

Groupe de travail Réseau
Request for Comments : 4636
 Catégorie: Sur la voie de la normalisation

C. Perkins, Nokia Research Center
 octobre 2006
 Traduction Claude Brière de L'Isle

Extension d'erreur d'agent étranger pour IPv4 Mobile

Statut du présent mémoire

Le présent document spécifie un protocole de l'Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Protocoles officiels de l'Internet" (STD 1) pour voir 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 (2006). Tous droits réservés.

Résumé

Le présent document spécifie une nouvelle extension pour l'usage des agents étrangers qui font fonctionner IP mobile pour IPv4. Actuellement, un agent étranger ne peut pas fournir des informations d'état sans détruire la capacité d'un nœud mobile de vérifier les données d'authentification fournies par l'agent de rattachement. La nouvelle extension résout ce problème en faisant une meilleure place à l'agent étranger pour fournir ses informations d'état au nœud mobile.

1. Introduction

Le présent document spécifie une nouvelle extension non sautable pour l'usage des agents étrangers qui opèrent sur IP mobile pour IPv4 [RFC3344]. La nouvelle option d'extension permet à un agent étranger de fournir un code d'erreur sans perturber les données fournies par l'agent de rattachement au sein du message de réponse d'enregistrement. De cette façon, le nœud mobile peut vérifier que le message Réponse d'enregistrement a été généré par l'agent de rattachement même dans les cas où l'agent étranger est obligé par le protocole d'insérer de nouvelles informations d'état dans le message de réponse d'enregistrement.

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]. Le reste de la terminologie utilisée est déjà défini dans la [RFC3344].

3. Format de l'extension d'erreur d'agent étranger

Le format de l'extension Erreur d'agent étranger se conforme au format court d'extension spécifié pour IPv4 mobile [RFC3344]. L'extension Erreur d'agent étranger n'est pas sautable.

```

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 | Sous type |      État      |
+-----+-----+-----+-----+-----+-----+

```

Type : 45

Longueur : 2

Sous type : 0

État : un code d'état utilisé par l'agent étranger pour fournir les informations d'état au nœud mobile.

4. Fonctionnement et utilisation de l'extension Erreur d'agent étranger

L'extension Erreur d'agent étranger n'est valide que pour être utilisée au sein des messages de réponse d'enregistrement IPv4 mobile. L'extension Erreur d'agent étranger n'est pas sautable. Un nœud mobile qui ne peut pas interpréter correctement le contenu de l'extension Erreur d'agent étranger NE DOIT PAS utiliser l'adresse d'entretien fournie dans le message de réponse d'enregistrement, jusqu'à ce qu'un autre message de demande d'enregistrement ait été envoyé et qu'un message de réponse d'enregistrement réussi ait été reçu.

Les codes d'état dont l'utilisation est permis au sein de l'extension Erreur d'agent étranger sont dans la gamme 64-127. Les codes actuellement spécifiés sont les suivants :

- 64 raison non spécifiée
- 65 administrativement interdit
- 66 ressources insuffisantes
- 68 l'agent de rattachement échoue à l'authentification
- 71 réponse mal formée
- 77 adresse d'entretien invalide
- 78 fin de temporisation d'enregistrement

comme défini dans la [RFC3344] pour l'usage de l'agent étranger. Les codes d'état à utiliser avec les extensions Erreur d'agent étranger ne doivent pas être définis différemment de ceux à utiliser dans le champ Code des Réponse d'enregistrement.

Quand un agent étranger ajoute une extension Erreur d'agent étranger à la réponse d'enregistrement comme reçue de l'agent de rattachement, il doit mettre à jour le champ Longueur UDP dans l'en-tête UDP [RFC0768] pour tenir compte des quatre octets supplémentaires.

Le présent document met à jour la spécification de base IP mobile IP [RFC3344] en ce qui concerne les procédures suivies par l'agent étranger dans le cas où l'agent de rattachement échoue à l'authentification. Au lieu de modifier le champ "État" de la réponse d'enregistrement pour qu'il contienne la valeur 68, maintenant l'agent étranger devrait ajouter l'extension Erreur d'agent étranger contenant la valeur d'état 68.

5. Considérations de nœud mobile

Si un nœud mobile reçoit une réponse d'enregistrement réussie (code d'état 0 ou 1) avec une extension Erreur d'agent étranger qui indique que l'agent étranger n'honore pas ladite réponse d'enregistrement, le nœud mobile DEVRAIT alors envoyer un message de dés-enregistrement à l'agent de rattachement. De cette façon, l'agent de rattachement ne conservera pas un état d'enregistrement incohérent avec l'état conservé par l'agent étranger.

6. Considérations d'agent étranger

Quand il refuse une réponse d'enregistrement réussie, l'agent étranger DEVRAIT envoyer un message de révocation d'enregistrement [RFC3543] à l'agent de rattachement si une association de sécurité de mobilité existe entre eux. Pour les cas où l'agent étranger n'a pas l'association de sécurité requise, cette façon d'informer l'agent de rattachement n'a pas la vulnérabilité aux actions destructrices d'agents étrangers malveillants, comme noté à la Section 8.

7. Considérations relatives à l'IANA

La présente spécification réserve un numéro pour l'extension Erreur d'agent étranger (voir la Section 3) dans l'espace de numéros pour les extensions de mobilité non sautables (c'est-à-dire, 0-127) défini dans la spécification de IPv4 mobile [RFC3344].

La présente spécification crée aussi un nouvel espace de numéros de sous types pour le numéro de type de cette extension. Le sous type zéro est à allouer dans cet espace de numéros pour l'extension de protocole spécifiée dans ce document. Comme avec les procédures spécifiées pour les espaces de numéros de IP mobile [RFC3344], les futures allocations dans

cet espace de numéros exigent une revue par expert [RFC2434].

Les codes d'état qui sont permis dans l'extension Erreur d'agent étranger sont un sous ensemble des codes d'état définis dans la spécification pour IPv4 mobile [RFC3344]. Si à l'avenir, des codes d'état supplémentaires sont définis pour IPv4 mobile, la définition de chaque nouveau code d'état devra indiquer si le nouveau code d'état est permis pour l'usage dans l'extension Erreur d'agent étranger.

8. Considérations sur la sécurité

L'extension du présent document améliore les caractéristiques de sécurité de IPv4 mobile en permettant au nœud mobile d'être assuré de l'authenticité des informations fournies dans une demande d'enregistrement. Précédemment, chaque fois que l'agent étranger était obligé de fournir des informations d'état au nœud mobile, il ne pouvait le faire qu'en détruisant la capacité de l'appareil mobile de vérifier les données d'extension d'authentification de rattachement mobile.

Dans la plupart des cas courants, le nœud mobile n'aura pas d'association de sécurité avec l'agent étranger qui a envoyé l'extension. Donc, le nœud mobile va être incapable de s'assurer que l'agent étranger qui envoie le message d'enregistrement étendu est le même agent étranger qui a antérieurement reçu la demande d'enregistrement associée de la part du nœud mobile. À cause de cela, un agent étranger malveillant pourrait provoquer un nœud mobile à fonctionner comme si l'enregistrement avait échoué, alors qu'en fait son agent de rattachement et un agent étranger fonctionnant correctement ont tous deux accepté la demande d'enregistrement du nœud mobile. Afin de réduire la vulnérabilité à de tels messages de réponse d'enregistrement transmis dans une intention malveillante avec l'extension non authentifiée, le nœud mobile PEUT retarder le traitement de tels messages de refus de réponse d'enregistrement pendant un petit moment afin de déterminer si une autre réponse d'enregistrement réussie pourrait être reçue de l'agent étranger.

9. Remerciements

Merci à Kent Leung et Henrik Lefkowitz pour les améliorations suggérées à cette spécification.

10. Références normatives

- [RFC0768] J. Postel, "Protocole de [datagramme d'utilisateur](#) (UDP)", (STD 6), 28 août 1980.
- [RFC2119] S. Bradner, "[Mots clés à utiliser](#) dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. (*MàJ par RFC8174*)
- [RFC2434] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, octobre 1998. (*Rendue obsolète par la RFC5226*)
- [RFC3344] C. Perkins, éd., "Prise en charge de la mobilité IP pour IPv4", août 2002. (*Obsolète, voir RFC5944*) (P.S.)
- [RFC3543] S. Glass, M. Chandra, "[Révocation d'enregistrement](#) dans IPv4 mobile", août 2003. (P.S.)

Adresse de l'auteur

Charles E. Perkins
Palo Alto Systems Research Lab
Nokia Research Center
975 Page Mill Road, Suite 200
Palo Alto, CA 94304-1003

téléphone : +1 650-496-4402
fax : +1-650-739-0779
mél : charles.perkins@nokia.com

Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2006). Tous droits réservés.

Le présent document est soumis aux droits, licences et restrictions contenus dans le BCP 78, et sauf pour ce qui est mentionné ci-après, les auteurs conservent tous leurs 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, le IETF TRUST 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 viole aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet particulier.

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 actuellement assuré par la Internet Society.