Groupe de travail Réseau
Request for Comments : 3580
Categorie : Information

P. Congdon, Hewlett Packard
B. Aboba, Microsoft
A. Smith, Trapeze Networks
G. Zorn, Cisco Systems
J. Roese, Enterasys

Traduction Claude Brière de L'Isle
septembre 2003

Lignes directrices pour l'utilisation du service d'authentification distante d'utilisateur appelant (RADIUS) par IEEE 802.1X

Résumé
Le présent document fait des suggestions sur l'utilisation du service d'authentification distante d'utilisateur appelant (RADIUS, *Remote Authentication Dial In User Service*) par les authentificateurs IEEE 802.1X. Le contenu du présent document est aussi inclus dans un appendice non normatif de la spécification IEEE 802.1X, et il est présenté comme RFC de l'IETF à des fins d'information.

Table des Matières

1. Introduction

La norme IEEE 802.1X permet l'accès authentifié aux supports IEEE 802, incluant les LAN Ethernet, à anneau à jeton *(Token Ring)*, et 802.11 sans fil. Bien que la prise en charge du service d'authentification distante d'utilisateur appelant (RADIUS, *Remote Authentication Dial In User Service*) soit facultative dans IEEE 802.1X, on s'attend à ce que de nombreux authentificateurs IEEE 802.1X fonctionnent comme clients RADIUS.

La norme IEEE 802.1X [IEEE8021X] fournit "l'authentification de l'accès réseau" pour les supports IEEE 802 [IEEE802], incluant les LAN Ethernet [IEEE8023], à anneau à jetons et 802.11 sans fil [IEEE80211].

La norme IEEE 802.1X n'exige pas l'utilisation d'un serveur d'authentification terminal, et il peut donc être déployé dans des ponts ou points d'accès autonomes, ainsi que dans des scénarios à gestion centralisée.

Dans des situations où il est souhaitable de gérer de façon centralisée l'authentification, l'autorisation et la comptabilité (AAA) pour les réseaux IEEE 802, le déploiement d'un serveur terminal d'authentification et de comptabilité est désirable. Dans de telles situations, on s'attend à ce que les authentificateurs IEEE 802.1X fonctionnent comme clients AAA.

Le présent document donne des suggestions pour l'utilisation de RADIUS par les authentificateurs IEEE 802.1X. La prise en charge d'un protocole AAA est facultative pour les authentificateurs IEEE 802.1X, et donc la présente spécification a été incorporée dans un appendice non normatif dans la spécification IEEE 802.1X.

1.1 Terminologie

Le présent document utilise les termes suivants :

Point d'accès (AP, *Access Point*) : station qui fournit l'accès aux services de distribution via le support sans fil pour les stations associées.

Association : service utilisé pour établir la transposition entre point d'accès et station et permettre l'invocation par la station des services du système de distribution.

Authentificateur : c'est une entité qui exige l'authentification de la part du solliciteur. L'authentificateur peut être connecté au solliciteur à l'autre extrémité d'un segment de LAN point à point ou d'une liaison 802.11 sans fil.

Serveur d'authentification : c'est une entité qui fournit un service d'authentification à un authentificateur. Ce service vérifie, d'après les accréditifs fournis par le solliciteur, la revendication d'identité faite par le solliciteur.

Entité d'accès (PAE, *Port Access Entity*) : entité de protocole associée à un accès physique ou virtuel (802.11). Un certain PAE peut prendre en charge la fonction de protocole associée à l'authentificateur, au solliciteur, ou aux deux.

Station (STA) : tout appareil qui contient une interface conforme à IEEE 802.11 de contrôle d'accès au support (MAC, *medium access control*) et de couche physique (PHY) au support sans fil (WM, *wireless medium*).

Solliciteur : entité qui est authentifiée par un authentificateur. Le solliciteur peut être connecté à l'authentificateur à une extrémité d'un segment de LAN point à point ou d'une liaison 802.11 sans fil.

1.1 Langage des exigences

Dans le présent 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" dans ce document sont à interpréter comme décrit dans la [RFC2119].

2. Attributs de la comptabilité RADIUS

Avec quelques exceptions, les attributs de comptabilité RADIUS définis dans les [RFC2866], [RFC2867], et [RFC2869] ont la même signification au sein des sessions IEEE 802.1X que dans les sessions commutées et aucun commentaire supplémentaire n'est nécessaire.

Les attributs qui demandent une présentation sont :
Acct-Terminate-Cause *(cause de terminaison de comptabilité)*
Acct-Multi-Session-Id *(identifiant de multi session de comptabilité)*
Acct-Link-Count *(compte de liaisons de comptabilité)*

2.1 Acct-Terminate-Cause

Cet attribut indique comment la session s'est terminée, comme décrit dans la [RFC2866]. [IEEE8021X] définit les valeurs de cause de terminaison suivantes, qui sont montrées avec leurs équivalents RADIUS dans le tableau suivant.

dot1xAuthSessionTerminateCause IEEE 802.1X Valeur	**Acct-Terminate-Cause RADIUS Valeur**
SupplicantLogoff(1)	User Request (1)
portFailure(2)	Lost Carrier (2)
SupplicantRestart(3)	Supplicant Restart (19)
reauthFailed(4)	Reauthentication Failure (20)
authControlForceUnauth(5)	Admin Reset (6)
portReInit(6)	Port Reinitialized (21)
portAdminDisabled(7)	Port Administratively Disabled (22)
notTerminatedYet(999)	N/A

Lorsque on utilise cet attribut, la cause de terminaison User Request (1) *(demande de l'utilisateur)* correspond à la situation dans laquelle la session s'est terminée à cause d'un EAPOL-Logoff reçu du solliciteur. Lorsque une session est déplacée à cause de l'itinérance, l'automate à états EAPOL va traiter cela comme un Supplicant Logoff *(déconnexion du solliciteur)*.

Une cause de terminaison Lost Carrier (2) *(perte de porteuse)* indique une terminaison de session due à la perte de la connexité physique pour des raisons autres que l'itinérance entre les points d'accès. Par exemple, si le solliciteur déconnecte une connexion de LAN point à point, ou passe hors de la portée d'un point d'accès, cette cause de terminaison est utilisée. Lost Carrier (2) équivaut donc à une condition d'accès désactivé dans les automates à états EAPOL.

Une cause de terminaison Supplicant Restart (19) *(redémarrage du solliciteur)* indique la réinitialisation des automates à états de solliciteur.

Une cause de terminaison Reauthentication Failure (20) *(échec de réauthentification)* indique qu'un solliciteur précédemment authentifié a échoué à se réauthentifier suite à l'expiration du temporisateur de réauthentification ou à une demande explicite de réauthentification par une action de gestion.

Dans [IEEE80211], une réauthentification périodique peut être utile pour empêcher la réutilisation d'une valeur d'initialisation avec une certaine clé. Comme la réussite de la réauthentification ne résulte pas en la terminaison de la session, les paquets de comptabilité ne sont pas envoyés suite à la réauthentification sauf si l'état de la session change. Par

exemple :

a. La session se termine due à l'échec de la réauthentification. Dans ce cas, on utilise la cause de terminaison Reauthentication Failure (20).
b. Les autorisations ont changé par suite d'une réauthentification réussie. Dans ce cas, la cause de terminaison Service Unavailable (15) *(service indisponible)* est utilisée. Pour les besoins de la comptabilité, la portion de la session après le changement d'autorisation est traitée comme une session séparée.

Lorsque l'authentification IEEE 802.1X se produit avant une association, les paquets de comptabilité ne sont pas envoyés tant qu'une association ne s'est pas produite.

Une cause de terminaison Admin Reset (6) *(réinitialisation administrative)* indique que l'accès a été administrativement forcé à passer à l'état non autorisé.

Une cause de terminaison Port Reinitialized (21) *(accès réinitialisé)* indique que le MAC de l'accès a été réinitialisé.

Une cause de terminaison Port Administratively Disabled (22) *(désactivation administrative de l'accès)* indique que l'accès a été désactivé par décision administrative.

2.2 Acct-Multi-Session-Id

L'objet de cet attribut est de rendre possible la liaison de plusieurs sessions en rapports. Bien que [IEEE8021X] n'agisse pas sur des accès agrégés, il est possible à un solliciteur en itinérance entre des points d'accès d'envoyer plusieurs paquets de comptabilité RADIUS par différents points d'accès.

Lorsque il est pris en charge par les points d'accès, l'attribut Acct-Multi-Session-Id peut être utilisé pour lier ensemble les multiples sessions en rapports d'un solliciteur en itinérance. Dans une telle situation, si le contexte de session est transféré entre les points d'accès, les paquets de comptabilité PEUVENT être envoyés sans un échange correspondant d'authentification et d'autorisation, pourvu que l'association se soit effectuée. Cependant, dans une telle situation, on suppose que le Acct-Multi-Session-Id est transféré entre les points d'accès au titre du protocole inter points d'accès (IAPP).

Si le Acct-Multi-Session-Id n'est pas unique entre les points d'accès, il est alors possible que le Acct-Multi-Session-Id choisi se chevauche avec une valeur existante alloué sur ce point d'accès, et le serveur de comptabilité sera donc incapable de distinguer une session d'itinérance d'une session multi liaisons.

Par suite, l'attribut Acct-Multi-Session-Id est unique parmi tous les ponts ou points d'accès, les solliciteurs et les sessions. Afin d'assurer cette unicité, il est suggéré que le Acct-Multi-Session-Id soit de la forme :

Adresse MAC d'AP d'origine | Adresse MAC du solliciteur | Horodatage NTP

Ici "|" représente l'enchaînement, l'adresse MAC d'AP d'origine est l'adresse MAC du pont ou point d'accès auquel la session a commencé, et les 64 bits de l'horodatage NTP indiquent le début de la session d'origine. Afin d'assurer la cohérence du Acct-Multi-Session-Id entre les sessions d'itinérance, il peut être déplacé entre les points d'accès au titre de IAPP ou d'un autre schéma de relais.

L'utilisation d'un Acct-Multi-Session-Id de cette forme garantit l'unicité parmi tous les points d'accès, solliciteurs et sessions. Comme l'horodatage NTP ne revient pas à zéro lors des réamorçages, il n'y a pas de possibilité qu'un point d'accès réamorcé puisse choisir un Acct-Multi-Session-Id qui serait confondu avec celui d'une session antérieure.

Comme le Acct-Multi-Session-Id est du type String *(chaîne)* comme défini dans la [RFC2866], pour son utilisation avec IEEE 802.1X, il est codé comme une chaîne ASCII de chiffres hexadécimaux. Exemple : "00-10-A4-23-19-C0-00-12-B2-14-23-DE-AF-23-83-C0-76-B8-44-E8"

2.3 Acct-Link-Count

L'attribut Acct-Link-Count peut être utilisé pour compter le nombre d'accès qui ont été agrégés.

3. Authentification RADIUS

Cette section décrit comment les attributs définis dans les [RFC2865], [RFC2867], [RFC2868], [RFC2869], [RFC3162] et [RFC3579] sont utilisés dans l'authentification IEEE 802.1X.

3.1 User-Name

Dans IEEE 802.1X, le solliciteur fournit normalement son identité via un message EAP-Response/Identity. Lorsque elle est disponible, l'identité du solliciteur est incluse dans l'attribut User-Name, et incluse dans les messages RADIUS Access-Request et Access-Reply comme spécifié dans les [RFC2865] et [RFC3579].

Autrement, comme exposé au paragraphe 2.1 de la [RFC3579], l'attribut User-Name peut contenir la valeur Calling-Station-ID *(identifiant de la station appelante)*, qui est réglée à l'adresse MAC du solliciteur.

3.2 User-Password, CHAP-Password, CHAP-Challenge

Comme IEEE 802.1X ne prend pas en charge l'authentification PAP ou CHAP, les attributs User-Password, CHAP-Password ou CHAP-Challenge ne sont pas utilisés par les authentificateurs IEEE 802.1X agissant comme clients RADIUS.

3.3 NAS-IP-Address, NAS-IPv6-Address

Pour l'utilisation avec IEEE 802.1X, l'attribut NAS-IP-Address contient l'adresse IPv4 du pont ou point d'accès agissant comme authentificateur, et l'attribut NAS-IPv6-Address contient l'adresse IPv6. Si l'authentificateur IEEE 802.1X a plus d'une interface, il peut être souhaitable d'utiliser une adresse de rebouclage à cette fin pour que l'authentificateur soit quand même joignable si une des interfaces était défaillante.

3.4 NAS-Port

Pour l'utilisation avec IEEE 802.1X, NAS-Port va contenir le numéro d'accès du pont, si il est disponible. Alors qu'un point d'accès n'a pas d'accès physiques, un "identifiant d'association" unique est alloué à chaque station mobile après un échange d'association réussi. Par suite, pour un point d'accès, si l'échange d'association a été achevé avant l'authentification, l'attribut NAS-Port va contenir l'identifiant d'association, qui est un entier non signé de 16 bits. Lorsque l'authentification IEEE 802.1X survient avant l'association, une valeur unique de NAS-Port peut n'être pas disponible.

3.5 Service-Type

Dans l'utilisation avec IEEE 802.1X, les valeurs Framed (2) *(tramé)*, Authenticate Only (8) *(seulement authentifié)*, et Call Check (10) *(vérification d'appel)* sont le plus couramment utilisées.
Un type de service de "Framed" indique que le tramage 802 approprié devrait être utilisé pour la connexion. Un type de service de "Authenticate Only" (8) indique qu'aucune information d'autorisation n'a besoin d'être retournée dans le Access-Accept. Comme décrit dans la [RFC2865], un type de service de "Call Check" est inclus dans un paquet de demande d'accès pour demander que le serveur RADIUS accepte ou rejette la tentative de connexion, normalement sur la base des attributs Called-Station-ID (réglé à l'adresse MAC du pont ou point d'accès) ou Calling-Station-ID (réglé à l'adresse MAC du solliciteur). Comme noté dans la [RFC2865], il est recommandé que dans ce cas, l'attribut User-Name reçoive la valeur de Calling-Station-Id.

3.6 Framed-Protocol

Comme il n'y a pas de valeur pour un support IEEE 802, l'attribut Framed-Protocol n'est pas utilisé par les authentificateurs IEEE 802.1X.

3.7 Framed-IP-Address, Framed-IP-Netmask

IEEE 802.1X ne fournit pas de mécanisme pour l'allocation d'adresse IP. Donc les attributs Framed-IP-Address et Framed-IP-Netmask ne peuvent être utilisés que par les authentificateurs IEEE 802.1X qui prennent en charge le mécanisme d'allocation d'adresse IP. Normalement, cette capacité est prise en charge par les appareils de couche 3.

3.8 Framed-Routing

L'attribut Framed-Routing indique la méthode d'acheminement pour le solliciteur. Il n'est donc pertinent que pour les authentificateurs IEEE 802.1X qui agissent comme appareils de couche 3, et ne peut être utilisé par un pont ou point d'accès.

3.9 Filter-ID

Cet attribut indique le nom de la liste de filtres à appliquer à la session du solliciteur. Pour l'utilisation avec un authentificateur IEEE 802.1X, il peut être utilisé pour indiquer des filtres de couche 2 ou de couche 3. Les filtres de couche 3 ne sont normalement pris en charge que par les authentificateurs IEEE 802.1X qui agissent comme appareils de couche 3.

3.10 Framed-MTU

Cet attribut indique la taille maximum d'un paquet IP qui peut être transmis sur le réseau entre le solliciteur et l'authentificateur. Les authentificateurs IEEE 802.1X règlent cela à la valeur correspondante du support 802 pertinent et l'incluent dans la demande d'accès RADIUS. Le serveur RADIUS peut envoyer un paquet EAP aussi grand que Framed-MTU moins quatre (4) octets, prenant en compte les frais généraux supplémentaires pour les champs IEEE 802.1X Version (1), Type (1) et Longueur de corps (2). Pour EAP sur les supports IEEE 802, les valeurs de Framed-MTU (qui n'incluent pas la redondance LLC/SNAP) et les valeurs de longueur maximum de trame (non inclus le préambule) sont les suivantes :

Support	**MTU tramée**	**Long. max. de trame**
Ethernet	1500	1522
802.3	1500	1522
802.4	8174	8193
802.5 (4 Mbit/s)	4528	4550
802.5 (16 Mbit/s)	18173	18200
802.5 (100 Mbit/s)	18173	18200
802.6	9191	9240
802.9a	1500	1518
802.11	2304	2346
802.12 (Ethernet)	1500	1518
802.12 (anneau à jetons)	4502	4528
FDDI	4479	4500

Note : la taille de Framed-MTU pour les supports IEEE 802.11 peut changer par suite des travaux en cours du groupe de travail IEEE 802.11. Comme certaines stations 802.11 ne peuvent pas traiter une MTU supérieure à 1500 octets, il est recommandé que les serveurs RADIUS qui rencontrent une valeur de NAS-Port-Type de 802.11 n'envoient pas de paquets EAP de plus de 1496 octets.

3.11. Framed-Compression

[IEEE8021X] ne prend pas en charge la compression. Cet attribut n'est donc pas compris par les authentificateurs [IEEE8021X].

3.12 Messages affichables

L'attribut Reply-Message, défini au paragraphe 5.18 de la [RFC2865], indique le texte qui peut être affiché à l'usager. Ceci est similaire au concept du type de notification EAP, défini dans la [RFC2284]. Comme noté au paragraphe 2.6.5 de la [RFC3579], lors de l'envoi d'un message affichable à un authentificateur [IEEE8021X], il vaut mieux envoyer les messages affichables au sein d'un attribut EAP-Message/EAP-Request/Notification plutôt que dans les attributs Reply-Message.

3.13 Callback-Number, Callback-ID

Ces attributs ne sont pas compris des authentificateurs IEEE 802.1X.

3.14 Framed-Route, Framed-IPv6-Route

Les attributs Framed-Route et Framed-IPv6-Route fournissent des chemins qui sont à configurer pour le solliciteur. Ces attributs ne sont donc pertinents que pour les authentificateurs IEEE 802.1X qui agissent comme appareils de couche 3, et ne peuvent pas être compris par un pont ou un point d'accès.

3.15 State, Class, Proxy-State

Ces attributs sont utilisés pour les mêmes objets que décrit dans la [RFC2865].

3.16 Vendor-Specific

Les attributs spécifiques du fabricant sont utilisés pour les mêmes objets que décrit dans la [RFC2865]. Les attributs MS-MPPE-Send-Key et MS-MPPE-Recv-Key, décrits au paragraphe 2.4 de la [RFC2548], PEUVENT être utilisés pour chiffrer et authentifier le descripteur RC4 EAPOL-Key du paragraphe 7.6 de [IEEE8021X]. Des exemples de la déduction des attributs MS-MPPE-Send-Key et MS-MPPE-Recv-Key de la clé maîtresse négociée par une méthode EAP sont donnés dans la [RFC2716]. Les détails du descripteur EAPOL-Key sont à la Section 4.

3.17 Session-Timeout

Lorsque il est envoyé avec un Access-Accept sans un attribut Termination-Action ou avec un attribut Termination-Action réglé à la valeur par défaut, l'attribut Session-Timeout spécifie le nombre maximum de secondes de service fourni avant la terminaison de session.

Lorsque envoyé dans un Access-Accept avec une valeur de Termination-Action de RADIUS-Request, l'attribut Session-Timeout spécifie le nombre maximum de secondes de service fourni avant une réauthentification. Dans ce cas, l'attribut Session-Timeout est utilisé pour charger la constante reAuthPeriod dans le temporisateur de réauthentification de l'automate à états de 802.1X. Lorsque il est envoyé avec une valeur de Termination-Action de RADIUS-Request, une valeur de Session-Timeout de zéro indique le désir d'effectuer une autre authentification (éventuellement d'un type différent) immédiatement après que la première authentification s'est achevée avec succès.

Lorsque envoyée dans un Access-Challenge, cet attribut représente le nombre maximum de secondes qu'un authentificateur IEEE 802.1X devrait attendre une réponse EAP avant de retransmettre. Dans ce cas, l'attribut Session-Timeout est utilisé pour charger la constante suppTimeout dans l'automate à états de relais de IEEE 802.1X.

3.18 Idle-Timeout

L'attribut Idle-Timeout est décrit dans la [RFC2865]. Pour les supports IEEE 802 autres que 802.11 les supports sont toujours activés. Par suite, l'attribut Idle-Timeout n'est normalement utilisé qu'avec des supports sans fil comme IEEE 802.11. Il est possible qu'un appareil sans fil erre en dehors de la gamme de tous les points d'accès. Dans ce cas, l'attribut Idle-Timeout indique la durée maximum pendant laquelle un appareil sans fil peut rester inactif.

3.19 Termination-Action

Cet attribut indique quelle action devrait être prise lorsque le service est achevé. La valeur RADIUS-Request (1) indique que la réauthentification devrait se produire à l'expiration de Session-Time. La valeur Default (0) indique que la session devrait se terminer.

3.20 Called-Station-Id

Pour les authentificateurs IEEE 802.1X, cet attribut est utilisé pour mémoriser l'adresse MAC du pont ou point d'accès en format ASCII (seulement en majuscules) avec les valeurs d'octets séparées par un "-". Exemple : "00-10-A4-23-19-C0". Dans IEEE 802.11, où le SSID est connu, il DEVRAIT être ajouté à l'adresse MAC du point d'accès, séparé de l'adresse MAC par un ":". Exemple : "00-10-A4-23-19-C0:AP1".

3.21 Calling-Station-Id

Pour les authentificateurs IEEE 802.1X, cet attribut est utilisé pour mémoriser l'adresse MAC du solliciteur en format ASCII (seulement en majuscules) avec les valeurs d'octets séparées par un "-". Exemple : "00-10-A4-23-19-C0".

3.22 NAS-Identifier

Cet attribut contient une chaîne qui identifie l'authentificateur IEEE 802.1X qui génère la demande d'accès.

3.23 NAS-Port-Type

Pour l'utilisation avec IEEE 802.1X, les valeurs de NAS-Port-Type de Ethernet (15) Wireless - IEEE 802.11 (19), Token Ring (20) et FDDI (21) peuvent être utilisées.

3.24 Port-Limit

Cet attribut n'a pas de signification lorsque il est envoyé à un authentificateur [IEEE8021X].

3.25 Password-Retry

Dans IEEE 802.1X, l'authentificateur passe toujours à l'état HELD après un échec d'authentification. Cet attribut n'a donc aucun sens pour IEEE 802.1X.

3.26 Connect-Info

Cet attribut est envoyé par un pont ou point d'accès pour indiquer la nature de la connexion du solliciteur. Lorsque envoyé dans la demande d'accès, il est recommandé que cet attribut contienne des informations sur la vitesse de la connexion du solliciteur. Pour 802.11, le format suivant est recommandé : "CONNECT 11Mbit/s 802.11b". Si il est envoyé dans le Accounting STOP, cet attribut peut être utilisé pour récapituler des statistiques sur la qualité de la session. Par exemple, dans IEEE 802.11, l'attribut Connect-Info peut contenir des informations sur le nombre de retransmissions de couche de liaison. Le format exact de cet attribut est spécifique de la mise en œuvre.

3.27 EAP-Message

Comme IEEE 802.1X assure l'encapsulation de EAP comme décrit dans la [RFC2284] et [IEEE8021X], l'attribut EAP-Message défini dans la [RFC3579] est utilisé pour encapsuler les paquets EAP pour leur transmission de l'authentificateur IEEE 802.1X au serveur d'authentification. Le paragraphe 2.2 de la [RFC3579] décrit comment le serveur d'authentification traite les paquets EAP invalides qui lui sont passés par l'authentificateur.

3.28 Message-authenticator

Comme noté au paragraphe 3.1 de la [RFC3579], l'attribut Message-authenticator DOIT être utilisé pour protéger les paquets au sein d'une conversation RADIUS/EAP.

3.29 NAS-Port-Id

Cet attribut est utilisé pour identifier l'accès de l'authentificateur IEEE 802.1X qui authentifie le solliciteur. Le NAS-Port-Id diffère du NAS-Port en ce qu'il est une chaîne de longueur variable tandis que le NAS-Port est une valeur de 4 octets.

3.30 Framed-Pool, Framed-IPv6-Pool

IEEE 802.1X ne donne pas de mécanisme pour allouer une adresse IP. Donc, les attributs Framed-Pool et Framed-IPv6-Pool ne peuvent être utilisés que par les authentificateurs IEEE 802.1X qui prennent en charge des mécanismes d'allocation d'adresse IP. Normalement, cette capacité est assurée par les appareils de couche 3.

3.31 Attributs de tunnel

La [RFC2868] définit les attributs de tunnel RADIUS qui sont utilisés pour l'authentification et l'autorisation, et la [RFC2867] définit les attributs de tunnel utilisés pour la comptabilité. Lorsque l'authentificateur IEEE 802.1X prend en charge le tunnelage, un tunnel obligatoire peut être établi pour le solliciteur par suite de l'authentification.

En particulier, il peut être désirable de permettre qu'un accès soit placé dans un LAN virtuel (VLAN) particulier, défini dans [IEEE8021Q], sur la base du résultat de l'authentification. Cela peut être utilisé, par exemple, pour permettre à un hôte sans fil de rester sur le même VLAN lorsque il se déplace au sein d'un réseau privé.

Le serveur RADIUS indique normalement le VLAN désiré en incluant les attributs de tunnel au sein de Access-Accept. Cependant, l'authentificateur IEEE 802.1X peut aussi fournir une indication quant au VLAN à allouer au solliciteur en incluant des attributs de tunnel au sein de la demande d'accès.

On utilise les attributs de tunnel suivants pour l'allocation de VLAN :
Tunnel-Type=VLAN (13)
Tunnel-Medium-Type=802
Tunnel-Private-Group-ID=VLANID

Noter que le VLANID fait 12 bits, prenant une valeur entre 1 et 4094, inclus. Comme le Tunnel-Private-Group-ID est du type String comme défini dans la [RFC2868], pour l'utilisation avec IEEE 802.1X, la valeur d'entier VLANID est codée comme une chaîne.

Lorsque les attributs de tunnel sont envoyés, il est nécessaire de remplir le champ Tag. Comme noté au paragraphe 3.1 de la [RFC2868] : "Le champ Tag fait un octet et est destiné à donner le moyen de grouper les attributs dans le même paquet qui se réfèrent au même tunnel. Les valeurs valides pour ce champ sont 0x01 à 0x1F, inclus. Si le champ Tag n'est pas utilisé, elle DOIT être zéro (0x00)."

Pour l'utilisation avec les attributs Tunnel-Client-Endpoint, Tunnel-Server-Endpoint, Tunnel-Private-Group-ID, Tunnel-Assignment-ID, Tunnel-Client-Auth-ID ou Tunnel-Server-Auth-ID (mais pas Tunnel-Type, Tunnel-Medium-Type, Tunnel-Password, ou Tunnel-Preference), un champ Tag de valeur supérieure à 0x1F est interprété comme le premier octet du champ suivant.

Sauf si d'autres types de tunnel sont fournis (par exemple pour des authentificateurs IEEE 802.1X qui pourraient prendre en charge le tunnelage mais pas les VLAN) il est seulement nécessaire que les attributs de tunnel spécifient un seul tunnel. Par suite, lorsque on désire seulement spécifier le VLANID, le champ Tag DEVRAIT être réglé à zéro (0x00) dans tous les attributs de tunnel. Si d'autres types de tunnels devaient être fournis, les valeurs de Tag entre 0x01 et 0x1F DEVRAIENT être choisies.

4. Trame RC4 EAPOL-Key

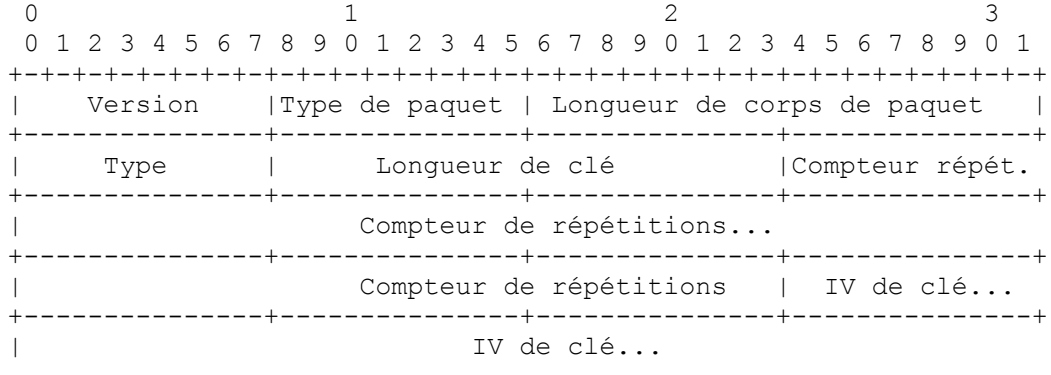
La trame RC4 EAPOL-Key est créée et transmise par l'authentificateur afin de fournir des informations de clés spécifiques du support. Par exemple, au sein de 802.11 la trame RC4 EAPOL-Key peut être utilisée pour distribuer des clés de diffusion/diffusion groupée ("par défaut") ou des clés d'envoi individuel ("transposition de clé"). La clé "par défaut" est la même pour toutes les stations au sein d'un domaine de diffusion.

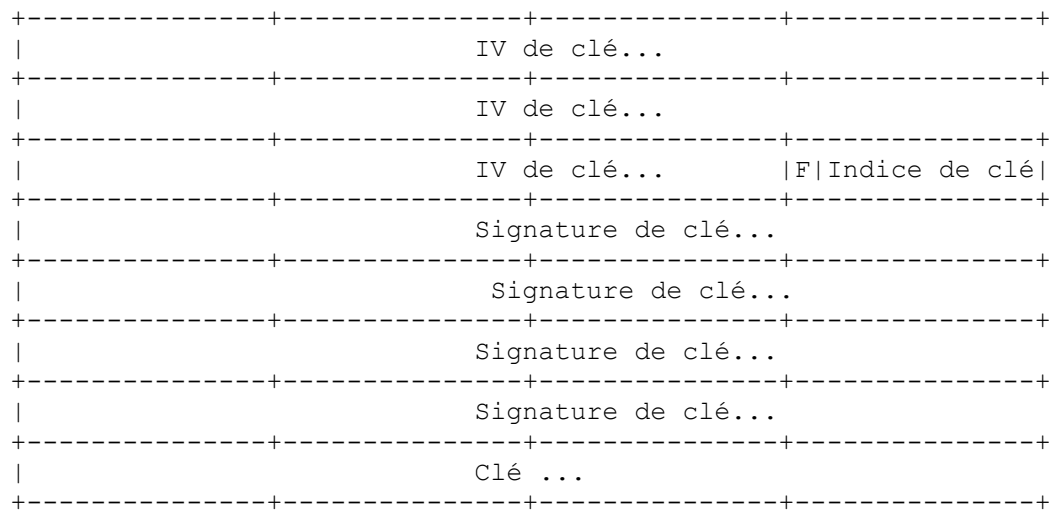
La trame RC4 EAPOL-Key n'est pas acquittée et donc l'authentificateur ne sait pas si le solliciteur l'a reçue. Si elle est perdue, le solliciteur et l'authentificateur n'auront donc pas le même matériel de chiffrement, et la communication va échouer. Si cela arrive, le problème est normalement réglé en refaisant l'authentification.

La trame RC4 EAPOL-Key est envoyée de l'authentificateur au solliciteur afin de provisionner la clé "par défaut", et ensuite de rafraîchir la clé "par défaut". Elle peut aussi être utilisée pour rafraîchir la clé de transposition de clé. Le changement de clé n'est normalement exigé qu'avec des suites de chiffrement faibles comme WEP, définie dans [IEEE80211].

Lorsque des clés sont requises, une méthode EAP qui déduit les clés est normalement choisie. Donc, les clés de "transposition de clé" initiales peuvent être déduites du matériel de chiffrement EAP, sans exiger que l'authentificateur envoie une trame RC4 EAPOL-Key au solliciteur. Un exemple de la façon dont le matériel ce chiffrement EAP peut être déduit et utilisé est présenté dans la [RFC2716].

Bien que la trame RC4 EAPOL-Key soit définie dans [IEEE8021X], une description plus complète est donnée ci-dessous.





Version : Le champ Version fait un octet. Pour IEEE 802.1X,, il contient la valeur 0x01.

Type de paquet : Le champ Type de paquet fait un octet, et détermine le type de paquet qui est transmis. Pour un descripteur de clé EAPOL, le champ Type de paquet contient 0x03.

Longueur de corps de paquet : le champ Longueur de corps de paquet fait deux octets, et contient la longueur du descripteur de clé EAPOL en octets, non inclus les champs Version, Type de paquet et Longueur de corps de paquet.

Type : Le champ Type fait un seul octet. Le descripteur de clé est défini différemment pour chaque type ; la présente spécification documente seulement le descripteur de clé RC4 (Type = 0x01).

Longueur de clé : Le champ Longueur de clé fait deux octets. Si Longueur de corps de paquet = 44 + Longueur de clé, alors le champ Clé contient la clé en forme chiffrée, de longueur Longueur de clé. C'est 5 octets (40 bits) pour WEP, et 13 octets (104 bits) pour WEP-128. Si Longueur de corps de paquet = 44, le champ Clé est alors absent, et Longueur de clé représente le nombre d'octets de moindre poids de l'attribut MS-MPPE-Send-Key [RFC2548] à utiliser comme matériel de chiffrement. Noter que les attributs MS- MPPE-Send-Key et MS-MPPE-Recv-Key sont définis du point de vue de l'authentificateur. Du point de référence du solliciteur, les termes sont inversés. Donc, le MS-MPPE-Recv-Key sur le solliciteur correspond au MS-MPPE-Send-Key sur l'authentificateur, et le MS-MPPE-Send-Key sur le solliciteur correspond au MS-MPPE-Recv-Key sur l'authentificateur.

Compteur de répétitions : Le champ Compteur de répétitions fait 8 octets. Il ne se répète pas sur la durée de vie du matériel de chiffrement utilisé pour chiffrer le champ Clé et calcule le champ Signature de clé. Un horodatage NTP de 64 bits PEUT être utilisé comme compteur de répétitions.

IV de clé : Le champ IV de clé fait 16 octets et inclut un nombre aléatoire cryptographique de 128 bits.

F : Le fanion F fait un seul bit, qui décrit le type de clé qui est inclus dans le champ Cl". Les valeurs sont :
0 = pour la diffusion (clé par défaut)
1 = pour l'envoi individuel (clé de transposition de clé)

Indice de clé : L'indice de clé fait 7 bits.

Signature de clé : Le champ Signature de clé fait 16 octets. Il contient une vérification d'intégrité HMAC-MD5 du message calculée sur le descripteur EAPOL-Key, commençant au champ Version, avec le champ Clé rempli s'il est présent, mais avec le champ Signature de clé réglé à zéro. Pour le calcul, les 32 octets (256 bit) de MS-MPPE-Send-Key [RFC2548] sont utilisés comme clé HMAC-MD5.

Clé : Si la longueur de corps de paquet = 44 + Longueur de clé, alors le champ Clé contient la clé en forme chiffrée, de longueur Longueur de clé. Si la longueur de corps de paquet = 44, le champ Clé est absent, et les octets de moindre poids de Longueur de clé provenant de l'attribut MS-MPPE-Send-Key sont utilisés comme matériel de chiffrement. Lorsque le champ Clé est chiffré avec RC4, la clé de chiffrement RC4 utilisée pour chiffrer ce champ est formée par l'enchaînement du champ IV de clé de 16 octets (128 bit) avec les 32 octets de l'attribut MS-MPPE-Recv-Key. Cela donne une clé RC4 de 48 octets (384 bits).

5. Considérations sur la sécurité

Comme le présent document décrit l'utilisation de RADIUS pour les besoins d'authentification, autorisation, et comptabilité dans les réseaux à capacité IEEE 802.1X, il est vulnérable à toutes les menaces qui sont présentes dans les autres applications RADIUS. Pour une discussion de ces menaces, voir les [RFC2607], [RFC2865], [RFC3162], [RFC3576], et [RFC3579].

Les vulnérabilités incluent :
Modification ou falsification de paquet
Attaques de dictionnaire
Attaques de texte source connu
Répétition
Discordance de résultat
Intégration 802.11
Problèmes de gestion de clé

5.1 Modification ou falsification de paquet

RADIUS, défini dans la [RFC2865], n'exige pas que toutes les demandes d'accès soient authentifiées ou protégées en intégrité. Cependant, IEEE 802.1X se fonde sur EAP. Comme décrit au paragraphe 3.1 de la [RFC3579] : "L'attribut Message-authenticator DOIT être utilisé pour protéger tous les paquets Access-Request, Access-Challenge, Access-Accept, et Access-Reject qui contiennent un attribut EAP-Message."

Par suite, lorsque utilisés avec IEEE 802.1X, tous les paquets RADIUS DOIVENT être authentifiés et protégés en intégrité. De plus, comme décrit au paragraphe 4.2 de la [RFC3579] : "Pour traiter les faiblesses de sécurité de RADIUS/EAP, les mises en œuvre de la présente spécification DEVRAIENT prendre en charge IPsec [RFC2401] ainsi que IKE [RFC2409] pour la gestion de clés. IPsec ESP [RFC2406] avec une transformation non nulle DEVRAIT être pris en charge, et IPsec ESP avec une transformation de chiffrement non nulle et la prise en charge de l'authentification DEVRAIT être utilisé pour assurer la confidentialité, l'authentification, et la protection de l'intégrité et contre la répétition, par paquet. IKE DEVRAIT être utilisé pour la gestion de clé".

5.2 Attaques de dictionnaire

Comme exposé au paragraphe 4.3.3 de la [RFC3579], le secret partagé RADIUS est vulnérable à l'attaque de dictionnaire hors ligne, fondée sur la capture de l'attribut Response-authenticator ou Message-authenticator. Pour diminuer le niveau de vulnérabilité, la Section 3 de la [RFC2865] recommande : "Le secret (mot de passe partagé entre le client et le serveur RADIUS) DEVRAIT être au moins aussi long et imprévisible qu'un mot de passe bien choisi. Il est préférable que le secret fasse au moins 16 octets".

De plus, le risque d'une attaque de dictionnaire hors ligne peut être encore diminué en employant IPsec ESP avec une transformation non nulle afin de chiffrer la conversation RADIUS, comme décrit au paragraphe 4.2 de la [RFC3579].

5.3 Attaques de texte source connu

Comme IEEE 802.1X se fonde sur EAP, qui ne prend pas PAP en charge, l'attribut RADIUS User-Password n'est pas utilisé pour porter les mots de passe d'utilisateur cachés. Le mécanisme de dissimulation utilise MD5, défini dans la [RFC1321], afin de générer un flux de clés fondé sur le secret partagé RADIUS et l'authentificateur de demande. Lorsque PAP est utilisé, il est possible de collecter les flux de clés qui correspondent à une valeur donnée de Request-authenticator, en capturant la conversation RADIUS correspondant à une tentative d'authentification PAP en utilisant un mot de passe connu. Comme le User-Password est connu, le flux de clés correspondant à un certain Request-authenticator peut être déterminé et mémorisé.

La vulnérabilité est décrite en détail au paragraphe 4.3.4 de la [RFC3579]. Bien que les authentificateurs IEEE 802.1X ne prennent pas en charge l'authentification PAP, une vulnérabilité de la sécurité peut quand même exister lorsque le même secret partagé RADIUS est utilisé pour cacher le mot de passe d'utilisateur ainsi que les autres attributs. Cela peut se produire, par exemple, si le même mandataire RADIUS traite les demandes d'authentification à la fois pour IEEE 802.1X (qui peut cacher les attributs Tunnel-Password, MS-MPPE-Send-Key et MS-MPPE-Recv-Key) et GPRS (qui peut cacher l'attribut User-Password).

La menace peut être atténuée en protégeant RADIUS avec IPsec ESP avec une transformation non nulle, comme décrit au

paragraphe 4.2 de la [RFC3579]. De plus, le même secret partagé RADIUS NE DOIT PAS être utilisé par les deux authentifications IEEE 802.1X et PAP.

5.4 Répétition

Comme noté au paragraphe 4.3.5 de la [RFC3579], le protocole RADIUS ne fournit qu'une prise en charge limitée de la protection contre la répétition. La protection contre la répétition pour l'authentification et la comptabilité RADIUS peut être assurée en activant la protection contre la répétition de IPsec avec RADIUS, comme décrit au paragraphe 4.2 de la [RFC3579].

Comme avec l'authentificateur de demandes, pour l'utilisation avec les authentificateurs IEEE 802.1X, le Acct-Session-Id DEVRAIT être unique au monde et à travers le temps.

5.5 Discordance de résultat

Le paragraphe 2.6.3 de la [RFC3579] expose les problèmes qui surviennent quand le paquet EAP encapsulé dans un attribut EAP-Message n'est pas en accord avec le type de paquet RADIUS. Par exemple, un paquet EAP Succès peut être encapsulé au sein d'un Access-Reject ; un EAP Échec peut être envoyé avec un Access-Accept; ou un EAP Succès ou Échec peut être envoyé avec un Access-Challenge.

Comme décrit au paragraphe 2.6.3 de la [RFC3579], ces messages contradictoires causent probablement une certaine confusion. Pour s'assurer que les décisions d'accès prises par les authentificateurs IEEE 802.1X se conforment aux souhaits du serveur RADIUS, il est nécessaire que l'authentificateur prenne sa décision sur la seule base du résultat de l'authentification (Access-Accept/Reject) et non sur la base du contenu des attributs EAP-Message, si il en est de présent.

5.6 Intégration 802.11

[IEEE8021X] a été développé pour être utilisé sur des réseaux IEEE 802 filaires comme Ethernet, et donc ne décrit pas comment adapter de façon sûre IEEE 802.1X pour l'utiliser avec 802.11. Ceci sera traité par une spécification de sécurité améliorée en cours de développement au sein de IEEE 802.11.

Par exemple, [IEEE8021X] ne spécifie pas si l'authentification se produit avant ou après l'association, ni comment les clés déduites sont utilisées au sein des diverses suites de chiffrement. Il ne spécifie pas non plus de suites de chiffrement traitant les vulnérabilités découvertes dans WEP, décrites dans [Berkeley], [Arbaugh], [Fluhrer], et [Stubbl]. [IEEE8021X] définit seulement un cadre d'authentification, laissant la définition des méthodes d'authentification à d'autres documents, comme la [RFC2716].

Comme [IEEE8021X] ne traite pas les questions d'intégration de 802.11, les mises en œuvre sont invitées à consulter les spécifications supplémentaires de sécurité IEEE 802.11 pour avoir des indications sur la façon d'adapter IEEE 802.1X pour son utilisation avec 802.11. Par exemple, il est probable que la spécification de sécurité améliorée IEEE 802.11 définira sa propre hiérarchie de clés IEEE 802.11 ainsi que de nouveaux descripteurs EAPOL-Key.

5.7 Problèmes de gestion de clé

Le descripteur EAPOL-Key décrit à la Section 4. sera probablement déconseillé à l'avenir, lorsque le groupe sur la sécurité améliorée IEEE 802.11 aura achevé ses travaux. Les questions de sécurité connues incluent :

[1] Prise en charge seulement de la clé par défaut. IEEE 802.1X permet la déduction de clés d'envoi individuel par station, appelée dans [IEEE80211] "clés de transposition de clé". Les clés utilisées pour chiffrer le trafic de diffusion/diffusion groupée sont appelées des "clés par défaut". Cependant, dans certaines mises en œuvre de 802.11, les clés d'envoi individuel, déduites au titre du processus d'authentification EAP, ne sont utilisées qu'afin de chiffrer, authentifier et protéger l'intégrité du descripteur EAPOL-Key, comme décrit à la Section 4. Ces mises en œuvre ne prennent en charge que les clés par défaut (ordinairement utilisées seulement avec du trafic de diffusion/diffusion groupée) pour sécuriser tout le trafic, d'envoi individuel ou de diffusion/diffusion groupée, d'où résulte une faiblesse de sécurité inhérente. Lorsque les clés de transposition de clé par station (par exemple, des clés d'envoi individuel) ne sont pas prises en charge, toute station qui possède la clé par défaut peut déchiffrer le trafic des autres stations ou se faire passer pour elles. Lorsque utilisées avec un chiffrement faible (par exemple, WEP) les mises en œuvre qui ne prennent en charge que les clés par défaut se prêtent mieux à des attaques telles que décrites dans [Fluhrer] et [Stubbl]. Si de plus, la clé par défaut n'est pas rafraîchie périodiquement, la déduction de clé dynamique de IEEE 802.1X ne présente que peu ou pas du tout d'avantage pour la sécurité. Pour comprendre les problèmes de sécurité avec WEP, voir [Berkeley], [Arbaugh],

[Fluhrer], et [Stubbl].

[2] Réutilisation du matériel de chiffrement. Le descripteur EAPOL-Key spécifié à la Section 4 utilise le même matériel de chiffrement (MS-MPPE-Recv-Key) pour chiffrer le champ Clé au sein du descripteur EAPOL-Key, et pour chiffrer les données passées entre la station et le point d'accès. Le matériel de chiffrement multi objets est déconseillé, car des utilisations multiples peuvent faire fuir des informations utiles à un attaquant.

[3] Algorithmes faibles. L'algorithme utilisé pour chiffrer le champ Clé au sein du descripteur EAPOL-Key est similaire à l'algorithme utilisé dans WEP, et par suite, partage certaines des mêmes faiblesses. Comme avec WEP, le chiffrement de flux RC4 est utilisé pour chiffrer la clé. En entrée au moteur RC4, la IV et la clé sont enchaînées plutôt que d'être combinées au sein d'une fonction de mixage. Comme avec WEP, la IV n'est pas un compteur, et donc il n'y a que peu de protection contre la réutilisation.

Par suite de ces vulnérabilités, les mises en œuvre qui ont l'intention d'utiliser le descripteur EAPOL-Key présenté dans ce document sont invitées à consulter la spécification 802.11 de sécurité améliorée pour une solution de remplacement plus sûre. Il est aussi conseillé de consulter l'évolution de la littérature sur les vulnérabilités de WEP, afin de mieux comprendre les risques, ainsi que pour obtenir des conseils sur le réglage approprié de l'intervalle de changement de clé.

6. Considérations relatives à l'IANA

La présente spécification ne crée aucun attribut RADIUS ni nouvel espace de numéros pour l'administration de l'IANA. Cependant, elle requiert l'allocation de nouvelles valeurs aux attributs RADIUS existants. Cela inclut :

Attribut	**Valeurs requises**
NAS-Port-Type	Token-Ring (20), FDDI (21)
Tunnel-Type	VLAN (13)
Acct-Terminate-Cause	Supplicant Restart (19)
	Reauthentication Failure (20)
	Port Reinitialized (21)
	Port Administratively Disabled (22)

8. Références

[Arbaugh] Arbaugh, W., Shankar, N. et J.Y.C. Wan, "Your 802.11 Wireless Network has No Clothes", Department of Computer Science, University of Maryland, College Park, mars 2001.

[Berkeley] Borisov, N., Goldberg, I. et D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11", ACM SIGMOBILE, Seventh Annual International Conference on Mobile Computing et Networking, juillet 2001, Rome, Italie.

[Fluhrer] Fluhrer, S., Mantin, I. et A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4", Eighth Annual Workshop on Selected Areas in Cryptography, Toronto, Canada, août 2001.

[IEEE8021X] IEEE Standards for Local et Metropolitan Area Networks: Port based Network Access Control, IEEE Std 802.1X-2001, juin 2001.

[IEEE802] IEEE Standards for Local et Metropolitan Area Networks: Overview et Architecture, ANSI/IEEE Std 802, 1990.

[IEEE8021Q] IEEE Standards for Local et Metropolitan Area Networks: Draft Standard for Virtual Bridged Local Area Networks, P802.1Q, janvier 1998.

[IEEE8023] ISO/IEC 8802-3, "Information technology - Telecommunications et information exchange between systems - Local et metropolitan area networks - Common specifications - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method et Physical Layer Specifications", (aussi ANSI/IEEE Std 802.3-1996), 1996.

[IEEE80211]IEEE Std. 802.11-1999, "Information technology - Telecommunications et information exchange between systems - Local et metropolitan area networks - Specific Requirements Part 11: Wireless LAN Medium

Access Control (MAC) et Physical Layer (PHY) Specifications", 1999.

[RFC1321] R. Rivest, "Algorithme de résumé de message MD5", avril 1992. *(Information)*

[RFC2104] H. Krawczyk, M. Bellare et R. Canetti, "HMAC : Hachage de clés pour l'authentification de message", février 1997.

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

[RFC2284] L. Blunk, J. Vollbrecht, "Protocole extensible d'authentification (EAP) en PPP", mars 1998. (*Obs., voir* RFC3748) *(P.S.)*

[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)

[RFC2548] G. Zorn, "Attributs Microsoft spécifiques du fabricant pour RADIUS", mars 1999. *(Information)*

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

[RFC2716] B. Aboba, D. Simon, "Protocole d'authentification des TLS d'EAP dans PPP" octobre 1999. (*Obs., voir* RFC5216) *(Exp.)*

[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)*

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

[RFC3280] R. Housley, W. Polk, W. Ford et D. Solo, "Profil de certificat d'infrastructure de clé publique X.509 et de liste de révocation de certificat (CRL) pour l'Internet", avril 2002. *(Obsolète, voir* RFC5280)

[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)*

[Stubbl] Stubblefield, A., Ioannidis, J. et A. Rubin, "Using the Fluhrer, Mantin et Shamir Attack to Break WEP", 2002 NDSS Conference.

8. Tableau des attributs

Le tableau qui suit précise quels attributs PEUVENT être envoyés et reçus au titre de l'authentification IEEE 802.1X. L3 note les attributs qui exigent des capacités de couche 3, et peuvent donc n'être pas pris en charge par tous les authentificateurs. Pour chaque attribut, la référence donne les informations normatives sur l'utilisation.

N°	Attribut	802.1X	Référence
1	User-Name	X	[RFC2865]
2	User-Password		[RFC2865]
3	CHAP-Password		[RFC2865]
4	NAS-IP-Address	X	[RFC2865]

5	NAS-Port	X	[RFC2865]
6	Service-Type	X	[RFC2865]
7	Framed-Protocol		[RFC2865]
8	Framed-IP-Address	L3	[RFC2865]
9	Framed-IP-Netmask	L3	[RFC2865]
10	Framed-Routing	L3	[RFC2865]
11	Filter-Id	X	[RFC2865]
12	Framed-MTU	X	[RFC2865]
13	Framed-Compression		[RFC2865]
14	Login-IP-Host	L3	[RFC2865]
15	Login-Service	L3	[RFC2865]
16	Login-TCP-Port	L3	[RFC2865]
18	Reply-Message		[RFC2865]
19	Callback-Number		[RFC2865]
20	Callback-Id		[RFC2865]
22	Framed-Route	L3	[RFC2865]
23	Framed-IPX-Network	L3	[RFC2865]
24	State	X	[RFC2865]
25	Class	X	[RFC2865]
26	Vendor-Specific	X	[RFC2865]
27	Session-Timeout	X	[RFC2865]
28	Idle-Timeout	X	[RFC2865]
29	Termination-Action	X	[RFC2865]
30	Called-Station-Id	X	[RFC2865]
31	Calling-Station-Id	X	[RFC2865]
32	NAS-Identifier	X	[RFC2865]
33	Proxy-State	X	[RFC2865]
34	Login-LAT-Service		[RFC2865]
35	Login-LAT-Node		[RFC2865]
36	Login-LAT-Group		[RFC2865]
37	Framed-AppleTalk-Link	L3	[RFC2865]
38	Framed-AppleTalk-Network	L3	[RFC2865]
39	Framed-AppleTalk-Zone	L3	[RFC2865]
40	Acct-Status-Type	X	[RFC2866]
41	Acct-Delay-Time	X	[RFC2866]
42	Acct-Input-Octets	X	[RFC2866]
43	Acct-Output-Octets	X	[RFC2866]
44	Acct-Session-Id	X	[RFC2866]
45	Acct-Authentic	X	[RFC2866]
46	Acct-Session-Time	X	[RFC2866]
47	Acct-Input-Packets	X	[RFC2866]
48	Acct-Output-Packets	X	[RFC2866]
49	Acct-Terminate-Cause	X	[RFC2866]
50	Acct-Multi-Session-Id	X	[RFC2866]
51	Acct-Link-Count	X	[RFC2866]
52	Acct-Input-Gigawords	X	[RFC2869]
53	Acct-Output-Gigawords	X	[RFC2869]
55	Event-Timestamp	X	[RFC2869]
60	CHAP-Challenge		[RFC2865]
61	NAS-Port-Type	X	[RFC2865]
62	Port-Limit		[RFC2865]
63	Login-LAT-Port		[RFC2865]
64	Tunnel-Type	X	[RFC2868]
65	Tunnel-Medium-Type	X	[RFC2868]
66	Tunnel-Client-Endpoint	L3	[RFC2868]
67	Tunnel-Server-Endpoint	L3	[RFC2868]
68	Acct-Tunnel-Connection	L3	[RFC2867]
69	Tunnel-Password	L3	[RFC2868]
70	ARAP-Password		[RFC2869]
71	ARAP-Features		[RFC2869]
72	ARAP-Zone-Access		[RFC2869]
73	ARAP-Security		[RFC2869]

74	ARAP-Security-Data		[RFC2869]
75	Password-Retry		[RFC2869]
76	Prompt		[RFC2869]
77	Connect-Info	X	[RFC2869]
78	Configuration-Token	X	[RFC2869]
79	EAP-Message	X	[RFC3579]
80	Message-authentificateur	X	[RFC3579]
81	Tunnel-Private-Group-ID	X	[RFC2868]
82	Tunnel-Assignment-ID	L3	[RFC2868]
83	Tunnel-Preference	X	[RFC2868]
84	ARAP-Challenge-Response		[RFC2869]
85	Acct-Interim-Interval	X	[RFC2869]
86	Acct-Tunnel-Packets-Lost	X	[RFC2867]
87	NAS-Port-Id	X	[RFC2869]
88	Framed-Pool	L3	[RFC2869]
90	Tunnel-Client-Auth-ID	L3	[RFC2868]
91	Tunnel-Server-Auth-ID	L3	[RFC2868]
95	NAS-IPv6-Address	X	[RFC3162]
96	Framed-Interface-Id		[RFC3162]
97	Framed-IPv6-Prefix	L3	[RFC3162]
98	Login-IPv6-Host	L3	[RFC3162]
99	Framed-IPv6-Route	L3	[RFC3162]
100	Framed-IPv6-Pool	L3	[RFC3162]
101	Error-Cause	X	[RFC3576]

Légende
X = Peut être utilisé avec l'authentification IEEE 802.1X
L3 = Seulement mis en œuvre par des authentificateurs qui ont des capacités de couche 3.

9. 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.

10. Remerciements

Les auteurs tiennent à remercier Bob O'Hara de Airespace, David Halasz de Cisco, Tim Moore, Sachin Seth et Ashwin Palekar de Microsoft, Andrea Li, Albert Young et Dave Bagby de 3Com de leurs contributions au présent document.

11. Adresse des auteurs

Paul Congdon
Hewlett Packard Company
HP ProCurve Networking
8000 Foothills Blvd, M/S 5662

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Andrew Smith
Trapeze Networks
5753 W. Las Positas Blvd.
Pleasanton, CA 94588-4084

Roseville, CA 95747
téléphone : +1 916 785 5753
mél : paul_congdon@hp.com

téléphone : +1 425 706 6605
mél : bernarda@microsoft.com

Fax: +1 415 345 1827
mél : ah_smith@acm.org

Glen Zorn
Cisco Systems, Inc.
500 108th Avenue N.E., Suite 500
Bellevue, WA 98004
téléphone : +1 425 438 8218
mél : gwz@cisco.com

John Roese
Enterasys
téléphone : +1 603 337 1506
mél : jjr@enterasys.com

12. Déclaration complète de droits de reproduction

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