

Groupe de travail Réseau
Request for Comments : 5192
 Catégorie : Sur la voie de la normalisation

L. Morand, France Telecom R&D
 A. Yegin, Samsung
 S. Kumar, Tech Mahindra Ltd
 S. Madanapalli, Samsung
 mai 2008

Traduction Claude Brière de L'Isle

Options DHCP pour les agents d'authentification du protocole pour porter l'authentification pour l'accès réseau (PANA)

Statut du présent mémoire

Le présent document spécifie un protocole Internet sur la voie de la 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 "Normes officielles des protocoles de l'Internet" (STD 1) pour connaître l'état de la normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé

Le présent document définit de nouvelles options DHCPv4 et DHCPv6 qui contiennent une liste des adresses IP pour localiser un ou plusieurs agents d'authentification du protocole pour porter l'authentification pour l'accès au réseau (PANA, *Protocol for carrying Authentication for Network Access*) (PAA, *PANA Authentication Agent*). C'est une des méthodes qu'un client PANA (PaC, *PANA Client*) peut utiliser pour localiser des PAA.

Table des Matières

1. Introduction.....	1
2. Spécification des exigences.....	1
3. Terminologie.....	2
4. Option DHCPv4 Agent d'authentification PANA.....	2
5. Option DHCPv6 Agent d'authentification PANA.....	2
6. Considérations relatives à l'IANA.....	3
7. Considérations sur la sécurité.....	3
8. Remerciements.....	4
9. Références.....	4
9.1 Références normatives.....	4
9.2 Références pour information.....	4
Adresse des auteurs.....	4
Déclaration complète de droits de reproduction.....	5

1. Introduction

Le protocole pour porter l'authentification pour l'accès au réseau (PANA, *Protocol for carrying Authentication for Network Access*) [RFC5191] définit une nouvelle couche inférieure du protocole d'authentification extensible (EAP, *Extensible Authentication Protocol*) [RFC3748] qui utilise IP entre les points d'extrémité du protocole.

Le protocole PANA fonctionne entre un client PANA (PaC) et un agent d'authentification PANA (PAA, *PANA Authentication Agent*) afin d'effectuer l'authentification et l'autorisation pour le service d'accès au réseau.

Le présent document spécifie les options DHCPv4 [RFC2131] et DHCPv6 [RFC3315] qui permettent aux clients PANA (PaC) de découvrir les agents d'authentification PANA (PAA). C'est une des méthodes pour localiser les PAA.

Les options DHCP définies dans le présent document ne sont utilisées que comme mécanisme de découverte de PAA. Ces options DHCP NE DOIVENT PAS être utilisées pour effectuer une négociation de l'utilisation de PANA entre le PaC et un PAA.

2. Spécification des exigences

Dans ce document, plusieurs mots sont utilisés pour signifier les exigences de la spécification. Ces mots sont souvent en majuscules. 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].

3. Terminologie

Le présent document utilise la terminologie DHCP définie dans les [RFC2131], [RFC2132], et [RFC3315].

Le présent document utilise la terminologie PANA définie dans la [RFC5191]. En particulier, les termes suivants sont définis :

Client PANA (PaC) : côté client du protocole qui réside dans l'appareil d'accès (par exemple, tablette, PDA, etc.). Il est chargé de fournir les accreditifs afin de prouver son identité (authentification) pour l'autorisation d'accès au réseau. Le PaC et l'homologue EAP sont colocalisés dans le même appareil d'accès.

Agent d'authentification PANA (PAA, *PANA Authentication Agent*) : entité du protocole dans le réseau d'accès dont la responsabilité est de vérifier les accreditifs fournis par un client PANA (PaC) et autoriser l'accès réseau à l'appareil d'accès. Le PAA et l'authentificateur EAP (et facultativement le serveur EAP) sont colocalisés dans le même nœud.

4. Option DHCPv4 Agent d'authentification PANA

Cette option DHCPv4 porte une liste d'adresses IPv4 de 32 bits (binaires) qui indiquent les agents d'authentification PANA (PAA) disponibles au client PANA (PaC).

L'option DHCPv4 pour l'agent d'authentification PANA a le format indiqué à la Figure 1.

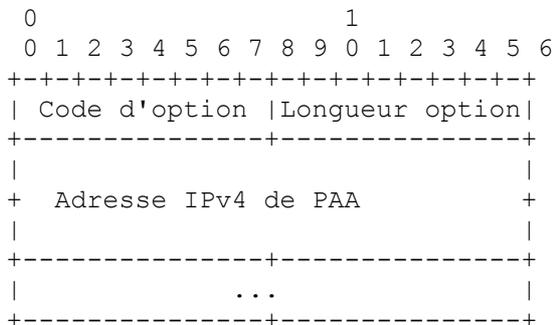


Figure 1 : option DHCPv4 de PAA

Code d'option : OPTION_PANA_AGENT (136).

Longueur option : longueur du champ "options" en octets ; DOIT être un multiple de quatre (4).

Adresse IPv4 de PAA : adresse IPv4 d'un PAA à utiliser par le client. Les PAA sont énumérés dans l'ordre de préférence d'utilisation par le client.

Un PaC (client DHCPv4) DEVRAIT demander l'option PAA DHCPv4 dans une liste de demande de paramètres, comme décrit dans les [RFC2131] et [RFC2132].

Si il est configuré avec une adresse (une liste d'adresses) de PAA, un serveur DHCPv4 DEVRAIT envoyer à un client l'option PAA DHCPv4, même si cette option n'est pas demandée explicitement par le client.

Un PaC (client DHCPv4) qui reçoit l'option PAA DHCPv4 DEVRAIT utiliser l'adresse IP (la liste des adresses) pour localiser les PAA.

7. Considérations sur la sécurité

Les considérations sur la sécurité des [RFC2131], [RFC2132], et [RFC3315] s'appliquent. Si un adversaire s'arrange pour modifier la réponse d'un serveur DHCP ou insérer sa propre réponse, un client PANA pourrait être conduit à contacter un agent d'authentification PANA félon, qui peut éventuellement intercepter les demandes d'authentification et/ou dénier l'accès au réseau à l'appareil d'accès.

Dans la plupart des réseaux, l'échange DHCP qui livre les options avant l'authentification de l'accès réseau n'est ni protégé en intégrité ni d'origine authentifiée. Donc, les options définies dans le présent document NE DOIVENT PAS être utilisées pour effectuer de négociation sur l'utilisation de PANA entre le client PANA et un agent d'authentification PANA. Utiliser la présence (ou l'absence) de ces options DHCP comme l'indication de l'obligation de l'authentification (ou non) PANA est un exemple d'un tel mécanisme de négociation. Cette négociation permettrait des attaques en dégradation en faisant choisir aux clients un mécanisme de sécurité dégradé (ou même pas de sécurité du tout).

8. Remerciements

Nous tenons à remercier Ralph Droms, Stig Venaas, Ted Lemon, Andre Kostur et Bernie Volz de leurs précieux commentaires. Merci aussi à Jari Arkko, Thomas Narten et Bernard Aboba qui ont effectué plusieurs relectures, ainsi que tous les membres des groupes de travail PANA et DHC qui ont contribué à améliorer ce document.

9. Références

9.1 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](#))
- [RFC2131] R. Droms, "Protocole de [configuration dynamique d'hôte](#)", mars 1997. (DS) (Mà J par [RFC3396](#), [RFC4361](#), [RFC5494](#), et [RFC6849](#))
- [RFC2132] S. Alexander et R. Droms, "Options DHCP et [Extensions de fabricant BOOTP](#)", mars 1997.
- [RFC3315] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins et M. Carney, "Protocole de [configuration dynamique d'hôte](#) pour IPv6 (DHCPv6)", juillet 2003. (MàJ par [RFC6422](#) et [RFC6644](#), [RFC7227](#) ; *rendue obsolète par [RFC8415](#)*)
- [RFC5191] D. Forsberg et autres, "[Protocole pour porter l'authentification d'accès](#) au réseau (PANA)", mai 2008. (MàJ par [RFC5872](#)) (P.S.)

9.2 Références pour information

- [RFC3748] B. Aboba et autres, "[Protocole extensible d'authentification](#) (EAP)", juin 2004. (P.S., MàJ par [RFC5247](#))

Adresse des auteurs

Suraj Kumar
Tech Mahindra Ltd
mél : surajk@techmahindra.com

Syam Madanapalli
Samsung
mél : syam@samsung.com

Lionel Morand
France Telecom R&D

mél : lionel.morand@orange-ftgroup.com

Alper E. Yegin

Samsung

mél : a.yegin@partner.samsung.com

Déclaration complète de droits de reproduction

Copyright (C) The IETF Trust (2008).

Le présent document est soumis aux droits, licences et restrictions contenus dans le BCP 78, et à www.rfc-editor.org, et sauf pour ce qui est mentionné ci-après, les auteurs conservent tous leurs droits.

Le présent document et les informations contenues sont fournis 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 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.