Groupe de travail Réseau
Request for Comments : 4014
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

R. Droms & J. Schnizlein
Cisco Systems

février 2005

Sous option d'attributs du service d'authentification distante d'utilisateur appelant (RADIUS) pour l'option d'information d'agent de relais du protocole de configuration dynamique d'hôte (DHCP)

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 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.

Résumé

La sous option Attributs de RADIUS permet à un élément de réseau de passer les attributs d'identification et d'autorisation reçus durant l'authentification RADIUS à un serveur DHCP. Lorsque le serveur DHCP reçoit un message d'un agent de relais contenant une sous option Attributs de RADIUS, il extrait le contenu de la sous option et utilise ces informations pour choisir les paramètres de configuration pour le client.

1. Introduction et fondements

La sous option Attributs de RADIUS pour l'option d'agent de relais DHCP donne un moyen pour permettre à un NAS de passer les attributs obtenus d'un serveur RADIUS à un serveur DHCP [RFC2131]. La norme IEEE 802.1X [IEEE802.1X] est un exemple de mécanisme par lequel un NAS comme un commutateur ou un point d'accès de LAN sans fil peut authentifier l'identité de l'utilisateur d'un appareil avant de lui fournir l'accès réseau de couche 2 avec RADIUS comme service d'authentification, comme spécifié dans la [RFC3580]. Dans l'accès authentifié de IEEE 802.1X, un appareil doit d'abord échanger des accréditifs d'authentification avec le NAS. Le NAS fournit alors ces accréditifs à un serveur RADIUS, qui va finalement envoyer un Access-Accept *(accès accepté)* ou un Access-Reject *(accès rejeté)* en réponse à une demande d'accès. Le NAS, sur la base de la réponse du serveur RADIUS, permet ou refuse alors l'accès réseau de l'appareil demandeur.

La Figure 1 résume l'échange de messages entre les participants dans l'authentification IEEE 802.1X.

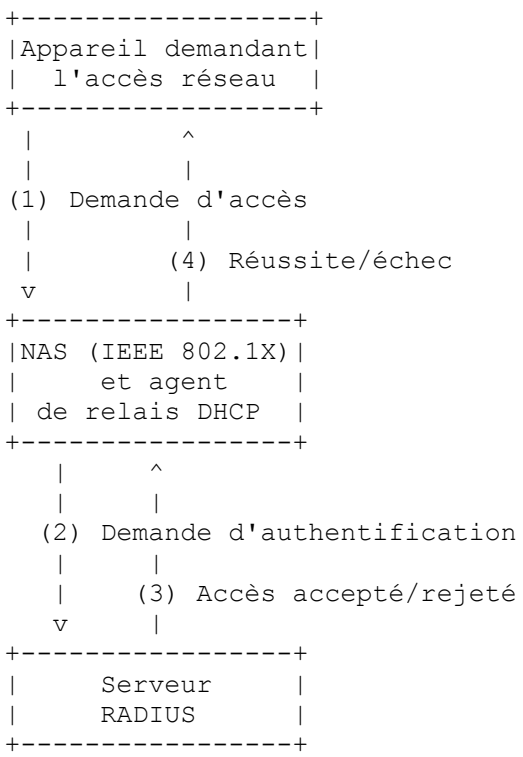

Figure 1

L'appareil d'accès agit comme un authentificateur IEEE 802.1X et ajoute une option d'agent de relais DHCP qui comporte une sous option Attributs RADIUS aux messages DHCP. À la conclusion réussie de l'authentification IEEE 802.1X, un Access-Accept RADIUS fournit les attributs pour les autorisations de service au NAS. Le NAS mémorise ces attributs en local. Lorsque le NAS relaie ensuite les messages DHCP provenant de l'appareil réseau, le NAS ajoute ces attributs dans une sous option Attributs RADIUS. La sous option Attributs RADIUS est une autre sous option de l'option Informations d'agent de relais [RFC3046].

La sous option Attributs RADIUS décrite dans le présent document ne se limite pas à une utilisation en conjonction avec IEEE 802.1X et peut être utilisée pour porter des attributs RADIUS obtenus par l'agent de relais pour n'importe quelles raisons. C'est-à-dire que l'option ne se limite pas à l'utilisation avec IEEE 802.1X mais est contrainte par la sémantique de RADIUS (voir la Section 4).

Le domaine d'applicabilité de la présente spécification est tel qu'une interopérabilité robuste n'est garantie que pour les mises en œuvre de service RADIUS qui existent dans la même portée que la mise en œuvre de service DHCP, c'est-à-dire, au sein d'un seul domaine administratif localisé. L'interopérabilité mondiale de cette spécification à travers les domaines administratifs n'est pas exigée.

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].

Dans la présente spécification, l'utilisation des mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" se rapporte aux clients et serveurs RADIUS qui mettent en œuvre les caractéristiques facultatives de cette spécification. L'utilisation de ces mots clés ne crée aucune exigence normative en dehors de cette portée, et ne modifie pas la spécification RADIUS de base comme la [RFC2865].

2.1 Terminologie DHCP

Les termes suivants sont utilisés comme défini dans la RFC 2131 et la RFC 3046 : agent de relais DHCP, serveur DHCP, client DHCP.

2.2 Terminologie RADIUS

Les termes suivants sont utilisés en conjonction avec RADIUS :

Serveur RADIUS : un serveur RADIUS est chargé de recevoir les demandes de connexion d'utilisateur, d'authentifier l'utilisateur, et ensuite de retourner toutes les informations de configuration nécessaires pour que le client rende le service à l'utilisateur.

Attribut : triplet Type-Longueur-Valeur qui encapsule des éléments de données, comme défini dans la [RFC2865].

NAS *(Network Access Server)* : un serveur d'accès réseau donne l'accès au réseau et fonctionne comme un client de RADIUS. Le client est chargé de passer les informations d'utilisateur aux serveurs RADIUS désignés et ensuite d'agir sur la réponse qui est retournée. À la différence du NAS commuté traditionnel, le NAS considéré ici peut n'avoir pas un protocole comme PPP par lequel il peut passer les informations de configuration des attributs RADIUS au client.

2.3 Terminologie IEEE 802.1X

Les termes suivants sont utilisés comme défini dans le protocole IEEE 802.1X : Authentificateur, Solliciteur.

3. Format de souscription d'attribut RADIUS

La sous option Attributs RADIUS est une nouvelle sous option pour l'option Agent de relais DHCP.

Le format de la sous option Attributs RADIUS est comme suit :

Code de sous option Longueur Attributs RADIUS

```
+------------+-------+------+------+------+------+--...-+------+
|     7      |   N   |  o1  |  o2  |  o3  |  o4  |      |  oN  |
+------------+-------+------+------+------+------+--...-+------+
```

Les attributs RADIUS sont codés conformément aux règles de codage de la RFC 2865, en octets o1...oN.

L'agent de relais DHCP tronque les attributs RADIUS pour tenir dans la sous option Attributs RADIUS.

4. Comportement de l'agent de relais DHCP

Lorsque l'agent de relais DHCP reçoit un message DHCP du client, il PEUT ajouter une option Informations d'agent de relais DHCP contenant la sous option Attributs RADIUS, ainsi que toutes les autres sous options qu'il est configuré à fournir. La sous option Attributs RADIUS DOIT seulement contenir les attributs fournis dans le message RADIUS Access/Accept. L'agent de relais DHCP NE DOIT PAS ajouter plus d'une sous option Attributs RADIUS dans un message.

L'agent de relais DOT inclure les attributs User-Name *(nom d'utilisateur* et Framed-Pool *(réservoir structuré)* dans la sous option Attributs RADIUS, si ils sont disponibles, et PEUT inclure d'autres attributs.

Pour éviter des interactions entre l'allocation d'adresse et les autres informations d'état entre le serveur RADIUS et le serveur DHCP, l'agent de relais DHCP DEVRAIT inclure seulement les attributs du tableau ci-dessous dans une instance de sous option Attributs RADIUS. Le tableau, fondé sur l'analyse de la [RFC3580], fait la liste des attributs qui PEUVENT être inclus :

N°	**Attribut**
1	User-Name *(nom d'utilisateur)* [RFC2865]
6	Service-Type *(type de service)* [RFC 2865]
26	Vendor-Specific *(spécifique du fabricant)* [RFC2865]
27	Session-Timeout *(fin de temporisation de session)* [RFC2865]
88	Framed-Pool *(réservoir structuré)* [RFC 2869]
100	Framed-IPv6-Pool *(réservoir IPv6 structuré)* [RFC3162]

5. Comportement du serveur DHCP

Lorsque le serveur DHCP reçoit un message d'un agent de relais contenant une sous option Attributs RADIUS, il extrait le contenu de la sous option et utilise ces informations pour choisir les paramètres de configuration pour le client. Si l'agent de relais relaye des attributs RADIUS qui ne sont pas inclus dans le tableau de la Section 4, le serveur DHCP DEVRAIT les ignorer. Si le serveur DHCP utilise des attributs non spécifiés ici, il peut en résulter des effets collatéraux non prévus par les spécifications RADIUS existantes.

6. Comportement du client DHCP

Les options d'agent de relais ne sont échangées qu'entre les agents de relais et le serveur DHCP, de sorte que les clients DHCP ne sont jamais informés de leur utilisation.

7. Considérations sur la sécurité

L'authentification de message dans DHCP pour l'utilisation intra domaine lorsque l'échange hors bande d'un secret partagé est faisable, est définie dans la [RFC3118]. Le potentiel d'exposition aux attaques est discuté à la Section 7 de la spécification du protocole DHCP dans la [RFC2131].

L'option d'agent de relais DHCP dépend d'une relation de confiance entre l'agent de relais DHCP et le serveur, comme décrit à la Section 5 de la [RFC3046]. Bien que l'introduction d'options d'agent de relais frauduleuses puisse être empêchée par un périmètre de défense qui bloque ces options sauf si l'agent de relais est de confiance, une défense plus en profondeur utilisant l'option d'authentification pour les options d'agent de relais [RFC4030] ou IPsec [Droms] DEVRAIT aussi être déployée.

8. Considérations relatives à l'IANA

L'IANA a alloué la valeur de 7 au code de sous option Information d'agent de relais DHCP pour cette sous option. Le présent document ne définit aucun nouvel espace de noms ni autre constante pour lesquels l'IANA doit tenir un registre.

9. Remerciements

Nous remercions de leur avis d'expert Bernard Aboba, Paul Funk, David Nelson, Ashwin Palekar, et Greg Weber qui nous ont éviter de compliquer RADIUS.

10. Références

10.1 Références normatives

[IEEE802.1X] Institute of Electrical and Electronics Engineers, "Local and Metropolitan Area Networks: Port based Network Access Control", IEEE Standard 802.1X, mars 2001.

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

[RFC2131] R. Droms, "Protocole de configuration dynamique d'hôte", mars 1997. *(DS) (Mà J par* RFC3396, RFC4361, RFC5494, et RFC6849)

[RFC2865] C. Rigney et autres, "Service d'authentification à distance de l'utilisateur appelant (RADIUS)", juin 2000. (*MàJ par* RFC2868, RFC3575, RFC5080) *(D.S.)*

[RFC3046] M. Patrick, "Option DHCP Information d'agent de relais", janvier 2001. (*MàJ par* RFC6607)

10.2 Références pour information

[RFC2869] C. Rigney, W. Willats, P. Calhoun, "Extensions à RADIUS", juin 2000. (*MàJ par* RFC3579, RFC5080) *(Info.)*

[RFC3118] R. Droms et W. Arbaugh, "Authentification des messages DHCP", juin 2001. *(P.S.)*

[RFC3162] B. Aboba, G. Zorn, D. Mitton, "RADIUS et IPv6", août 2001. *(P.S.)*

[RFC3580] P. Congdon et autres, "Lignes directrices pour l'utilisation du service d'authentification distante d'utilisateur appelant (RADIUS) IEEE 802.1X", septembre 2003. *(Information)*

[RFC4030] M. Stapp, T. Lemon, "Sous-option d'authentification de l'option d'agent de relais pour le protocole de configuration dynamique d'hôte (DHCP)", mars 2005. *(P.S.)*

[Droms] Droms, R., "Authentication of DHCP Relay Agent Options Using IPsec", Travail en cours, septembre 2003.

Adresse des auteurs

Ralph Droms
Cisco Systems
1414 Massachusetts Avenue
Boxborough, MA 01719
USA
mél : rdroms@cisco.com

John Schnizlein
Cisco Systems
9123 Loughran Road
Fort Washington, MD 20744
USA
mél : jschnizl@cisco.com

Déclaration complète de droits de reproduction

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