Groupe de travail Réseau
Request for Comments : 3162
Catégorie :En cours de normalisation
Traduction Claude Brière de L'Isle

B. Aboba, Microsoft
G. Zorn, Cisco Systems
D. Mitton, Circular Logic UnLtd.
août 2001

RADIUS et IPv6

Statut du présent mémoire
La présente RFC spécifie un protocole de normalisation pour la communauté Internet et appelle à des discussions et suggestions pour son amélioration. Prière de se reporter à l'édition en cours des "Internet Official Protocol Standards" *(normes officielles de protocole de l'Internet)* (STD 1) pour connaître l'état de la normalisation et le statut du présent protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Le présent document spécifie le fonctionnement du service d'accès commuté entrant d'utilisateur distant (RADIUS, *Remote Authentication Dial In User Service*) lorsque utilisé sur IPv6 ainsi que les attributs RADIUS utilisés pour prendre en charge l'accès réseau IPv6.

Table des Matières

1. Introduction

Le présent document spécifie le fonctionnement de RADIUS [RFC2865]-[RFC2869] sur IPv6 [RFC2460] ainsi que les attributs RADIUS utilisés pour la prise en charge de l'accès réseau IPv6.

Noter qu'un serveur d'accès réseau (NAS, *Network Access Server*) qui envoie une demande d'accès RADIUS peut ne pas savoir à priori si l'hôte va utiliser IPv4, IPv6, ou les deux. Par exemple, dans le protocole point à point PPP, IPv6CP [RFC2472] survient après le protocole de contrôle des liaisons (LCP, *Link Control Protocol*) de sorte que l'allocation d'adresse ne va pas se faire tant que l'authentification et l'autorisation RADIUS ne sont pas achevées.
On suppose donc que les attributs IPv6 décrits dans le présent document PEUVENT être envoyés avec des attributs en rapport avec IPv4 au sein du même message RADIUS et que le NAS va décider quels attributs utiliser. Le NAS DEVRAIT cependant seulement allouer des adresses et préfixes que le client peut réellement utiliser. Par exemple, il n'est pas nécessaire que le NAS réserve l'utilisation d'une adresse IPv4 pour un hôte qui ne prend en charge que IPv6 ; de même, un hôte qui n'utilise que IPv4 ou 6à4 [RFC3056] n'a pas besoin d'allocation de préfixe IPv6.

Le NAS peut fournir de façon native l'accès IPv6, ou autrement, via d'autres méthodes telles que IPv6 dans des tunnels IPv4 [RFC2893] ou 6sur4 [RFC2529]. Le choix de la méthode pour fournir l'accès IPv6 n'a pas d'effet sur l'utilisation de RADIUS en soi, bien que si on désire que soit ouvert un IPv6 dans un tunnel IPv4 pour une localisation particulière, les attributs de tunnel devraient être utilisés, comme décrit dans les [RFC2867] et [RFC2868].

1.1 Langage des exigences

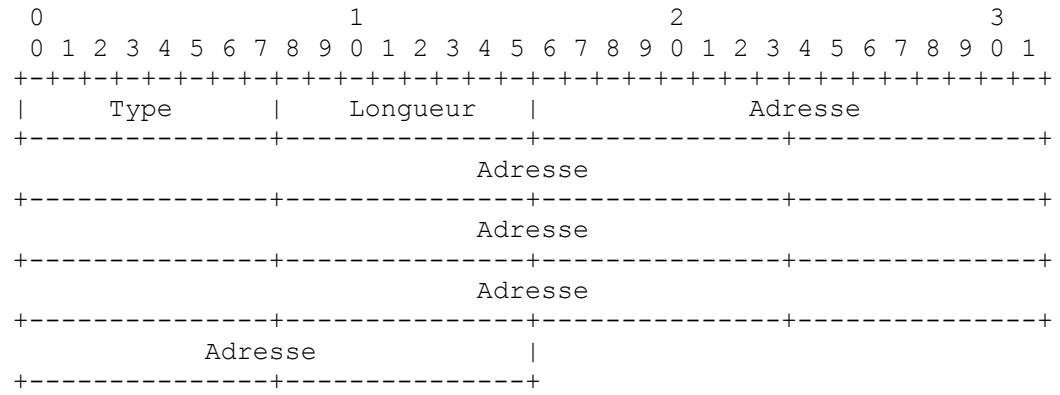
Dans le présent document, les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRAIT" "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" doivent être interprétés comme décrit dans le BCP 14, [RFC2119].

2. Attributs

2.1 NAS-IPv6-Address

Description
Cet attribut indique l'adresse IPv6 qui identifie le NAS qui demande l'authentification de l'usager, et DEVRAIT être unique pour le NAS dans la portée du serveur RADIUS. NAS-IPv6-Address n'est utilisé que dans les paquets de demande d'accès. NAS-IPv6-Address et/ou NAS-IP-Address PEUVENT être présents dans un paquet de demande d'accès ; cependant, si n'y l'un ni l'autre attribut n'est présent, alors NAS-Identifier DOIT être présent.

Le format de l'attribut NAS-IPv6-Address est présenté ci-dessous. Les champs sont transmis de gauche à droite.

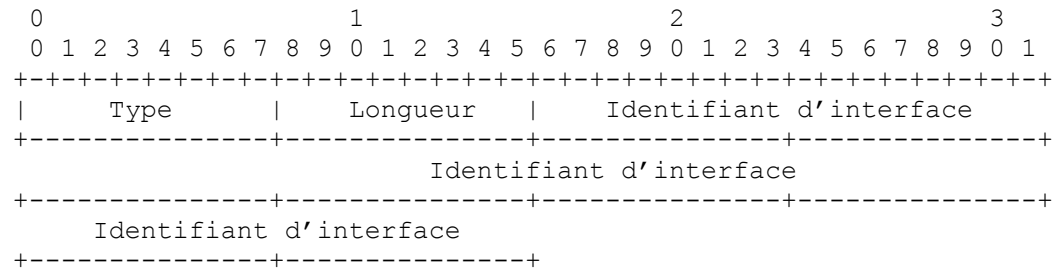


Type : 95 pour NAS-IPv6-Address
Longueur ; 18
Adresse : Le champ Adresse fait 16 octets.

3.2 Framed-Interface-Id

Description
Cet attribut indique l'identifiant d'interface IPv6 à configurer pour l'usager. Il PEUT être utilisé dans les paquets Acceptation d'accès. Si l'option IPv6CP Interface-Identifier [RFC2472] a été négociée avec succès, cet attribut DOIT être inclus dans un paquet Demande d'accès comme indication du NAS au serveur qu'il préfèrerait cette valeur. Il est recommandé, mais pas exigé, que le serveur honore l'indication.

Le format de l'attribut Framed-Interface-Id est donné ci-dessous. Les champs sont transmis de gauche à droite.

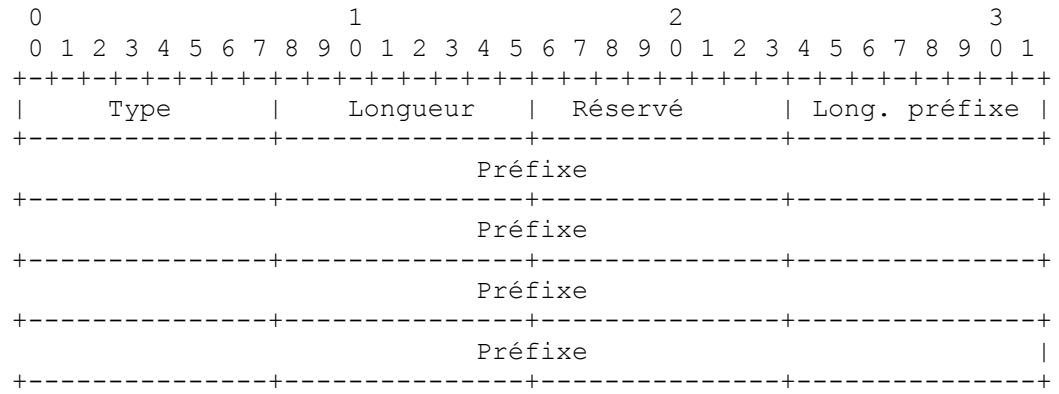


Type : 96 pour Framed-Interface-Id
Longueur : 10
Identifiant d'interface : Le champ Identifiant d'interface fait 8 octets.

2.3 Framed-IPv6-Prefix

Description
Cet attribut indique un préfixe IPv6 (et le chemin correspondant) pour être configuré pour l'usager. Il PEUT être utilisé dans les paquets Acceptation d'accès, et peut apparaître plusieurs fois. Il PEUT être utilisé dans un paquet Demande d'accès comme indication par le NAS au serveur qu'il préfèrerait ces préfixes, mais le serveur n'est pas obligé de suivre ce conseil. Comme on suppoose que le NAS va sonder un chemin correspondant au préfixe, il n'est pas nécessaire que le serveur envoie aussi un attribut Framed-IPv6-Route pour le même préfixe.

Le format de l'attribut Framed-IPv6-Prefix est donné ci-dessous. Les champs sont transmis de gauche à droite.

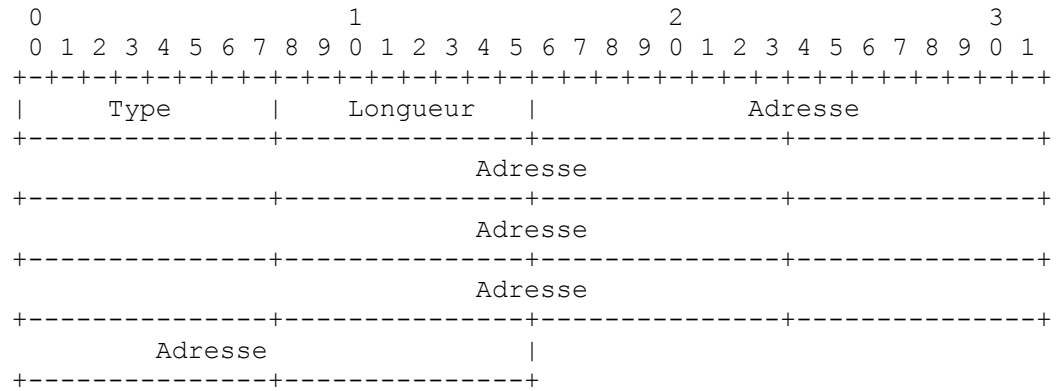


Type : 97 pour Framed-IPv6-Prefix
Longueur : Au moins 4 et pas plus de 20.
Réservé : Ce champ, qui est réservé et DOIT être présent, est toujours réglé à zéro.
Longueur de préfixe : Longueur du préfixe, en bits. Au moins 0 et pas plus de 128.
Préfixe : Le champ Préfixe fait jusqu'à 16 octets. Les bits en plus de la longueur de préfixe, s'il en est d'inclus, doivent être à zéro.

2.4 Login-IPv6-Host

Description
Cet attribut indique le système avec lequel connecter l'usager, quand l'attribut Login-Service est inclus. Il PEUT être utilisé dans les paquets Acceptation d'accès. Il PEUT être utilisé dans un paquet Demande d'accès comme indication au serveur que le NAS préfèrerait utiliser cet hôte, mais le serveur n'est pas obligé de suivre ce conseil.

Le format de l'attribut Login-IPv6-Host est donné ci-dessous. Les champs sont transmis de gauche à droite.

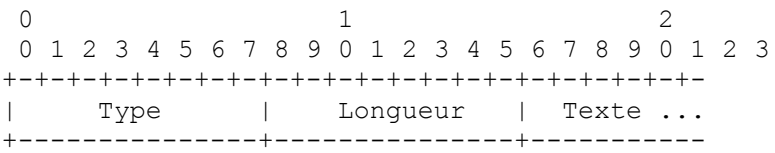


Type : 98 pour Login-IPv6-Host
Longueur : 18
Adresse : Le champ Adresse fait 16 octets. La valeur 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF indique que le NAS DEVRAIT permetre à l'usager de choisir une adresse ou un nom auquel se connecter. La valeur 0 indique que le NAS DEVRAIT choisir un hôte auquel connecter l'usager. Les autres valeurs indiquent l'adresse à laquelle le NAS DEVRAIT connecter l'usager.

2.5 Framed-IPv6-Route

Description
Cet attribut fournit des informations d'acheminement à configurer pour l'usager sur le NAS. Il est utilisé dans le paquet Acceptation d'accès et peut apparaître plusieurs fois.

Le format de l'attribut Framed-IPv6-Route est donné ci-dessous. Les champs sont transmis de gauche à droite.



Type : 99 pour Framed-IPv6-Route
Longueur : ≥ 3
Texte : Le champ Texte fait un ou plusieurs octets, et son contenu dépend de la mise en œuvre. Le champ n'est pas terminé par la valeur NUL (hex 00). Il est destiné à être lisible par l'homme et NE DOIT PAS affecter le fonctionnement du protocole.

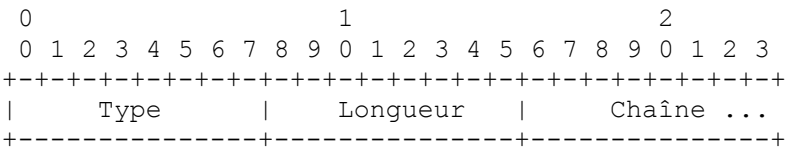
Pour les routeurs IPv6, il DEVRAIT contenir un préfixe de destination facultativement suivi par une barre oblique et la spécification d'une longueur décimale déclarant combien de bits de poids fort du préfixe utiliser. Cela est suivi d'une espace, d'une adresse de passerelle, d'une espace, et d'une ou plusieurs métriques (codées en décimal) séparées par des espaces. Les préfixes et les adresses sont formatés comme décrit dans la [RFC2373]. Par exemple, "2000:0:0:106::/64 2000::106:a00:20ff:fe99:a998 1".

Chaque fois que l'adresse de la passerelle est l'adresse IPv6 inspécifiée , l'adresse IP de l'usager DEVRAIT être utilisée comme adresse de passerelle. L'adresse inspécifiée peut être exprimée dans tout format acceptable décrit dans la [RFC2373]. Par exemple, "2000:0:0:106::/64 :: 1".

2.6 Framed-IPv6-Pool

Description
Cet attribut contient le nom d'un réservoir alloué qui DEVRAIT être utilisé pour allouer un préfixe IPv6 pour l'usager. Si un NAS ne prend pas en charge les réservoirs de plusieurs préfixes, le NAS DOIT ignorer cet attribut.

Le format de l'attribut Framed-IPv6-Pool est donné ci-dessous. Les champs sont transmis de gauche à droite.



Type : 100 pour Framed-IPv6-Pool

Longueur : ≥ 3

Chaîne : Le champ Chaîne contient le nom d'un réservoir de préfixes IPv6 alloués configuré surle NAS. Le champ n'est pas terminé par la valeur NUL (hex 00).

3. Tableau des attributs

Le tableau qui suit indique dans quelle sorte de paquets et en quelle quantité peuvent se trouver les attributs.

Demande	Acceptation	Rejet	Challenge	Demande de comptabilité	n°	Attribut
0-1	0	0	0	0-1	95	NAS-IPv6-Address
0-1	0-1	0	0	0-1	96	Framed-Interface-Id
0+	0+	0	0	0+	97	Framed-IPv6-Prefix
0+	0+	0	0	0+	98	Login-IPv6-Host
0	0+	0	0	0+	99	Framed-IPv6-Route
0	0-1	0	0	0-1	100	Framed-IPv6-Pool

4. Références

[RFC2044] F. Yergeau, "UTF-8, un format de transformation d'Unicode et d'ISO 10646", octobre 1996. (*Ob., voir* RFC2279) *(Info.)*

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

[RFC2373] R. Hinden, S. Deering, "Architecture d'adressage IP version 6", juillet 1998. (*Obsolète, voir* RFC4291) *(PS)*

[RFC2401] S. Kent et R. Atkinson, "Architecture de sécurité pour le protocole Internet", novembre 1998. (*Obsolète, voir* RFC4301)

[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)

[RFC2460] S. Deering et R. Hinden, "Spécification du protocole Internet, version 6 (IPv6) ", décembre 1998. *(MàJ par* 5095, 6564 *; D.S)*

[RFC2472] D. Haskin, E. Allen, "IP version 6 sur PPP", décembre 1998. (*Obsolète, voir* RFC5072, RFC5172) *(P.S.)*

[RFC2529] B. Carpenter, C. Jung, "Transmission d'IPv6 sur des domaines IPv4 sans tunnels explicites", mars 1999. *(P.S.)*

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

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

[RFC2866] C. Rigney, "Comptabilité RADIUS", juin 2000. (*MàJ par* RFC2867, RFC5080) *(Information)*

[RFC2867] G. Zorn, B. Aboba, D. Mitton, "Modifications de la comptabilité RADIUS pour la prise en charge du protocole de tunnel", juin 2000. *(Information)*

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

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

[RFC2893] R. Gilligan, E. Nordmark, "Mécanismes de transition pour les hôtes et routeurs IPv6", août 2000. (*Obs., voir* RFC4213)

[RFC3056] B. Carpenter, K. Moore, "Connexion des domaines IPv6 via des nuages IPv4", février 2001. *(P.S.)*

5. Considérations sur la sécurité

Le présent document décrit l'utilisation de RADIUS aux fins d'authentification, d'autorisation et de comptabilité dans les réseaux à capacité IPv6. Dans de tels réseaux, le protocole RADIUS peut fonctionner soit sur IPv4, soit sur IPv6. Les faiblesses de sécurité connues du protocole RADIUS sont décrites dans les [RFC2607], [RFC2865] et [RFC2869].

Depuis qu'IPsec [RFC2401] est de mise en œuvre obligatoire pour IPv6, il est estimé que les mises en œuvre de RADIUS qui prennent en chage IPv6 vont normalement fonctionner avec IPsec. Lorsque RADIUS fonctionne avec IPsec et que des

certificats sont utilisés pour l'authentification, il peut être souhaitable d'éviter la gestion des secrets partagés RADIUS, afin de démultiplier l'adaptabilité améliorée de l'infrastructure de clés publiques.

Dans RADIUS, un secret partagé est utilisé pour cacher des attributs comme le mot de passe d'usager [RFC2865] et le mot de passe de tunnel [RFC2868]. De plus, le secret partagé est utilisé dans le calcul de l'authentifiant de réponse [RFC2865], ainsi que dans l'attribut Authentifiant de message [RFC2869]. Donc, dans RADIUS, un secret partagé est utilisé pour fournir la protection de la confidentialité ainsi que de l'intégrité et l'authentification. Il en résulte que seule l'utilisation de IPsec ESP avec une transformation non nulle peut assurer des services de sécurité suffisants pour se substituer à la sécurité de couche application RADIUS. Donc, lorsque IPSEC AH ou ESP nul est utilisé, il sera normalement toujours nécessaire de configurer un secret partagé RADIUS.

Cependant, lorsque RADIUS fonctionne sur IPsec ESP avec une transformation non nulle, le secret partagé entre le NAS et le serveur RADIUS PEUT ne pas être configuré. Dans ce cas, un secret partagé de longueur zéro DOIT être supposé.

6. Considérations relatives à l'IANA

Le présent document requiert l'allocation de six nouveaux numéros d'attributs RADIUS pour les attributs suivants :

NAS-IPv6-Address
Framed-Interface-Id
Framed-IPv6-Prefix
Login-IPv6-Host
Framed-IPv6-Route
Framed-IPv6-Pool

Voir à la Section 3 la liste des numéros enregistrés.

7. Remerciements

Les auteurs tiennent à remercier Jun-ichiro itojun Hagino de IIJ Research Laboratory, Darran Potter de Cisco et Carl Rigney de Lucent pour leurs contributions au présent document.

8. Adresse des auteurs

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

Glen Zorn
Cisco Systems, Inc.
500 108th Avenue N.E., Suite 500
Bellevue, WA 98004
téléphone : +1 425 471 4861
mél : gwz@cisco.com

Dave Mitton
Circular Logic UnLtd.
733 Turnpike Street #154
North Andover, MA 01845
téléphone : 978 683-1814
mél : david@mitton.com

Déclaration complète de droits de reproduction

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.