Groupe de travail Réseau
Request for Comments : 4675
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

P. Congdon, Cisco Systems, Inc.
M. Sanchez, Hewlett-Packard Company
B. Aboba, Microsoft Corporation
septembre 2006

Attributs RADIUS pour la prise en charge de LAN virtuel et de priorité

Résumé
Le présent document propose des attributs supplémentaires au service d'authentification à distance de l'utilisateur appelant (RADIUS, *Remote Authentication Dial-In User Service*) pour l'allocation dynamique de LAN virtuel et de priorités, à utiliser pour provisionner l'accès aux réseaux de zone locale IEEE 802. Ces attributs sont utilisables dans RADIUS ou Diameter.

Table des matières

1. Introduction

Le présent document décrit des attributs de LAN virtuel (VLAN, *Virtual LAN*) et de reprioritisation qui peuvent se révéler utiles pour provisionner l'accès aux réseaux de zone locale IEEE 802 [IEEE-802] avec les services d'authentification à distance de l'utilisateur appelant (RADIUS, *Remote Authentication Dial-In User Service*) ou Diameter.

Bien que la [RFC3580] permette la prise en charge de l'allocation de VLAN sur la base des attributs de tunnel définis dans la [RFC2868], elle ne fournit pas de prise en charge d'un ensemble plus complet de fonctionnalités de VLAN définies par [IEEE-802.1Q]. Ces attributs qui sont définis dans le présent document fournissent au sein de RADIUS et Diameter une prise en charge analogue aux variables de gestion prises en charge dans [IEEE-802.1Q] et aux objets de MIB définis dans la [RFC4363]. De plus, le présent document permet la prise en charge d'une gamme plus large de configurations de [IEEE-802.1X].

1.1 Terminologie

Ce document utilise les termes suivants :

Serveur d'accès réseau (NAS, *Network Access Server*) : appareil qui fournit un service d'accès au réseau à un utilisateur. Aussi appelé un client RADIUS.

Serveur RADIUS : un serveur d'authentification RADIUS est une entité qui fournit un service d'authentification à un NAS.

Mandataire RADIUS : il agit comme serveur d'authentification pour le NAS, et comme client RADIUS pour le serveur RADIUS.

1.2 Langage des exigences

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].

1.3 Interprétation des attributs

Les attributs décrits dans ce document s'appliquent à une seule instance d'un accès de NAS, ou plus précisément un accès de pont IEEE 802.1Q. [IEEE-802.1Q], [IEEE-802.1D], et [IEEE-802.1X] ne reconnaissent pas de granularité de gestion plus fine que "par accès". Dans certains cas, comme celui des LAN sans fil IEEE 802.11, le concept d'un "accès virtuel" est utilisé à la place de l'accès physique. De tels accès virtuels sont normalement fondés sur des associations de sécurité et ont une portée par station, ou adresse de contrôle d'accès de support (MAC, *Media Access Control*).

Les attributs définis dans le présent document sont appliqués utilisateur par utilisateur et il est prévu qu'il y ait un seul utilisateur par accès ; cependant, dans certains cas cet accès peut être un "accès virtuel". Si une mise en œuvre de NAS conforme au présent document prend en charge les "accès virtuels", il est possible de provisionner ces "accès virtuels" avec des valeurs uniques des attributs décrits dans le présent document, permettant que plusieurs utilisateurs partagent le même accès physique pour chacun de ceux qui ont un ensemble unique de paramètres d'autorisation.

Si un NAS conforme à la présente spécification reçoit un paquet Access-Accept contenant un attribut défini dans le présent document qu'il ne peut pas appliquer, il DOIT agir comme si il avait reçu un Access-Reject. La [RFC3576] exige qu'un NAS qui reçoit une demande de changement d'autorisation (CoA-Request) réponde avec un CoA-NAK si la demande contenait un attribut non pris en charge. Il est recommandé qu'un attribut Error-Cause avec la valeur réglée à "Attribut non pris en charge" (401) soit inclus dans le CoA-NAK. Comme noté dans la [RFC3576], les changements d'autorisation sont atomiques, de sorte que cette situation ne résulte pas en une terminaison de session et que la configuration pré existante reste inchangée. Par suite, aucun paquet de comptabilité ne devrait être généré.

2. Attributs

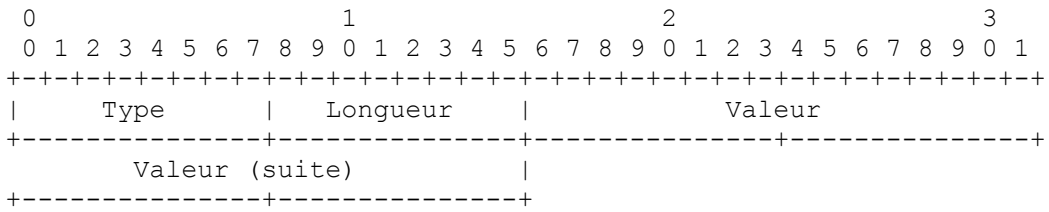
2.1 Egress-VLANID

Description : l'attribut Egress-VLANID représente un identifiant de VLAN de sortie IEEE 802 permis pour cet accès, indiquant si le VLANID est permis pour les trames étiquetées ou non ainsi que pour le VLANID.

Comme défini dans la [RFC3580], le VLAN alloué via les attributs de tunnel s'applique à la fois au VLANID d'entrée pour les paquets non étiquetés (appelé le PVID) et au VLANID de sortie pour les paquets non étiquetés. À l'opposé, l'attribut Egress-VLANID configure seulement le VLANID de sortie pour les paquets étiquetés ou non étiquetés. L'attribut Egress-VLANID PEUT être inclus dans le même paquet RADIUS que les attributs de tunnel de la [RFC3580] ; cependant, l'attribut Egress-VLANID n'est pas nécessaire si il est utilisé pour configurer le même VLANID non étiqueté inclus dans les attributs de tunnel. Pour configurer un VLAN non étiqueté pour l'entrée et la sortie, les attributs de tunnel de la [RFC3580] DOIVENT être utilisés.

Plusieurs attributs Egress-VLANID PEUVENT être inclus dans les paquets Access-Request, Access-Accept, CoA-Request, ou Accounting-Request ; cet attribut NE DOIT PAS être envoyé dans un Access-Challenge, Access-Reject, Disconnect-Request, Disconnect-ACK, Disconnect-NAK, CoA-ACK, ou CoA-NAK. Chaque attribut ajoute le VLAN spécifié à la liste des VLAN de sortie permis pour l'accès.

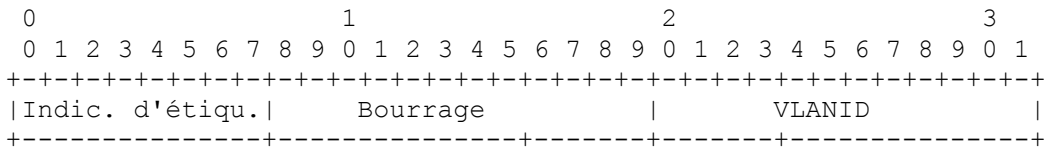
L'attribut Egress-VLANID est montré ci-dessous. Les champs sont transmis de gauche à droite :



Type : 56

Longueur : 6

Valeur : le champ Valeur fait quatre octets. Le format est décrit ci-dessous :

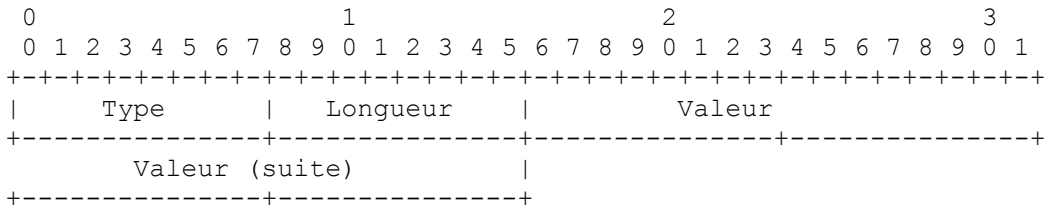


Le champ Indication d'étiquette fait un octet et indique si les trames sur le VLAN sont étiquetées (0x31) ou non étiquetées (0x32). Le champ Bourrage fait 12 bits et DOIT être 0 (zéro). Le VLANID est long de 12 bits et contient la valeur de l'identifiant de VLAN [IEEE-802.1Q].

2.2 Ingress-Filters

Description : l'attribut Ingress-Filters correspond à la variable Ingress Filter par accès définie au paragraphe 8.4.5 de [IEEE-802.1Q]. Quand l'attribut a la valeur "Activé", l'ensemble de VLAN qui sont admis à entrer sur un accès doit correspondre à l'ensemble des VLAN qui sont admis à sortir d'un accès. Un seul attribut Ingress-Filters PEUT être envoyé au sein d'un paquet Access-Request, Access-Accept, CoA-Request, ou Accounting-Request ; cet attribut NE DOIT PAS être envoyé au sein d'un Access-Challenge, Access-Reject, Disconnect-Request, Disconnect-ACK, Disconnect-NAK, CoA-ACK, ou CoA-NAK.

L'attribut Ingress-Filters est montré ci-dessous. Les champs sont transmis de gauche à droite :



Type : 57

Longueur : 6

Valeur : le champ Valeur fait quatre octets. Les valeurs acceptées incluent :
1 - Activé
2 - Désactivé

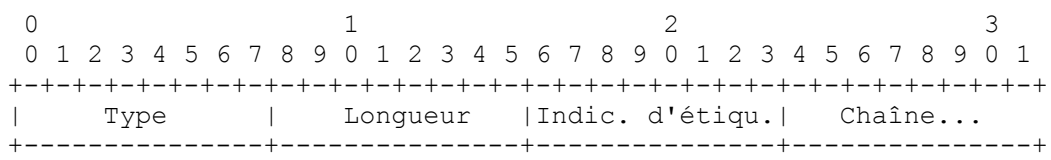
2.3 Egress-VLAN-Name

Description : le paragraphe 12.10.2.1.3 (a) de [IEEE-802.1Q] décrit les noms de VLAN alloués administrativement associés à un identifiant de VLAN défini dans un pont IEEE 802.1Q. L'attribut Egress-VLAN-Name représente un VLAN permis pour cet accès. Il est similaire à l'attribut Egress-VLANID, sauf que le VLAN-ID lui-même n'est pas spécifié ou connu ; le nom du VLAN est plutôt utilisé pour identifier le VLAN au sein du système.

Les attributs de tunnel décrits dans la [RFC3580] et l'attribut Egress-VLAN-Name peuvent tous deux être utilisés pour configurer le VLAN de sortie pour les paquets non étiquetés. Ces attributs peuvent être utilisés concurremment et PEUVENT apparaître dans le même paquet RADIUS. Quand ils apparaissent concurremment, la liste des VLAN permis est l'enchaînement des attributs Egress-VLAN-Name et Tunnel-Private-Group-ID (81). L'attribut Egress-VLAN-Name n'altère pas le VLAN d'entrée pour le trafic non étiqueté sur un accès (aussi appelé le PVID). On devrait s'appuyer sur les attributs de tunnel provenant de la [RFC3580] plutôt que d'établir le PVID.

L'attribut Egress-VLAN-Name contient deux parties ; la première partie indique si les trames sur le VLAN pour cet accès sont à représenter en format étiqueté ou non étiqueté ; la seconde partie est le nom du VLAN.

Plusieurs attributs Egress-VLAN-Name PEUVENT être inclus dans un paquet Access-Request, Access-Accept, CoA-Request, ou Accounting-Request ; cet attribut NE DOIT PAS être envoyé dans un Access-Challenge, Access-Reject, Disconnect-Request, Disconnect-ACK, Disconnect-NAK, CoA-ACK, ou CoA-NAK. Chaque attribut ajoute le VLAN désigné à la liste des VLAN de sortie permis pour l'accès. L'attribut Egress-VLAN-Name est montré ci-dessous. Le champs sont transmis de gauche à droite :



Type : 58

Longueur : ≥ 4

Indication d'étiquette : le champ Indication d'étiquette fait un octet et indique si les trames sur le VLAN sont étiquetées (0x31, ASCII "1") ou non étiquetées (0x32, ASCII "2"). Ces valeurs ont été choisies afin de les rendre plus faciles à entrer par les utilisateurs.

Chaîne : le champ Chaîne est au moins d'un octet et contient le nom de VLAN comme défini au paragraphe 12.10.2.1.3 (a) de [IEEE-802.1Q]. Les caractères codés en UTF-8 [RFC3629] sont RECOMMANDÉS, mais une mise en œuvre robuste DEVRAIT accepter le champ comme des octets non distingués.

2.4 User-Priority-Table

Description : le paragraphe 7.5.1 de [IEEE-802.1D] discute de la façon de régénérer (ou retransposer) la priorité d'utilisateur sur les trames reçues à un accès. Cette configuration par accès permet à un pont de causer la transposition de priorité du trafic reçu à un accès en une priorité particulière. Le paragraphe 6.3.9 de [IEEE-802.1D] décrit l'utilisation de la retransposition :

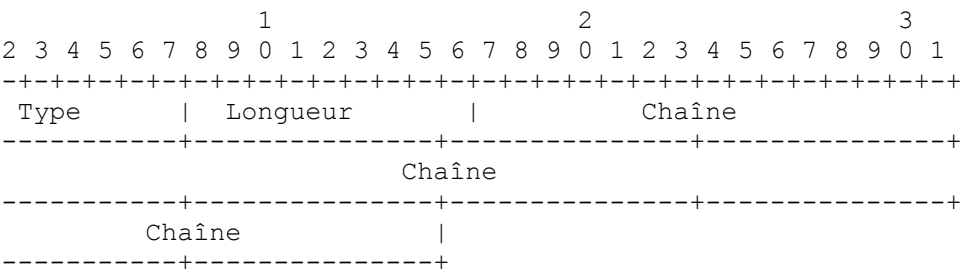
> La capacité de signaler la priorité d'utilisateur dans les LAN IEEE 802 permet à la priorité d'utilisateur d'être portée avec une signification de bout en bout à travers un réseau de zone locale ponté. Ceci, couplé avec une approche cohérente de la transposition de la priorité d'utilisateur en classes de trafic et de priorité d'utilisateur en priorité d'accès, permet une utilisation cohérente des informations de priorité, en accord avec les capacités des ponts et des MAC dans le chemin de transmission ...
>
> Dans des circonstances normales, la priorité d'utilisateur n'est pas modifiée dans le transit à travers la fonction de relais d'un pont ; cependant, la gestion de réseau peut contrôler comment la priorité d'utilisateur est propagée. Le Tableau 7-1 donne la capacité de transposer les valeurs de priorité d'utilisateur entrantes accès par accès. Par défaut, la priorité d'utilisateur régénérée est identique à la priorité d'utilisateur entrante.

Cet attribut représente la priorisation de IEEE 802 qui va être appliquée aux trames arrivant à cet accès. Il y a huit priorités d'utilisateur possibles, selon la norme [IEEE-802]. Le paragraphe 14.6.2.3.3 de [IEEE-802.1D] spécifie le tableau de régénération comme 8 valeurs, chacune étant un entier dans la gamme de 0 à 7. Les variables de gestion sont décrites au paragraphe 14.6.2.2.

Un seul attribut User-Priority-Table PEUT être inclus dans un paquet Access-Accept ou CoA-Request ; cet attribut NE DOIT PAS être envoyé dans un Access-Request, Access-Challenge, Access-Reject, Disconnect-Request, Disconnect-ACK,

Disconnect-NAK, CoA-ACK, CoA-NAK ou Accounting-Request. Comme le tableau de régénération est seulement tenu par un pont conforme à [IEEE-802.1D], cet attribut devrait seulement être envoyé à un client RADIUS qui prend en charge la présente spécification.

L'attribut User-Priority-Table est montré ci-dessous. Les champs sont transmis de gauche à droite :



Type : 59

Longueur : 10

Chaîne : le champ Chaîne fait 8 octets et inclut un tableau qui transpose la priorité entrante (si il est établi – la valeur par défaut est 0) en une des huit priorités régénérées. Le premier octet se transpose en la priorité entrante de 0, le second octet en la priorité entrante de 1, etc. Les valeurs dans chaque octet représentent la priorité régénérée de la trame.
Il est donc possible soit de retransposer les priorités entrantes en valeurs plus appropriées ; pour respecter les priorités entrantes; ou pour outre passer une priorités entrante, les forçant à toutes se transposer en une seule priorité choisie.
L'Annexe G de la spécification [IEEE-802.1D] donne une description utile des transpositions de type de trafic en classe de trafic.

3. Tableau des attributs

Le tableau suivant est un guide sur quels attributs peuvent être trouvés dans quels types de paquets, et en quelle quantité.

Access-Request	Access-Accept	Access-Reject	Access-Challenge	CoA-Req	Acct-Req	n°	Attribut
0+	0+	0	0	0+	0+	56	Egress-VLANID
0-1	0-1	0	0	0-1	0-1	57	Ingress-Filters
0+	0+	0	0	0+	0+	58	Egress-VLAN-Name
0	0-1	0	0	0-1	0	59	User-Priority-Table

La signification des entrées du tableau ci-dessus est la suivante :
0 : cet attribut NE DOIT PAS être présent dans le paquet.
0+ : zéro, une ou plusieurs instances de cet attribut PEUVENT être présentes dans le paquet.
0-1 : zéro ou une instance de cet attribut PEUT être présente dans le paquet.

4. Considérations sur Diameter

Quand ils sont utilisés dans Diameter, les attributs définis dans la présente spécification peuvent être utilisés comme des paires d'attribut-valeur (AVP) Diameter à partir de l'espace de codes 1 à 255 (espace de compatibilité d'attribut RADIUS). Aucune valeur supplémentaire de code Diameter n'est donc allouée. Les règles de types de données et de fanions pour les attributs sont les suivantes :

		Règles de fanion d'AVP				
Nom d'attribut	**Type de valeur**	**DOIT**	**PEUT**	**NE DEVRAIT PAS**	**NE DOIT PAS**	**Chiffrement**
Egress-VLANID	OctetString	Oblig.	Peut	-	V	Oui
Ingress-Filters	Enumerated	Oblig.	Peut	-	V	Oui
Egress-VLAN-Name	UTF8String	Oblig.	Peut	-	V	Oui
User-Priority-Table	OctetString	Oblig.	Peut	-	V	Oui

(Note du traducteur : le V dans la colonne NE DOIT PAS signifie que le fanion V ne doit pas être établi dans cet attribut)

Les attributs dans la présente spécification n'ont pas d'exigence de traduction particulière pour les passerelles de Diameter en RADIUS ou de RADIUS en Diameter ; ils sont copiés tels quels, sauf pour les changements relatifs aux en-têtes, à l'alignement, et au bourrage. Voir aussi le paragraphe 4.1 de la [RFC3588] et la Section 9 de la [RFC4005].

Ce que dit la présente spécification sur l'applicabilité des attributs pour les paquets RADIUS Access-Request s'applique dans Diameter à AA-Request [RFC4005] ou Diameter-EAP-Request [RFC4072]. Ce qui est dit sur Access-Challenge s'applique dans Diameter à AA-Answer [RFC4005] ou Diameter-EAP-Answer [RFC4072] avec l'AVP Code de résultat réglé à DIAMETER_MULTI_ROUND_AUTH.

Ce qui est dit sur Access-Accept s'applique dans Diameter aux messages AA-Answer ou Diameter-EAP-Answer qui indiquent le succès. De même, ce qui est dit sur les paquets RADIUS Access-Reject s'applique dans Diameter aux messages AA-Answer ou Diameter-EAP-Answer qui indiquent l'échec.

Ce qui est dit de COA-Request s'applique dans Diameter à Re-Auth-Request [RFC4005].
Ce qui est dit de Accounting-Request s'applique aussi dans le Accounting-Request [RFC4005] de Diameter.

5. Considérations relatives à l'IANA

La présente spécification ne crée aucun nouveau registre.

Le présent document utilise l'espace de noms de RADIUS [RFC2865] ; voir <http://www.iana.org/assignments/radius-types>. L'allocation de quatre mises à jour de la Section "Types d'attributs RADIUS" a été faite par l'IANA. Les attributs RADIUS sont :

56 - Egress-VLANID
57 - Ingress-Filters
58 - Egress-VLAN-Name
59 - User-Priority-Table

6. Considérations sur la sécurité

La présente spécification décrit l'utilisation de RADIUS et Diameter pour les besoins de l'authentification, autorisation, et comptabilité dans les réseaux de zone locale IEEE 802. Les questions de menaces et de sécurité de RADIUS pour cette application sont décrites dans les [RFC3579] et [RFC3580] ; les questions de sécurité rencontrées en itinérance sont décrites dans la [RFC2607]. Pour Diameter, les questions de sécurité relatives à cette application sont décrites dans les [RFC4005] et [RFC4072].

Le présent document spécifie de nouveaux attributs qui peuvent être inclus dans les paquets RADIUS existants, qui sont protégés comme décrit dans les [RFC3579] et [RFC3576]. Dans Diameter, les attributs sont protégés comme spécifié dans la [RFC3588]. Voir ces documents pour une description plus détaillée.

Les mécanismes de sécurité pris en charge dans RADIUS et Diameter se concentrent sur la prévention des attaques par usurpation de paquets ou modification des paquets en transit. Ils n'empêchent pas un serveur ou mandataire RADIUS/Diameter autorisé d'insérer des attributs dans une intention malveillante.

Les attributs de VLAN envoyés par un serveur ou mandataire RADIUS/Diameter peuvent permettre l'accès à des VLAN non autorisés. Cette vulnérabilité peut être limitée en effectuant des vérifications d'autorisation au NAS. Par exemple, un NAS peut être configuré à n'accepter que certains identifiants de VLAN d'un certain serveur/mandataire RADIUS/Diameter.

De même, un attaquant qui obtient le contrôle d'un serveur ou mandataire RADIUS/Diameter peut modifier le tableau de priorité d'utilisateur, causant soit la dégradation de la qualité de service (en dégradant la priorité d'utilisateur des trames qui arrivent à un accès) soit un déni de service (en élevant le niveau de priorité du trafic à plusieurs accès d'un appareil, submergeant les capacités du commutateur ou de la liaison).

7. Références

7.1 Références normatives

[IEEE-802] "IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture", ANSI/IEEE Std 802, 1990.

[IEEE-802.1D] "IEEE Standards for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges", IEEE Std 802.1D-2004, juin 2004.

[IEEE-802.1Q] "IEEE Standards for Local and Metropolitan Area Networks: Draft Standard for Virtual Bridged Local Area Networks", P802.1Q-2003, janvier 2003.

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

[RFC2865] C. Rigney et autres, "Service d'authentification à distance de l'utilisateur appelant (RADIUS)", juin 2000. (*MàJ par* RFC2868, RFC3575, RFC5080, RFC8044) *(D.S.)*

[RFC3588] P. Calhoun et autres, "Protocole fondé sur Diameter", septembre 2003. (*Remplacée par la* RFC6733) *(P.S.)*

[RFC3629] F. Yergeau, "UTF-8, un format de transformation de la norme ISO 10646", STD 63, novembre 2003.

[RFC4363] D. Levi, D. Harrington, "Définitions des objets gérés pour Bridges avec extensions de classes de trafic, filtrage de diffusion groupée et LAN virtuel", janvier 2006. (*Remplace* RFC2674) *(P.S.)*

7.2 Références pour information

[IEEE-802.1X] "IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control", IEEE Std 802.1X-2004, décembre 2004.

[RFC2607] B. Aboba, J. Vollbrecht, "Chaînage de mandataire et mise en œuvre de politique dans l'itinérance", juin 1999. *(Info.)*

[RFC2868] G. Zorn et autres, "Attributs RADIUS pour la prise en charge du protocole de tunnel", juin 2000. *(Information)*

[RFC3576] M. Chiba et autres, "Extensions d'autorisation dynamique au service d'authentification distante d'utilisateur appelant (RADIUS)", juillet 2003. (*Obsolète, voir* RFC5176) *(Information)*

[RFC3579] B. Aboba, P. Calhoun, "Prise en charge du protocole d'authentification extensible (EAP) par RADIUS", septembre 2003. (*MàJ par* RFC5080) *(Information)*

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

[RFC4005] P. Calhoun et autres, "Application de serveur d'accès réseau Diameter", août 2005. *(P.S.) (Remplacée par* RFC7155)

[RFC4072] P. Eronen et autres, "Application Diameter du protocole d'authentification extensible (EAP)", août 2005. *(P.S. ; MàJ par* RFC8044)

8. Remerciements

Les auteurs tiennent à remercier Joseph Salowey de Cisco, David Nelson de Enterasys, Chuck Black de Hewlett-Packard, et Ashwin Palekar de Microsoft.

Adresse des auteurs

Paul Congdon
Hewlett-Packard Company
HP ProCurve Networking
8000 Foothills Blvd, M/S 5662
Roseville, CA 95747
téléphone : +1 916 785 5753
Fax : +1 916 785 8478
mél : paul.congdon@hp.com

Mauricio Sanchez
Hewlett-Packard Company
HP ProCurve Networking
8000 Foothills Blvd, M/S 5559
Roseville, CA 95747
téléphone : +1 916 785 1910
Fax : +1 916 785 1815
mél : mauricio.sanchez@hp.com

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
USA
téléphone : +1 425 706 6605
Fax : +1 425 936 7329
mél : bernarda@microsoft.com

Déclaration complète de droits de reproduction

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