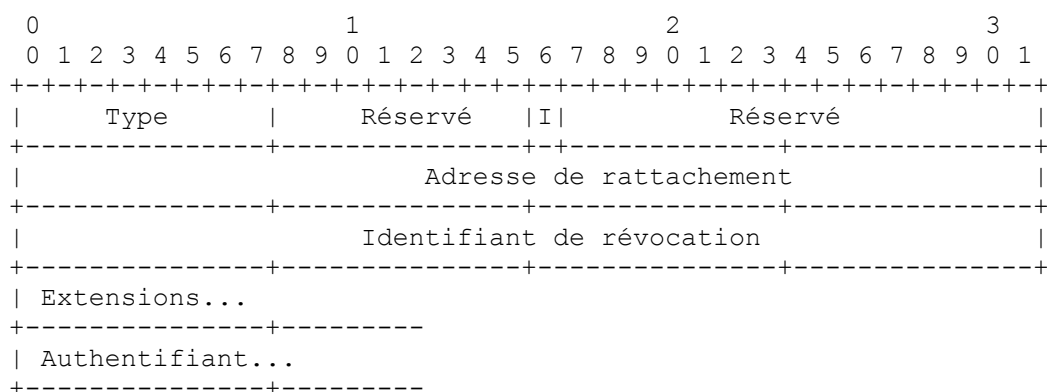
Adresse de destination : copiée de l'adresse de source du message de révocation d'enregistrement reçu pour lequel ce message d'accusé de réception de révocation d'enregistrement est généré.

Champs UDP :

Accès de source : 434 (copié de l'accès de destination du message de révocation).

Accès de destination : copié de l'accès de source du message de révocation.

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



Type : 15

Réservé : DOIT être envoyé à 0, ignoré à réception.

I : Bit Informe.

Le bit 'I' NE DOIT PAS être réglé à '1' dans les messages d'accusé de réception de révocation sauf si il était réglé à '1' dans le message de révocation. Si un agent reçoit un message d'accusé de réception de révocation dans lequel le bit 'I' est réglé à '1', mais pour lequel le message de révocation qui est acquitté avait le bit 'I' réglé à '0', le bit 'I' dans le message d'accusé de réception de révocation DOIT être ignoré.

Lorsque envoyé par l'agent de rattachement :

il est réglé à '1' par l'agent de rattachement pour demander que l'agent étranger informe le nœud mobile de la révocation.

il est réglé à '0' par l'agent de rattachement pour demander à l'agent étranger de ne pas informer le nœud mobile de la révocation.

Lorsque envoyé par un agent étranger :

il est réglé à '1' pour indiquer à l'agent de rattachement que le nœud mobile a été informé.

il est réglé à '0' pour indiquer à l'agent de rattachement que l'agent étranger a utilisé la politique locale pour déterminer si le nœud mobile devrait ou non être informé. Pour les besoins de la robustesse du protocole, il est fortement recommandé qu'une telle valeur par défaut soit fixée pour que l'agent étranger informe le nœud mobile de la révocation.

Réservé : DOIT être à 0 à l'envoi et ignoré à réception.

Adresse de rattachement : c'est l'adresse de rattachement copiée du message de révocation pour lequel cet accusé de réception est envoyé.

Identifiant de révocation : copié de l'identifiant de révocation du message de révocation pour lequel cet accusé de réception est envoyé. Voir au paragraphe 3.5.

Un message d'accusé de réception de révocation d'enregistrement DOIT être envoyé en réponse à un message de révocation d'enregistrement valide et authentifié.

Un message d'accusé de réception d'enregistrement DOIT être protégé par, soit un authentifiant valide comme spécifié dans la [RFC3344], à savoir un authentifiant rattachement-étranger si la communication est entre un agent de rattachement et un agent étranger, soit un authentifiant mobile-rattachement si la communication est entre un agent de rattachement et un nœud mobile colocalisé 'direct', ou par un autre mécanisme de sécurité au moins aussi sûr et ayant fait l'objet d'un accord entre les domaines de rattachement et étranger, par exemple, IPsec.

Un exemple de l'utilisation des messages d'accusé de réception de révocation est donnée à l'Appendice A.

### 3.5 Protection contre la répétition

Comme les messages de révocation d'enregistrement sont conçus pour terminer le service d'un nœud mobile, ou de plusieurs nœuds mobiles simultanément, la protection contre la répétition est cruciale pour empêcher les attaques de déni de service par des "répétiteurs malveillants" – qui mémorisent les datagrammes dans l'intention de les répéter ultérieurement, ou par des

"réflecteurs malveillants" – qui renvoient des paquets à leur source (qui sont toutes deux une forme "d'attaque active"). Voir à la Section 6 une discussion de ces considérations de sécurité.

Tous les messages de révocation et messages d'accusé de réception de révocation DOIVENT être authentifiés ainsi que protégés contre la répétition. L'ordre dans lequel cela est fait est à la discrétion de la mise en œuvre.

La protection contre la répétition est traitée par un simple mécanisme d'horodatage, en utilisant un seul champ d'identifiant de 32 bits dans le message de révocation d'enregistrement, en conjonction avec le champ d'adresse de rattachement, pour associer tout message d'accusé de réception de révocation avec son message de révocation. Pour ce faire :

- L'agent qui révoque règle le bit 'A' à son type d'agent, et le champ Identifiant de révocation dans le message de révocation d'enregistrement à un horodatage valide de 32 bits à partir de la même horloge qu'utilisée pour régler le champ Horodatage de ses extensions de révocation incluses dans les messages d'enregistrement.
- À réception d'un message de révocation authentifié, l'agent receveur (ou le nœud mobile colocalisé 'direct') DOIT vérifier la valeur du bit 'A' et l'identifiant de révocation pour s'assurer que ce message de révocation n'est pas une répétition d'un vieux message de révocation reçu du même agent. L'agent receveur DOIT aussi vérifier que le message n'est pas un reflet d'un message de révocation qu'il a envoyé en relation avec le lien identifié. Si le bit 'A' et le champ Identifiant impliquent que ce paquet est une répétition, le message de révocation DOIT être éliminé en silence.
- Lors de la construction d'un message d'accusé de réception de révocation, l'agent qui accuse réception (ou le nœud mobile colocalisé 'direct') copie les valeurs des champs Adresse de rattachement et Identifiant de révocation provenant du message de révocation dans l'adresse de rattachement et l'identifiant de révocation du message d'accusé de réception de révocation. Ceci afin que l'agent qui révoque puisse faire correspondre cet accusé de réception de révocation avec le message de révocation correspondant.
- À réception d'un accusé de réception de révocation valide, l'agent qui révoque DOIT vérifier les champs Adresse de rattachement et Identifiant pour s'assurer qu'ils correspondent aux champs du message de révocation correspondant qu'il a envoyé à l'agent qui accuse réception. Sinon, ce message d'accusé de réception de révocation DOIT être éliminé en silence.

Noter que comme l'identifiant dans un message de révocation entrant est un horodatage de 32 bits, il est possible à un agent de vérifier la validité des champs Identifiant sans avoir à se souvenir de tous les identifiants qu'il a envoyés.

Note : comme il est possible à un nœud mobile de s'enregistrer à des moments différents auprès de différents agents de rattachement, et à des moments différents auprès de différents agents étrangers, il est crucial qu'il ne soit pas exigé que les champs Identifiant soient uniques dans les messages provenant de différents agents car il n'est pas garanti que les horloges des différents agents soient synchronisées. Par exemple, si un nœud mobile a des liens simultanés avec plusieurs agents étrangers, et si des messages de révocation sont reçus par plus d'un de ces agents étrangers "simultanément", il est possible que le message de révocation provenant d'un de ces agents étrangers contienne un champ Identifiant qui se trouve correspondre à un, ou tous, de ceux des autres agents étrangers. Il NE DOIT PAS résulter de ceci qu'un de ces messages de révocation soit ignoré.

## 4. Vue d'ensemble de la révocation d'enregistrement

La révocation d'enregistrement consiste en deux opérations distinctes : un mécanisme de signalisation entre les points d'extrémité de tunnel, et un mécanisme de signalisation entre l'agent étranger et le nœud mobile. Un nœud mobile colocalisé 'direct' PEUT mettre en œuvre les extensions de révocation et d'accusé de réception de révocation afin de recevoir et de répondre aux messages de révocation provenant de son agent de rattachement, cependant, un nœud mobile colocalisé 'direct' NE DOIT PAS envoyer de message de révocation car les messages de désenregistrement définis dans la [RFC3344] sont suffisants pour le faire.

Pour un exposé plus complet sur les questions de sécurité relatives à la révocation d'enregistrement, se reporter à la Section 6.

### 4.1 Notification du nœud mobile

Un mécanisme qui fournit à un agent étranger un moyen pour notifier activement à un nœud mobile que son lien a été réinitialisé existe déjà dans la [RFC3344], bien que cela ait été un peu oublié.

Un bref survol du mécanisme de numéro de séquence dans l'annonce d'agent dans la [RFC3344] afin de bien comprendre le mécanisme par lequel l'agent étranger 'fait savoir implicitement' au nœud mobile que son lien n'est plus actif.

Lorsque un agent étranger commence à envoyer des annonces d'agent, il commence par un numéro de séquence de 0, et augmente de façon monotone le numéro de séquence à chaque annonce d'agent suivante. Pour qu'un nœud mobile soit capable de distinguer entre un agent étranger qui a simplement épuisé l'espace de numéros de séquence d'un autre qui est revenu à



zéro, lorsque l'agent incrémente le compteur de numéros de séquence au delà de sa valeur maximum, il règle le numéro de séquence à 256 au lieu de revenir à 0 [RFC3344]. De cette façon, un nœud mobile devrait manquer tout d'un coup 256 annonces pour prendre par erreur une réinitialisation pour un "retour à zéro". De plus, la durée de vie contenue dans une annonce d'agent devrait être réglée d'une façon telle que lorsque un nœud mobile pense qu'il a manqué trois balises, l'entrée pour cet agent étranger devrait arriver à expiration, et si le nœud mobile est enregistré là, il devrait envoyer une sollicitation d'agent [RFC3344]. Si, cependant, un agent est réinitialisé d'une façon ou d'une autre, il va commencer à annoncer avec un numéro de séquence de 0, et le nœud mobile peut présumer que cet agent étranger a perdu son lien, et le nœud mobile DEVRAIT se réenregistrer pour s'assurer qu'il obtient toujours les services IP mobile à travers cet agent étranger.

Pour renforcer ce mécanisme, un agent étranger peut consciemment notifier à tous les nœuds mobiles qui lui sont actuellement liés qu'il a "réinitialisé" tous leurs liens, même si l'agent lui-même n'a pas été réinitialisé, en re-réglant simplement le numéro de séquence de la prochaine annonce d'agent à 0. De plus, un agent étranger peut informer tous les nœuds mobiles actuellement liés à lui qu'ils devraient se réenregistrer auprès d'un agent étranger différent en réglant simultanément le bit 'B' à 1 dans l'annonce, ce qui indique que cet agent étranger est occupé et n'accepte pas de nouveaux enregistrements [RFC3344]. Dans ces situations, tout nœud mobile conforme à la [RFC3344] va supposer que cet agent étranger a perdu son lien, et doit se réenregistrer si il souhaite rétablir la fonctionnalité IP mobile avec son sous réseau de rattachement.

Pour indiquer à tout nœud mobile enregistré que son lien n'existe plus, l'agent étranger auprès duquel le nœud mobile est enregistré peut envoyer en envoi individuel une annonce d'agent avec le numéro de séquence réglé à 0 au nœud mobile [RFC3344], [RFC1256]. De plus, si un tel agent étranger souhaite indiquer au nœud mobile que son lien a été révoqué, et que le nœud mobile ne devrait pas tenter de renouveler son enregistrement auprès de lui, l'agent étranger PEUT aussi régler le bit 'B' à 1 dans ces annonces d'agent, pour indiquer qu'il est occupé, et n'accepte pas de nouveaux enregistrements [RFC3344]. Tous les nœuds mobiles conformes à la [RFC3344] vont comprendre que cela signifie que l'agent est occupé, et PEUVENT soit tenter immédiatement de se réenregistrer auprès d'un autre agent dans leur antémémoire d'agent étranger, soit PEUVENT solliciter des agents supplémentaires. Dans ce dernier cas, un agent étranger peut facultativement se souvenir que le lien du nœud mobile a été révoqué, et répondre à la sollicitation de la même manière, à savoir avec le bit 'B' réglé à 1. On devrait cependant noter que comme l'agent étranger ne va vraisemblablement pas régler le bit 'B' à 1 dans des annonces d'agent en diffusion (envoyées à toutes la liaison) le nœud mobile révoqué, en entendant cette annonce d'agent en diffusion groupée sans le bit 'B' établi provenant de l'agent, peut tenter de se réenregistrer auprès de lui. Si cela arrive, selon la politique du domaine étranger, l'agent étranger peut simplement refuser le nœud mobile avec un code d'erreur approprié (par exemple, "interdit administrativement"). À cet instant, un nœud mobile peut utiliser l'agent étranger de secours pour tenter de s'enregistrer auprès d'un agent étranger différent, comme décrit dans la [RFC3344].

Les nœuds mobiles qui comprennent le mécanisme de révocation décrit par ce document peuvent comprendre qu'une annonce d'agent en envoi individuel avec un numéro de séquence remis à 0 pourrait indiquer une révocation, et peuvent tenter de se réenregistrer auprès du même agent étranger, ou de s'enregistrer auprès d'un agent étranger différent, ou colocalisé.

Les annonces d'agent en envoi individuel à un nœud mobile DOIVENT être envoyées comme décrit dans la [RFC3344] en plus de toutes méthodes actuellement utilisées sur la liaison pour les rendre sûres ou authentifiables pour les protéger des attaques de déni de service.

#### **4.2 Mécanisme de révocation d'enregistrement – Notification d'agent**

Un agent étranger qui prend en charge la révocation d'enregistrement sur une liaison DOIT établir le bit 'X' dans ses extensions d'annonce d'agent qu'il envoie sur cette liaison. Cela permet aux nœuds mobiles qui requièrent des services de révocation d'enregistrement de s'enregistrer auprès de ces agents étrangers qui annoncent leur prise en charge.

##### **4.2.1 Négociation de la prise en charge de révocation**

Durant le processus d'enregistrement, si l'agent étranger souhaite participer aux messages de révocation avec le domaine de rattachement, il DOIT avoir une association de sécurité existante avec l'agent de rattachement identifié dans la demande d'enregistrement, et ajouter une extension de prise en charge de la révocation (définie au paragraphe 3.2.) avec lui. Si la réponse d'enregistrement correspondante provenant de cet agent de rattachement ne contient pas d'extension de prise en charge de la révocation, l'agent étranger DEVRAIT supposer que l'agent de rattachement ne comprend pas la révocation d'enregistrement, ou ne veut pas y participer. Si c'est inacceptable pour l'agent étranger, il PEUT refuser l'enregistrement avec par exemple, "Interdit administrativement". Noter que dans ce cas, lorsque existe une association de sécurité, comme spécifié dans la [RFC3344], la demande d'enregistrement et la réponse d'enregistrement DOIVENT toutes deux contenir quand même les authentifiants de rattachement-étranger.

Si un agent de rattachement souhaite être capable d'échanger des messages de révocation avec le domaine étranger, il DOIT avoir une association de sécurité existante avec l'agent étranger qui a relayé la demande d'enregistrement, et il DOIT ajouter

une extension de prise en charge de la révocation à la réponse d'enregistrement. Si la demande d'enregistrement provenant d'un agent étranger ne contenait pas d'extension de prise en charge de la révocation, l'agent de rattachement DEVRAIT supposer que l'agent étranger ne comprend pas la révocation d'enregistrement, ou ne veut pas y participer pour cette liaison spécifique. Si c'est inacceptable pour l'agent de rattachement, il PEUT refuser l'enregistrement avec par exemple, "Interdit administrativement". L'agent de rattachement PEUT inclure une extension de prise en charge de la révocation dans la réponse d'enregistrement.

Si un nœud mobile colocalisé 'direct' souhaite être informé de la libération d'un lien par son agent de rattachement, il DOIT insérer une extension de prise en charge de la révocation dans la demande d'enregistrement. Si c'est acceptable pour l'agent de rattachement, il DOIT inclure une extension de prise en charge de la révocation dans sa réponse d'enregistrement. Noter que si ce n'est pas acceptable, l'agent de rattachement PEUT refuser l'enregistrement, ou il PEUT simplement ne pas inclure une extension de prise en charge de la révocation dans sa réponse d'enregistrement, indiquant au nœud mobile qu'il ne va pas participer à la révocation pour ce lien. Un agent de rattachement, recevant une demande d'enregistrement provenant d'un nœud mobile colocalisé 'direct' qui ne contient pas d'extension de prise en charge de la révocation, PEUT refuser l'enregistrement avec, par exemple, "Interdit administrativement" et PEUT aussi inclure ou non une extension de prise en charge de la révocation dans la réponse d'enregistrement.

Noter qu'un nœud mobile non colocalisé NE DOIT PAS insérer une extension de prise en charge de la révocation dans sa demande d'enregistrement. Si un agent étranger reçoit une telle demande d'enregistrement, il DOIT l'éliminer en silence, et PEUT la signaler comme erreur de protocole.

Le bit 'T' dans l'extension de révocation est utilisé pour indiquer si la décision d'informer le nœud mobile de la terminaison de son lien sera ou non laissée à l'agent de rattachement. Cette fonctionnalité est offerte par l'agent étranger, et acceptée par l'agent de rattachement. Plus précisément, en envoyant une extension de révocation attachée à une demande d'enregistrement dans laquelle le bit 'T' est réglé à 1, l'agent étranger indique à l'agent de rattachement qu'il PEUT laisser la décision d'informer ce nœud mobile que son enregistrement est terminé à l'agent de rattachement. (Le terme "PEUT" est utilisé ici parce que il est reconnu que la politique du domaine peut changer pendant la durée de vie de tout enregistrement). L'agent de rattachement peut reconnaître qu'il souhaite faire ainsi en réglant le bit 'T' à 1, ou il peut indiquer qu'il ne fera pas ainsi en réglant le bit 'T' à 0, dans l'extension de révocation qui apparaît dans la réponse d'enregistrement.

La prise en charge de la révocation est considérée comme négociée pour un lien lorsque les deux côtés ont inclus une extension de prise en charge de la révocation durant un échange réussi d'enregistrement.

#### **4.2.2 Domaine de rattachement révoquant/libérant un enregistrement**

Les paragraphes qui suivent détaillent les responsabilités de chaque partie selon la fonctionnalité négociée dans l'extension de prise en charge de la révocation lorsque le domaine de rattachement révoque un enregistrement.

##### **4.2.2.1 Responsabilités de l'agent de rattachement**

Dans le cas où un agent de rattachement révoque le lien d'un nœud mobile, et où la prise en charge de la révocation a été négociée, l'agent de rattachement DOIT notifier à l'adresse de domaine étranger qu'il termine le point d'entrée de tunnel en envoyant un message de révocation. Noter que l'adresse de domaine étranger peut être l'adresse d'entretien de l'agent étranger ou l'adresse d'entretien colocalisée d'un nœud mobile colocalisé 'direct'.

Comme agent de rattachement, il DOIT régler le bit 'A' à '1', indiquant que ce paquet vient de l'agent de rattachement qui dessert ce lien.

Lorsque un message de révocation est envoyé à un agent étranger, et lorsque l'utilisation du bit 'T' a été négociée dans le processus d'enregistrement, l'agent de rattachement DOIT régler le bit 'T' à 1 si l'agent de rattachement veut que l'agent étranger informe le nœud mobile de la révocation. À l'inverse, si l'agent de rattachement ne veut pas que le nœud mobile la notifie, il DOIT régler le bit 'T' à 0. Noter que l'agent de rattachement pourrait aussi régler le bit 'T' à '0' parce qu'il sait que le nœud mobile s'est enregistré auprès d'un agent étranger différent, et qu'il n'est donc pas besoin que l'agent étranger tente une notification.

L'agent de rattachement DOIT régler le bit Identifiant comme défini au paragraphe 3.5, et DOIT inclure un authentifiant valide comme spécifié au paragraphe 3.3.

Si l'agent de rattachement ne reçoit pas de message d'accusé de réception de révocation dans un délai raisonnable, il DOIT retransmettre le message de révocation. La durée pendant laquelle l'agent de rattachement attend pour retransmettre, et le nombre de retransmissions du message sont limités par l'exigence que :

- chaque fois que l'agent de rattachement est sur le point de retransmettre le message de révocation, il DOIT mettre à jour la

valeur de l'horodatage dans l'identifiant de révocation avec la valeur actuelle de la même horloge qu'utilisée pour générer les horodatages dans les extensions de révocation envoyées à cet agent étranger. Noter que ceci signifie aussi nécessairement de mettre à jour tout champ dérivé qui utilise l'identifiant de révocation (par exemple, un authentifiant rattachement-étranger) ;

- l'agent de rattachement NE DOIT PAS envoyer plus d'une révocation par seconde pour un certain lien,
- le délai entre les retransmissions DEVRAIT augmenter de façon analogue à celles indiquée par les lignes directrices d'enregistrement de la [RFC3344], à savoir un retard exponentiel, et
- l'agent de rattachement NE DOIT PAS retransmettre les messages de révocation au delà de la durée de vie normale du lien identifié par le message de révocation.

#### 4.2.2.2 Responsabilités de l'agent étranger

À réception d'un message de révocation d'enregistrement, l'agent étranger DOIT vérifier la validité de l'authentifiant, du bit 'A', et du champ d'identifiant, contre la répétition, comme défini au paragraphe 3.5. L'agent étranger DOIT aussi identifier le lien décrit par l'agent de rattachement comme étant libéré en utilisant les informations du message de révocation, à savoir les adresses identifiées par l'adresse du nœud mobile, l'adresse du domaine étranger, l'adresse du domaine de rattachement, ainsi que l'horodatage dans le message de révocation, et aussi l'horodatage dans le dernier message d'enregistrement accepté ; les révocations ne sont valides que pour les enregistrements existants, et donc l'horodatage d'un enregistrement DOIT précéder le message de révocation (noter que ces deux horodatages ont été établis par le même agent de rattachement). Ayant localisé le lien, l'agent étranger DOIT le révoquer, et DOIT répondre par un accusé de réception de révocation envoyé à l'adresse de source du message de révocation. Si le bit 'I' a été négocié, l'agent étranger DOIT vérifier la valeur du bit 'I' dans le message de révocation et agir en conséquence.

Si il notifie le nœud mobile par les méthodes décrites au paragraphe 4.1, l'agent étranger DOIT régler le bit 'I' à '1' dans l'accusé de réception de révocation à envoyer à l'agent de rattachement, ou si il ne notifie pas le nœud mobile, l'agent étranger DOIT régler le bit 'I' à '0'.

L'agent étranger peut arrêter tous les services IP sur l'ancien lien à ce moment, et libérer toutes les ressources qui étaient utilisées par lui.

L'agent étranger DOIT alors générer un accusé de réception de révocation, régler les champs Adresse de rattachement et Identifiant dans le message d'accusé de réception de révocation comme décrit au paragraphe 3.5, et le protéger avec un authentifiant valide comme spécifié au paragraphe 3.3.

#### 4.2.2.3 Responsabilités du nœud mobile colocalisé 'direct'

À réception d'un message de révocation, le nœud mobile colocalisé 'direct' DOIT valider l'authentifiant, et vérifier l'adresse de rattachement et l'identifiant spécifiés dans le message de révocation en cas de répétition. Si le paquet est authentifié, et si l'identifiant révèle que cette révocation est nouvelle, le nœud mobile DOIT vérifier que les informations contenues dans les messages de révocation identifient l'agent de rattachement avec lequel il a le lien actuel, que ce lien identifie correctement ce nœud mobile et toute adresse de domaine étranger qu'il utilise actuellement. Si le nœud mobile est capable d'identifier un tel lien, le nœud mobile DEVRAIT d'abord générer un message d'accusé de réception de révocation qui DOIT être envoyé à l'adresse IP de source du message de révocation. Le nœud mobile peut alors terminer toute encapsulation de tunnel inverse [RFC3024] qu'il utilise avec cet agent de rattachement, et considérer que son lien est révoqué, et libérer toutes les autres ressources associées à l'ancien lien.

#### 4.2.3 Domaine étranger révoquant/libérant un enregistrement

Les paragraphes qui suivent détaillent les responsabilités de chaque partie selon la fonction négociée dans les extensions de prise en charge de la révocation lorsque le domaine étranger révoque un enregistrement. Noter que la prise en charge de la révocation pour un nœud mobile colocalisé qui s'enregistre via un agent étranger (parce que le bit 'R' était établi dans l'annonce de l'agent) n'est pas acceptée. Voir les détails au paragraphe 4.3.1.

##### 4.2.3.1 Responsabilités de l'agent étranger

Si l'utilisation du bit 'I' a été négociée, et si la politique du domaine étranger d'information du nœud mobile n'a pas changé depuis le dernier échange réussi d'enregistrement, l'agent étranger NE DOIT PAS informer un nœud mobile de sa révocation à ce moment. L'agent étranger DOIT plutôt régler le bit 'I' à '1' dans le message de révocation, demandant par là à l'agent de rattachement d'utiliser le bit 'I' dans l'accusé de réception de révocation pour indiquer si il devrait notifier les nœuds mobiles affectés. Si la politique du domaine étranger était de ne pas notifier le nœud mobile, ou si elle a changé depuis le plus récent enregistrement réussi, et si l'agent étranger n'est plus capable d'utiliser le bit 'I', l'agent étranger DOIT régler le bit 'I' à '0', et

suivre les politiques du domaine étranger à l'égard de la notification des nœuds mobiles.

Noter que le bit 'A' DOIT être réglé à '0' pour indiquer que le message de révocation vient de l'agent étranger qui dessert ce lien.

Avant de transmettre le message de révocation, l'agent étranger DOIT régler l'identifiant de révocation comme décrit au paragraphe 3.5, et DOIT inclure un authentifiant, comme décrit au paragraphe 3.3.

Si l'agent étranger ne reçoit pas de message d'accusé de réception de révocation dans un délai raisonnable, il DOIT retransmettre le message de révocation. La durée pendant laquelle l'agent étranger attend avant de retransmettre, et combien de fois le message est retransmis, n'est limité que par les spécifications suivantes :

- chaque fois que l'agent étranger est sur le point de retransmettre le message de révocation, il DOIT mettre à jour la valeur de l'horodatage dans l'identifiant de révocation avec la valeur actuelle de la même horloge qu'utilisée pour générer les horodatages dans les extensions de révocation envoyées à cet agent de rattachement. Noter que cela signifie aussi nécessairement de mettre à jour tous les champs dérivés qui utilisent l'identifiant de révocation (par exemple, un authentifiant rattachement-étranger) ;
- il NE DOIT PAS envoyer plus d'une révocation par seconde pour un lien particulier,
- il DEVRAIT régler ses retransmissions à un retard analogue à celui des lignes directrices d'enregistrement de la [RFC3344], à savoir un retard exponentiel, et
- il NE DOIT PAS retransmettre de messages de révocation au delà de la durée de vie normale du lien identifié par le message de révocation.

#### 4.2.3.2 Responsabilités de l'agent de rattachement

À réception d'un message de révocation d'enregistrement, l'agent de rattachement DOIT vérifier le bit 'A', et le champ d'identifiant, ainsi que l'authentifiant. Si le paquet est acceptable, l'agent de rattachement DOIT localiser le lien identifié par l'agent étranger comme ayant été libéré en utilisant les informations du message de révocation, à savoir les adresses identifiées par les champs Adresse de rattachement, Adresse de domaine étranger et Adresse du domaine de rattachement. Comme les révocations ne sont valides que pour les enregistrements existants, l'horodatage d'un enregistrement DOIT précéder le message de révocation (noter que ces deux horodatages ont été établis par le même agent étranger). Comme ce lien n'est plus actif, l'agent de rattachement peut libérer toutes les ressources associées à l'ancien lien et cesser tous les services IP mobile pour lui.

Ayant traité un message valide de révocation d'enregistrement, l'agent de rattachement DOIT envoyer un accusé de réception de révocation à l'adresse IP de source du message de révocation d'enregistrement.

Si l'utilisation du bit 'I' a été négociée, et si le bit 'I' était réglé à '1' dans le message de révocation, l'agent de rattachement devrait décider si il veut que le nœud mobile soit informé de la révocation de ce lien. Si il veut que le nœud mobile soit informé, il DOIT régler le bit 'I' dans le message d'accusé de réception de révocation à '1'. Si il ne veut pas que le nœud mobile soit informé, il DOIT régler le bit 'I' à '0'.

L'agent de rattachement DOIT régler les champs Adresse de rattachement, et Identifiant de révocation comme décrit au paragraphe 3.5, et protéger le message d'accusé de réception de révocation avec un authentifiant valide comme spécifié au paragraphe 3.3.

#### 4.2.4 Nœud mobile désenregistrant un enregistrement

Dans les cas où un nœud mobile est enregistré auprès d'un agent de rattachement, qu'il soit enregistré directement auprès de son agent de rattachement (nœud mobile colocalisé 'direct') ou enregistré via un agent étranger, et souhaite terminer son propre lien, le nœud mobile NE DOIT PAS envoyer un message de révocation, mais DEVRAIT simplement se désenregistrer de l'adresse d'entretien appropriée auprès de son agent de rattachement, comme décrit dans la [RFC3344].

### 4.3 Bits d'enregistrement IP mobile dans le processus de révocation

Plusieurs des bits utilisés dans le processus d'enregistrement doivent faire l'objet d'une considération particulière lorsque on utilise le mécanisme de révocation.

#### 4.3.1 Bit 'R' utilisé

Si l'agent étranger souhaite être capable de révoquer l'enregistrement d'un nœud mobile, il DOIT établir le bit 'R' dans ses

annonces d'agent. (Un agent étranger qui annonce le bit 'R' demande à chaque nœud mobile, même celui qui est colocalisé (et dont l'enregistrement court-circuiterait autrement l'agent étranger) de s'enregistrer auprès de l'agent étranger.) Cependant, dans ce cas, l'agent étranger DEVRAIT refuser une demande d'enregistrement comme "Administrativement interdite" provenant d'un nœud mobile qui s'enregistre de façon colocalisée. La raison en est que l'agent étranger ne sera pas capable de révoquer le lien d'un nœud mobile colocalisé pour des raisons expliquées au paragraphe 4.3.2.

Comment l'agent étranger et/ou le domaine étranger mettent en application le bit 'R' sort du domaine d'application du présent document.

#### 4.3.2 Bit 'D' utilisé

Un nœud mobile qui s'enregistre directement auprès de son agent de rattachement d'une façon colocalisée avec le bit 'D' établi dans sa demande d'enregistrement est pris en charge dans la révocation d'enregistrement. Cependant, la prise en charge d'un nœud mobile colocalisé (avec le bit 'D' établi dans sa demande d'enregistrement) qui s'enregistre via un agent étranger n'est pas acceptée pour les raisons suivantes.

Les demandes d'enregistrement où le bit 'D' est établi, et qui sont relayées par un agent étranger (par exemple, à cause de l'annonce du bit 'R') devraient théoriquement contenir l'adresse de l'agent étranger comme adresse de source de la demande d'enregistrement lorsque elle est reçue par l'agent de rattachement. Un agent de rattachement peut conclure que l'adresse de source de cette demande d'enregistrement n'est pas la même que l'adresse d'entretien colocalisée contenue dans la demande d'enregistrement, et est donc vraisemblablement l'adresse de l'agent étranger. Cependant, comme il n'y a aucun moyen de garantir que cette adresse IP de source est en fait une adresse de l'agent étranger qui dessert le nœud mobile, accepter un message de révocation de cette adresse IP de source peut conduire à une attaque de déni de service par interposition sur le nœud mobile.

De plus, il n'y a actuellement aucune méthode pour que l'agent étranger qui dessert le nœud mobile s'identifie lui-même auprès de l'agent de rattachement durant la phase d'enregistrement IP mobile. Même si un agent étranger pouvait s'identifier, le nœud mobile colocalisé aurait aussi besoin d'autoriser que cet agent étranger soit bien l'agent qui lui fournit les services IP mobile. C'est pour déjouer une attaque de déni de service contre le nœud mobile par un agent étranger qui a une association de sécurité avec l'agent de rattachement, et est sur le chemin entre le nœud mobile colocalisé et l'agent de rattachement.

## 5. Codes d'erreur

Comme l'intention d'un message de révocation d'enregistrement n'est pas une demande de cesser les services, mais est une notification que les services IP mobile sont interrompus, il n'y a pas de nouveau code d'erreur.

## 6. Considérations sur la sécurité

Il y a deux faiblesses potentielles, une dans le mécanisme d'annonce d'agent, et une qui se rapporte aux messages de révocation non autorisés.

### 6.1 Annonces d'agent

Bien que les mécanismes définis par le présent document n'introduisent pas ce problème, il a été reconnu que les annonces d'agent telles que définies dans la [RFC3344] exposent les nœuds mobiles à un déni de service potentiel. C'est parce que l'annonce d'agent telle que définie dans la [RFC3344] peut être simulée par d'autres machines résidant sur la liaison. Cela rend possible pour un tel nœud d'amener le nœud mobile à croire que son enregistrement a été révoqué soit en envoyant une annonce en individuel avec un numéro de séquence remis à zéro à l'adresse de liaison locale du nœud mobile, soit en la diffusant au sous-réseau, trompant ainsi tous les nœuds mobiles enregistrés sur un certain agent étranger en leur faisant croire que leur enregistrement a été perdu.

Des travaux ont été conduits dans ce groupe de travail et d'autres (par exemple, IPsec) pour sécuriser ces annonces de routeur, bien qu'au moment de la présente publication, aucune solution ne soit devenue de pratique courante. Pour aider à circonvier de possibles problèmes de déni de service en réduisant à un minimum leur potentiel de perturbation, les mises en œuvre de nœud mobile devraient s'assurer que toute annonce d'agent qui ne se conforme pas strictement à la [RFC3344], et précisément celles dont le TTL n'est pas 1, ou qui n'émanent pas de la même adresse de liaison (lorsque présente) que les autres annonces d'agent supposées provenir du même agent, ou même de celle de la dernière réponse d'enregistrement réussie, sont éliminées en silence.

## 6.2 Messages de révocation

Comme la révocation d'enregistrement, lorsque elle est effectuée, termine la fourniture des services IP mobile au nœud mobile, il est crucial que tous les mécanismes de sécurité et de protection contre la répétition soient vérifiés avant qu'un agent de mobilité puisse croire que l'autre agent a révoqué un lien. Les messages qui sont envoyés sur une liaison locale (par exemple, entre le nœud mobile et l'agent étranger) PEUVENT aussi être sécurisés par des méthodes qui sont précisées dans la [RFC3344], à savoir l'utilisation d'authentifiants mobile-étranger, mais ceux-ci n'ont pas de relation directe avec la révocation d'enregistrement.

La [RFC3344] définit un mécanisme de sécurité qui DOIT être utilisé entre les agents de rattachement et les nœuds mobiles, et PEUT être utilisé entre les agents de rattachement et les agents étrangers, à savoir l'utilisation d'authentifiants. Tous les agents étrangers et de rattachement DOIVENT prendre en charge la protection des messages de révocation via les authentifiants étranger-rattachement définis dans la [RFC3344]. Ils PEUVENT mettre en œuvre d'autres mécanismes de force égale ou supérieure ; si de tels mécanismes sont connus pour être disponibles aux deux parties, ils PEUVENT être utilisés à la place.

Les messages de révocation sont au moins aussi sûrs que les messages d'enregistrement passés entre les agents de rattachement et étrangers et qui contiennent des authentifiants de rattachement-étranger comme défini dans la [RFC3344]. Donc, il n'y a pas de nouvelles menaces pour la sécurité introduites par le mécanisme de révocation autres que celles présentes dans la [RFC3344] par rapport à la compromission du secret partagé utilisé pour générer les authentifiants de rattachement-étranger.

Ceci dit, il y a deux types d'attaques actives qui utilisent les messages capturés "en vol" par un agresseur interposé entre les agents de rattachement et étranger, les "répéteurs malveillants" et les "réflecteurs malveillants".

Dans le cas d'un "répéteur malveillant", un agresseur interposé capture un message de révocation, puis le répète à la même adresse de destination IP ultérieurement. En présumant que l'authentifiant du paquet original était réputé valide, sans protection contre la répétition, l'authentifiant de rattachement-étranger du paquet répété va (à nouveau) réussir l'authentification. Noter que comme il n'est pas garanti que les datagrammes arrivent non dupliqués, une répétition peut se produire sans intention malveillante.

Dans le cas du "réflecteur malveillant", un agresseur interposé capture un message de révocation, puis le retourne ultérieurement à son générateur. Si l'association de sécurité entre les domaines de rattachement et étranger utilise une association de sécurité qui implique un (seul) secret partagé qui ne protège que le contenu de la portion UDP du paquet (de tels authentifiants de rattachement-étranger sont définis par la [RFC3344]) sans protection contre la répétition, l'expéditeur du paquet va aussi penser que le message de révocation est authentique.

Le mécanisme de protection contre la répétition utilisé par les messages de révocation définis par le présent document est conçu pour protéger contre ces deux attaques actives. Il profite de l'utilisation de l'horodatage de 32 bits qui peut être plus rapidement déterminé si les messages de révocation sont répétés, bien qu'on conseille au lecteur d'utiliser cette approche avec certaines précautions. Un agent qui reçoit un message de révocation authentifié peut comparer le champ Identifiant avec celui d'un message de révocation reçu précédemment, et si l'horodatage dans le nouveau message se trouve avoir été généré après celui de l'horodatage dans le dernier message de révocation reçu, il peut immédiatement déterminer qu'il n'est pas une répétition. Noter cependant que comme les datagrammes ne sont pas garantis d'arriver dans l'ordre, on ne devrait pas présumer que parce que les valeurs contenues dans un champ Identifiant sont horodatées, elles vont nécessairement être croissantes à chaque message de révocation reçu successivement. Si une mise en œuvre devait décider de fonder son mécanisme de détection de répétition sur les horodatages croissants, et donc des valeurs croissantes d'identifiant, une fenêtre temporelle convenable devrait être définie dans laquelle les messages de révocation peuvent être reçus. Au pire, ignorer un message de révocation devrait résulter en la retransmission d'un autre message de révocation, cette fois avec un horodatage postérieur au dernier reçu.

Noter que toute demande ou réponse d'enregistrement peut être répétée. Avec l'échange des horodatages entre les agents dans les extensions de révocation, un agent devrait avoir la certitude que de tels messages ont été livrés à temps. Pour les besoins de la révocation d'enregistrement, la livraison à temps d'un paquet d'enregistrement se fonde simplement sur la granularité de chaque enregistrement. Comme la [RFC3344] fournit un mécanisme de protection contre la répétition à utiliser par l'agent de rattachement, il a le moyen de dire si la demande d'enregistrement présentée est nouvelle. L'agent étranger, cependant, n'a pas un tel mécanisme avec le nœud mobile. Il est conseillé aux agents étrangers de continuer de considérer les enregistrements 'en suspens' jusqu'à ce que la réponse d'enregistrement associée soit retournée de l'agent de rattachement avant d'utiliser les informations dans une de ses entrées de visiteur. Même alors, cela laisse l'agent étranger ouvert à une potentielle attaque de déni de service dans laquelle les demandes d'enregistrement et les réponses sont répétées par plusieurs nœuds. Lorsque cela arrive, l'agent étranger pourrait être amené à croire que de tels enregistrements sont actifs, mais avec de vieilles informations, qui peuvent avoir des effets adverses sur eux, ainsi que sur la capacité que cet agent utilise avec succès les procédures

mentionnées dans le présent document. Une protection suffisante contre ce scénario est offerte par le mécanisme de mise en cause-réponse de la [RFC3012] par lequel un agent étranger génère une mise en cause en direct à un nœud mobile afin de s'assurer, entre autres choses, que la demande d'enregistrement n'est pas une répétition.

## 7. Considérations relatives à l'IANA

Le présent document définit un ensemble supplémentaire de messages entre l'agent de rattachement et l'agent étranger spécifiques des services fournis au même nœud mobile, ou sous ensemble de nœuds mobiles. Pour assurer une interopération correcte sur la base de la présente spécification, l'IANA a réservé des valeurs dans l'espace de numéros IP mobile pour deux nouveaux types de message, et une seule nouvelle extension.

### 7.1 Nouveaux types de message

Les types de message suivants sont introduits par la présente spécification :

Révocation d'enregistrement : nouveau message de commande IP mobile, utilisant l'accès UDP 434, type 7. Cette valeur a été prise dans le même espace de numéros que Demande d'enregistrement IP (Type = 1), et Réponse d'enregistrement IP mobile (Type = 3).

Accusé de réception de révocation d'enregistrement : nouveau message de commande IP mobile, utilisant l'accès UDP 434, type 15. Cette valeur a été prise dans le même espace de numéros que Demande d'enregistrement IP (Type = 1), et Réponse d'enregistrement IP mobile (Type = 3).

### 7.2 Nouvelles valeurs d'extension

L'extension suivante est introduite par la présente spécification :

Extension prise en charge de révocation : nouvelle extension IP mobile, ajoutée à une demande d'enregistrement, ou une réponse d'enregistrement. La valeur allouée est 137. Cette extension est dérivée de l'espace de numéros Extension. Elle DOIT être dans la gamme 'sautable' (128 - 255) comme défini dans la RFC 3344.

### 7.3 Nouveaux codes d'erreur

Le présent document n'introduit pas de nouveau code d'erreur IP mobile.

## 8. Références

### 8.1 Références normatives

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

[RFC3012] C. Perkins, P. Calhoun, "Extensions de mise en cause/réponse pour IPv4 mobile", novembre 2000. (*Obs., voir RFC4721*) (*P.S.*)

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

### 8.2 Références pour information

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

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

[RFC2977] S. Glass, T. Hiller, S. Jacobs, C. Perkins, "Exigences d'authentification, d'autorisation et de comptabilité pour IP mobile", octobre 2000. (*Information*)

[RFC2989] B. Aboba et autres, "Critères d'évaluation des protocoles AAA pour l'accès réseau", novembre 2000. (*Information*)

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

## Appendice A Exemple des messages de révocation utilisés

À titre d'éclaircissement, l'exemple suivant est destiné à illustrer l'utilisation des nouveaux messages dans la phase d'enregistrement, et dans la phase de révocation. Dans cet exemple, un agent étranger et un agent de rattachement vont négocier la révocation durant la phase d'enregistrement. Durant la phase de révocation, l'agent étranger va révoquer le lien d'un nœud mobile.

### A.1 Phase d'enregistrement

Considérons un agent étranger qui prend en charge la révocation d'enregistrement, et a une association de sécurité avec un agent de rattachement auquel il transmet une demande d'enregistrement. L'agent étranger va inclure l'extension de prise en charge de la révocation après l'authentifiant mobile-rattachement. Supposons que l'agent étranger prenne en charge l'utilisation du bit 'I', et qu'il veuille laisser l'agent de rattachement décider si le nœud mobile devrait être informé de la révocation de son enregistrement. Donc, l'agent étranger va régler le bit 'I' à '1'. L'agent étranger va ajouter un authentifiant étranger-rattachement à la demande d'enregistrement.

À réception de la demande d'enregistrement contenant une extension de révocation, l'agent de rattachement va inclure une extension de prise en charge de la révocation dans la réponse d'enregistrement. Comme l'agent étranger a réglé le bit 'I' à '1' dans son extension de révocation, et que l'agent de rattachement prend en charge l'utilisation du bit 'I', l'agent de rattachement va régler le bit 'I' dans son extension d'enregistrement à '1'. De plus, l'agent de rattachement va ajouter un authentifiant rattachement-étranger à la demande d'enregistrement.

À réception de la réponse d'enregistrement authentifiée, l'agent étranger va vérifier l'extension de prise en charge de la révocation et noter que l'agent de rattachement veut décider si le nœud mobile devrait être notifié en cas de révocation de cet enregistrement, c'est-à-dire, que l'agent de rattachement a établi le bit 'I' dans l'extension de révocation retournée.

### A.2 Phase de révocation

L'agent étranger révoque le lien d'un nœud mobile, et génère un message de révocation à envoyer à l'agent de rattachement du nœud mobile. Comme le bit 'I' a été négocié dans l'extension de révocation, et comme l'agent étranger veut encore laisser l'agent de rattachement indiquer si ce nœud mobile devrait être informé de la révocation, il va régler le bit 'I' à '1' dans le message de révocation. L'agent étranger s'assure aussi que le bit 'A' est réglé à '0'.

L'agent étranger va aussi placer l'adresse du nœud mobile dont il souhaite révoquer l'enregistrement dans le champ Adresse de rattachement, l'adresse que le nœud mobile a enregistré comme adresse d'entretien dans le champ Domaine étranger, et l'adresse enregistrée comme agent de rattachement dans le champ Adresse de domaine de rattachement. L'agent étranger va régler l'identifiant de révocation à l'horodatage actuel de 32 bits, et ajouter l'authentifiant étranger-rattachement.

À réception du message de révocation ci-dessus, l'agent de rattachement utilise l'adresse identifiée comme adresse de domaine étranger pour identifier l'association de sécurité, et authentifier le message de révocation. Après l'authentification du message, l'agent de rattachement va vérifier que le bit 'A' et l'identifiant indiquent que cette révocation n'est pas une répétition. L'agent de rattachement utilise alors l'adresse de rattachement du nœud mobile, l'adresse de domaine étranger et l'adresse de domaine de rattachement pour localiser le nœud mobile dont l'enregistrement est révoqué.

En traitant un message de révocation d'enregistrement valide, l'agent de rattachement génère un message d'accusé de réception de révocation. Comme le bit 'I' a été réglé à '1' dans le message de révocation et comme l'agent de rattachement souhaite que le nœud mobile identifié soit informé de la révocation, il va régler le bit 'I' dans l'accusé de réception de révocation à '1'. L'agent de rattachement copie alors l'adresse de rattachement et le champ Identifiant de révocation dans l'accusé de réception de révocation. L'agent de rattachement protège l'accusé de réception de révocation avec un authentifiant rattachement-étranger.

À réception d'un accusé de réception de révocation valide (dans lequel les champs Authentifiant et Identifiant sont acceptables) l'agent étranger vérifie l'état du bit 'I'. Comme le bit 'I' est réglé à '1', l'agent étranger va notifier la révocation au nœud mobile.



## Appendice B Adresse disparate, et considérations de receveur

Comme le message de révocation d'enregistrement vient d'une adresse de source qui est topologiquement acheminable à partir de l'interface qui reçoit le datagramme, les agents, par définition, sont topologiquement connectés (si ce n'était pas le cas, le mécanisme d'enregistrement initial aurait échoué). Si l'un ou l'autre est le dernier bond à partir de cette région topologiquement connectée à un ou plusieurs espaces d'adresses disparates, aucun problème ne se pose. Pour que le nœud mobile se soit enregistré avec succès auprès de son agent de rattachement, il DOIT avoir fourni au réseau (agent étranger) auquel il est actuellement rattaché une adresse acheminable de son agent de rattachement. À l'inverse, l'adresse d'entretien qui est utilisée par le nœud mobile doit aussi être topologiquement significative pour l'agent de rattachement afin que la réponse d'enregistrement ait été reçue, et le tunnel initié. Par définition, l'adresse de l'agent de rattachement et l'adresse d'entretien doivent chacune être significatives, et l'une et l'autre adresse doivent former une paire unique dans le contexte de ce nœud mobile avec les deux agents.

Une autre façon de comprendre cela est que les points d'extrémité du tunnel sont connectés d'une certaine façon, et donc chacun est unique pour autant que l'autre extrémité est concernée. L'adresse à l'autre extrémité du tunnel, en combinaison avec l'adresse du nœud mobile, doit donc former une paire unique qui peut être identifiée par l'agent qui reçoit le message de révocation d'enregistrement.

Par exemple, considérons un nœud mobile dont l'adresse de rattachement se tient dans un espace d'adresses disparate A derrière son agent de rattachement. Dans le diagramme suivant, [x] indique une interface de l'entité dans laquelle il apparaît.

```

MN[a]-----[c]FA[b]====(( ))====[b]HA[a]-----[a]CN
Espace d'adresses C   Un réseau topologiquement connecté   Espace d'adresses A

```

On suppose qu'il existe un lien pour MN, et donc un tunnel entre FA[b] et HA[b]. Alors, comme l'adresse allouée à MN[a] DOIT être unique dans l'espace d'adresses A, l'unicité de la paire {FA[b],MN[a]} est garantie dans le tableau des liaisons de HA, et l'unicité de la paire {HA[b],MN[a]} est garantie dans la liste des visiteurs de l'agent étranger.

Il en résulte qu'un agent de rattachement qui reçoit un message de révocation d'enregistrement et un authentifiant étranger-rattachement pour MN[a] de FA[b] est capable de déterminer l'unique adresse du nœud mobile qui est désenregistrée. À l'inverse, un agent étranger qui reçoit un message de révocation d'enregistrement et un authentifiant rattachement-étranger pour MN[a] de HA[b] est capable de déterminer l'adresse exacte du nœud mobile qui est désenregistré. Pour cette raison, si un agent étranger reçoit un message de révocation d'enregistrement avec le champ Domaine de rattachement réglé à l'adresse zéro, il DOIT être éliminé en silence. C'est pour éviter les confusions dans le cas de chevauchement d'adresses privées ; lorsque plusieurs nœuds mobiles sont enregistrés via la même adresse d'entretien et, par coïncidence, utilisent la même adresse de rattachement (disparate/privée) l'adresse d'agent de rattachement qui apparaît dans le champ Domaine de rattachement est la seule façon qu'a un agent étranger pour discerner la différence entre ces nœuds mobiles.

## Remerciements

Les auteurs tiennent à remercier Rajesh Bhalla, Kent Leung, et Alpesh Patel de leurs contributions aux concepts détaillés dans le projet draft-subbarao-mobileip-resource-00.txt, "Libération de ressources dans IP mobile," à partir duquel a été dérivée l'extension de prise en charge de la révocation, et le mécanisme d'accusé de réception contenu dans le présent document.

Les auteurs tiennent aussi à remercier Pete McCann pour ses discussions sur les mécanismes de répétition, et les questions de sécurité, et Ahmad Muhanna pour avoir soulevé un problème dans le mécanisme initial de répétition, qui a finalement conduit à l'ajout d'un horodatage à l'extension de révocation.

Les auteurs tiennent aussi à remercier Henrik Levkowitz de sa relecture détaillée du document, et Michael Thomas de sa révision du mécanisme de répétition décrit ici.

## Adresses des auteurs

Steven M. Glass  
Solaris Network Technologies  
Sun Microsystems  
1 Network Drive  
Burlington, MA. 01801  
téléphone : +1.781.442.0000  
mél : [steven.glass@sun.com](mailto:steven.glass@sun.com)

Madhavi W. Chandra  
IOS Technologies Division  
Cisco Systems  
7025 Kit Creek Road  
Research Triangle Park, NC 27709  
téléphone : +1.919.392.8387  
mél : [mchandra@cisco.com](mailto:mchandra@cisco.com)

## **Déclaration complète de droits de reproduction**

Copyright (C) The Internet Society (2003). Tous droits réservés.

Le présent document et ses traductions peuvent être copiés et fournis aux tiers, et les travaux dérivés qui les commentent ou les expliquent ou aident à leur mise en œuvre peuvent être préparés, copiés, publiés et distribués, en tout ou partie, sans restriction d'aucune sorte, pourvu que la déclaration de droits de reproduction ci-dessus et le présent paragraphe soient inclus dans toutes telles copies et travaux dérivés. Cependant, le présent document lui-même ne peut être modifié d'aucune façon, en particulier en retirant la notice de droits de reproduction ou les références à la Internet Society ou aux autres organisations Internet, excepté autant qu'il est nécessaire pour le besoin du développement des normes Internet, auquel cas les procédures de droits de reproduction définies dans les procédures des normes Internet doivent être suivies, ou pour les besoins de la traduction dans d'autres langues que l'anglais.

Les permissions limitées accordées ci-dessus sont perpétuelles et ne seront pas révoquées par la Internet Society ou ses successeurs ou ayant droits.

Le présent document et les informations y contenues sont fournies sur une base "EN L'ÉTAT" et le contributeur, l'organisation qu'il ou elle représente ou qui le/la finance (s'il en est), la INTERNET SOCIETY et la INTERNET ENGINEERING TASK FORCE déclinent toutes garanties, exprimées ou implicites, y compris mais non limitées à toute garantie que l'utilisation des informations ci encloses ne violent aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet particulier.

### **Remerciement**

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