Groupe de travail Réseau
Request for Comments : 2869
Catégorie : Information
Traduction Claude Brière de L'Isle

C. Rigney, Livingston
W. Willats, Cyno Technologies
P. Calhoun, Sun Microsystems
juin 2000

Extensions RADIUS

Résumé
Le présent document décrit des attributs supplémentaires pour porter les informations d'authentification, d'autorisation et de comptabilité entre un serveur d'accès réseau (NAS, *Network Access Server*) et un serveur de comptabilité partagé utilisant le protocole du service d'authentification distante d'utilisateur appelant (RADIUS, *Remote Authentication Dial In User Service*) décrit dans les [RFC2865] et [RFC2866].

Table des Matières

1. Introduction

La [RFC2865] décrit le protocole RADIUS comme il est mis en œuvre et déployé aujourd'hui, et la [RFC2866] décrit comment la comptabilité peut être tenue avec RADIUS.

Le présent mémoire suggère plusieurs attributs supplémentaires qui peuvent être ajoutés à RADIUS pour effectuer diverses fonctions utiles. Ces attributs n'ont pas encore un champ d'expérience très large et devraient donc être considérés comme expérimentaux.

Le protocole extensible d'authentification (EAP, *Extensible Authentication Protocol*) [RFC2284] est une extension à PPP qui assure la prise en charge de méthodes d'authentification supplémentaires au sein de PPP. Le présent mémoire décrit comment les attributs EAP-Message et Message-Authenticator peuvent être utilisés pour assurer la prise en charge de EAP au sein de RADIUS.

Tous les attributs sont composés de triplets type-longueur-valeur (TLV, *Type-Length-Value*) de longueur variable. De nouvelles valeurs d'attributs pourront être ajoutées sans perturber les mises en œuvre existantes du protocole.

1.1 Spécification des exigences

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].

Une mise en œuvre n'est pas conforme si elle ne satisfait pas à une ou plusieurs des exigences "DOIT" ou "NE DOIT PAS" pour le protocole qu'elle met en œuvre. Une mise en œuvre qui satisfait à toutes les exigences marquées "DOIT", "NE DOIT PAS", "DEVRAIT" et "NE DEVRAIT PAS" pour ses protocoles est dite être "inconditionnellement conforme" ; une mise en œuvre qui satisfait à toutes les exigences marquées "DOIT" et "NE DOIT PAS" mais pas toutes les exigences marquées "DEVRAIT" ou "NE DEVRAIT PAS" pour ses protocoles est dite être "conditionnellement conforme."

Un NAS qui ne met pas en œuvre un certain service NE DOIT PAS mettre en œuvre les attributs RADIUS pour ce service. Par exemple, un NAS qui n'est pas capable d'offrir le service ARAP NE DOIT PAS mettre en œuvre les attributs RADIUS pour ARAP. Un NAS DOIT traiter une demande d'accès RADIUS qui demande un service indisponible comme un rejet d'accès.

1.2 Terminologie

Le présent document utilise les termes suivants :

service : le NAS fournit un service à l'usager appelant, comme PPP ou Telnet.

session : chaque service fourni par le NAS à un usager appelant constitue une session, dont le début est défini comme le point où le service est fourni en premier et la fin de la session est définie comme le point où le service se termine. Un usager peut avoir plusieurs sessions en parallèle ou à la suite si le NAS l'accepte, chaque session générant un enregistrement séparé de début et de fin de comptabilité.

éliminer en silence : cela signifie que la mise en œuvre élimine le paquet sans autre traitement. La mise en œuvre DEVRAIT fournir la capacité d'enregistrer les erreurs, y compris le contenu des paquets éliminés en silence, et DEVRAIT enregistrer l'événement dans un compteur de statistiques.

2. Fonctionnement

Le fonctionnement est identique à celui défini dans les [RFC2865] et [RFC2866].

2.1 Prise en charge par RADIUS des mises à jour intermédiaires de comptabilité

Lorsque un usager est authentifié, un serveur RADIUS produit un Access-Accept *(accès accepté)* en réponse à une Access-

Request *(demande d'accès)* réussie. Si le serveur souhaite recevoir des messages comptables intermédiaires pour un certain usager, il doit inclure l'attribut RADIUS Acct-Interim-Interval dans le message, qui indique l'intervalle en secondes entre les messages intermédiaires

Il est aussi possible de configurer statiquement une valeur intermédiaire dans le NAS lui-même. Noter qu'une valeur configurée en local sur le NAS DOIT prendre le pas sur la valeur qui se trouve dans un Access-Accept.

Ce schéma ne rompt pas la rétro compatibilité car un serveur RADIUS qui ne prend pas en charge cette extension n'ajoutera tout simplement pas le nouvel attribut. Les NAS qui ne prennent pas en charge cette extension vont ignorer l'attribut.

Noter que toutes les informations dans un message intermédiaire sont cumulatives (c'est-à-dire que le nombre de paquets envoyés est le total depuis le début de la session, et non depuis le dernier message intermédiaire).

Il est envisagé que tout enregistrement intermédiaire de comptabilité (avec Acct-Status-Type = Interim-Update (3)) contienne tous les attributs qui se trouvent normalement dans un message Arrêt de comptabilité *(Accounting Stop)* à l'exception de l'attribut Acct-Term-Cause *(cause de la terminaison de la comptabilité)*.

Comme toutes les informations sont cumulatives, un NAS DOIT s'assurer qu'une seule génération d'un message de comptabilité intermédiaire est présente pour une certaine session dans la file d'attente de retransmission à chaque instant.

Un NAS PEUT utiliser un facteur de cadrage pour ajouter un retard aléatoire entre les messages de comptabilité intermédiaires pour des sessions séparées. Cela va assurer que ne se produira pas un cycle où tous les messages sont envoyés en une seule fois, comme cela pourrait autrement se produire si une liaison principale était restaurée et que de nombreux usagers appelants étaient dirigés d'un coup sur le même NAS.

La charge de CPU du réseau et du NAS pour l'utilisation des mises à jour intermédiaires devrait être considérée avec attention, et des valeurs appropriées de Acct-Interim-Interval devraient être choisies.

2.2 Prise en charge par RADIUS du protocole d'accès distant d'Apple

Le protocole RADIUS donne une méthode qui permet que plusieurs serveurs d'accès réseau (NAS) partagent une base de données d'authentification commune.

Le protocole Apple d'accès à distance (ARAP, *Apple Remote Access Protocol*) donne une méthode pour envoyer du trafic réseau AppleTalk sur des liaisons point à point, normalement, mais pas exclusivement, asynchrones, et des connexions RNIS à commutation de circuit. Bien que Apple passe sur ATCP on PPP pour les futurs services d'accès distant, ARAP est encore une façon courante pour que les utilisateurs de la base installée de Macintosh effectuent leurs connexions réseaux à distance, et va probablement le rester pendant un certain temps.

ARAP est pris en charge par plusieurs fabricants de NAS qui prennent aussi en charge PPP, IPX et d'autres protocoles dans le même NAS. Les connexions ARAP dans ces appareils multi protocoles sont souvent non authentifiées avec RADIUS, ou si elles le sont, chaque fabricant crée une solution individuelle pour le problème.

La présente section décrit l'utilisation d'attributs RADIUS supplémentaires pour prendre en charge ARAP. Les mises en œuvre de clients et serveurs RADIUS de la présente spécification devraient être capables d'authentifier les connexions ARAP d'une façon interopérable.

Cette section suppose la connaissance de RADIUS, et va entrer dans les détails du fonctionnement de ARAP avant de procéder à une discussion détaillée des attributs ARAP RADIUS proposés.

Deux caractéristiques de ARAP ne sont pas traitées dans le présent document :

1. Changement de mot de passe à l'initiative de l'usager. Ceci ne fait pas partie de RADIUS, mais peut être mis en œuvre par un processus logiciel autre que RADIUS.

2. Messages hors bande. À tout moment, le NAS peut envoyer à un client ARA des messages qui apparaissent dans une boîte de dialogue sur l'écran de l'usager appelant. Ceci ne fait pas partie de l'authentification et n'est pas traité ici. Cependant, on note qu'un attribut Reply-Message *(message de réponse)* dans un Access-Accept peut être passé à l'usager comme un message de signature de la chaîne ordinaire en utilisant le canal hors bande.

On a essayé de respecter autant que possible l'esprit du protocole RADIUS existant en prenant des décisions de conception compatibles avec les pratiques courantes. De plus, on a essayé de garder un équilibre entre inonder le monde RADIUS de

nouveaux attributs, et cacher tout le fonctionnement de ARAP au sein d'une seule chaîne d'attributs ARAP multiplexée ou au sein d'une mécanique du protocole étendu d'authentification (EAP) [RFC2284].

Cependant, on estime que ARAP s'appuie suffisamment sur PPP pour garantir un petit ensemble en propre d'attributs de noms similaires.

On a supposé qu'un serveur RADIUS à capacité ARAP sera capable de faire le chiffrement DES et générer des mises en cause de module de sécurité. Cela est conforme au but général de RADIUS d'un serveur intelligent et d'un NAS simple.

ARAP authentifie une connexion en deux phases. La première est un échange de nombres aléatoires "DES bidirectionnel", utilisant le mot de passe de l'usager comme clé. On dit "bidirectionnel" parce que le NAS ARAP met au défi le client appelant de s'authentifier, et le client appelant met au défi le NAS ARAP de s'authentifier.

Spécifiquement, ARAP fait ce qui suit :

1. Le NAS envoie des nombres aléatoires de 32 bits au client appelant dans un paquet ARAP msg_auth_challenge.

2. Le client appelant utilise le mot de passe de l'usager pour chiffrer en DES les deux nombres aléatoires qui lui ont été envoyés par le NAS. Le client appelant renvoie alors au NAS ce résultat, le nom de l'usager et deux nombres aléatoires de 32 bits de son cru dans un paquet ARAP msg_auth_request.

3. Le NAS vérifie que les nombres aléatoires chiffrés envoyés par le client appelant sont ce qu'il attendait. Si c'est le cas, il chiffre le défi du client appelant en utilisant le mot de passe et le renvoie au client appelant dans un paquet ARAP msg_auth_response.

Noter que si la réponse du client appelant était fausse, ce qui signifie que l'usager a un mauvais mot de passe, le serveur peut initier une séquence de réessai jusqu'au compte maximum de réessais permis par le NAS. Dans ce cas, lorsque le client appelant reçoit le paquet ARAP msg_auth_response, il va en accuser réception avec un paquet ARAP msg_auth_again.

Après cette première "phase DES" le NAS ARAP PEUT initier une phase d'authentification secondaire en utilisant ce que Apple appelle des "modules de sécurité ajoutés". Les modules de sécurité sont de petits morceaux de code qui fonctionnent à la fois chez le client et le serveur et qui ont la permission de lire et écrire des données arbitraires à travers la liaison de communications pour effectuer des fonctions d'authentification supplémentaires. Divers fabricants de jetons de sécurité utilisent ce mécanisme pour authentifier les appelants ARA.

Bien que ARAP permette que des modules de sécurité lisent et écrivent ce qu'ils veulent, tous les modules de sécurité existants utilisent de simples cycles de défi réponse, avec peut-être des informations de contrôle globales. Le présent document suppose que tous les modules de sécurité existants peuvent être pris en charge avec un ou plusieurs cycles de défi/réponse.

Pour compliquer l'intégration de RADIUS et d'ARAP, ARAP envoie des informations de profil après la phase DES et avant la phase de module de sécurité. Cela signifie qu'à côté des réponses aux défis, ces informations de profil doivent aussi être présentes, à des moments parfois inattendus. Heureusement, ces informations ne sont que de petits morceaux de données numériques relatives aux mots de passe, que le présent document englobe dans un seul nouvel attribut.

La présentation d'une Access-Request à RADIUS au nom d'une connexion ARAP est directe. Le NAS ARAP génère le nombre aléatoire du défi, et reçoit ensuite la réponse du client appelant, le défi du client appelant, et le nom de l'usager. En supposant que l'usager n'est pas un invité, les informations suivantes sont transmises dans un paquet Access-Request : User-Name (jusqu'à 31 caractères de long), Framed-Protocol (réglé à 3, ARAP), ARAP-Password, et tous les attributs supplémentaires désirés, comme Service-Type, NAS-IP-Address, NAS-Id, NAS-Port-Type, NAS-Port, NAS-Port-Id, Connect-Info, etc.

L'authentifiant de demande est un nombre aléatoire de 16 octets généré par le NAS. Les 8 octets de moindre poids de ce nombre sont envoyés à l'usager appelant comme les deux nombres aléatoires de quatre octets requis dans le paquet ARAP msg_auth_challenge. Les octets 0 à 3 sont le premier nombre aléatoire et les octets 4 à 7 sont le second nombre aléatoire.

Le mot de passe ARAP dans la demande d'accès contient un nombre aléatoire de 16 octets, et il est utilisé pour porter la réponse de l'usager au défi du NAS et le propre défi du client au NAS. Les octets de poids fort contiennent le défi de l'usager appelant au NAS (2 nombres de 32 bits, 8 octets) et les octets de moindre poids contiennent la réponse de l'usager appelant au défi du NAS (2 nombres de 32 bits, 8 octets).

Un seul de User-Password, CHAP-Password, ou ARAP-Password doit être présent dans une demande d'accès, ou un ou plusieurs messages EAP.

Si le serveur RADIUS ne prend pas en charge ARAP, il DEVRAIT retourner un Access-Reject au NAS.

Si le serveur RADIUS prend en charge ARAP, il devrait vérifier la réponse de l'usager en utilisant le défi (d'après les 8 octets de moindre poids de l'authentifiant de demande) et la réponse de l'usager (d'après les 8 octets de moindre poids du mot de passe ARAP).

Si l'authentification échoue, le serveur RADIUS devrait retourner un paquet Access-Reject au NAS, avec les attributs facultatifs Password-Retry et Reply-Messages. La présence de Password-Retry indique que le NAS ARAP PEUT choisir d'initier un autre cycle défi-réponse, jusqu'au nombre total de fois égal à la valeur d'entier de l'attribut Password-Retry.

Si l'usager est authentifié, le serveur RADIUS devrait retourner un paquet Access-Accept (code 2) au NAS, avec l'ID et l'authentifiant de réponse comme d'habitude, et les attributs comme suit :

Service-Type de Framed-Protocol.

Framed-Protocol de ARAP (3).

Session-Timeout avec le temps maximum de connexion pour l'usager en secondes. Si un temps non limité est donné à l'usager, Session-Timeout ne devrait pas être inclus dans le paquet Access-Accept, et ARAP traitera cela comme une temporisation illimitée (-1).

ARAP-Challenge-Response, contient 8 octets avec la réponse au défi du client appelant. Le serveur RADIUS calcule cette valeur en prenant le défi du client appelant d'après les 8 octets de poids fort de l'attribut ARAP-Password et en effectuant le chiffrement DES sur cette valeur avec le mot de passe de l'usager qui s'authentifie comme clé. Si le mot de passe de l'usager fait moins de 8 octets, le mot de passe est bourré à la fin avec des octets NUL à une longueur de 8 octets avant de l'utiliser comme clé. Si le mot de passe de l'usager fait plus de 8 octets, un Access-Reject DOIT être envoyé.

ARAP-Features, contient les informations que le NAS devrait envoyer à l'usager dans un paquet ARAP "feature flags".

Octet 0 : s'il est à zéro, l'usager ne peut pas changer le mot de passe. S'il il n'est pas à zéro l'usager le peut. (RADIUS ne traite pas le changement de mot de passe, juste l'attribut qui indique si ARAP indique qu'il le peut.)

Octet 1 : longueur minimum acceptable du mot de passe (0-8).

Octets 2-5 : date de création du mot de passe en format Macintosh, défini comme 4 octets non signés représentant les secondes depuis le 1er janvier 1904 à minuit en GMT.

Octets 6-9 : différence d'expiration de mot de passe depuis la date de création en secondes.

Octets 10-13 : heure RADIUS actuelle en format Macintosh.

Facultativement un seul message de réponse avec une chaîne de texte faisant jusqu'à 253 caractères qui PEUT être envoyé à l'usager pour être affiché dans une signature/message du dialogue.

Framed-AppleTalk-Network peut être inclus.

Framed-AppleTalk-Zone, jusqu'à 32 caractères, peut être inclus.

ARAP définit la notion d'une liste de zones pour un usager. Avec une liste de noms de zones, un fanion Zone Access est défini (et utilisé par le NAS) qui dit comment utiliser la liste des noms de zones. C'est-à-dire, l'usager appelant peut seulement être autorisé à voir la zone par défaut, ou seulement les zones dans la liste des zones (inclusive) ou toute zone excepté celles de la liste des zones (exclusive).

Le NAS ARAP traite cela en ayant un filtre désigné qui contient (au moins) les noms de zones. Cela résout le problème où un seul serveur RADIUS gère des NAS clients disparates qui peuvent n'être pas capables de "voir" tous les noms de zone dans une liste de zones d'utilisateur. Les noms de zones n'ont de signification que "au NAS". L'inconvénient de cette approche est que ces filtres de zones doivent d'une certaine manière être établis sur le NAS, puis référencés par l'identifiant de filtre RADIUS.

ARAP-Zone-Access contient un entier qui spécifie comment la "liste des zones" pour cet utilisateur pourrait être utilisée. Si cet attribut est présent et si la valeur est 2 ou 4, un identifiant de filtre doit alors aussi être présent pour désigner un filtre de liste de zone auquel le fanion d'accès va s'appliquer.

L'inclusion d'un attribut Callback-Number ou Callback-Id dans le Access-Accept PEUT causer la déconnexion du NAS ARAP après l'envoi des fanions de caractéristiques pour commencer un traitement du rappel spécifique d'ARAP.

D'autres attributs peuvent aussi être présents dans le paquet Access-Accept.

Un NAS ARAP aura besoin d'autres informations pour finir l'établissement de la connexion avec le client appelant, mais ces informations peuvent être fournies par le NAS ARAP sans aucune aide de la part de RADIUS, soit par configuration par SNMP, par un programme d'administration de NAS, soit déduites par la pile AppleTalk dans le NAS. Précisément :

1. Les valeurs AppearAsNet et AppearAsNode envoyées au client pour lui dire quels numéros de réseau et de nœud il devrait utiliser dans ses paquets de datagrammes. AppearAsNet peut être pris de l'attribut Framed-AppleTalk-Network ou de la configuration ou de la pile AppleTalk sur le NAS.

2. La zone par "défaut" – qui est le nom de la zone AppleTalk dans laquelle le client appelant va apparaître. (Ou peut être spécifié avec l'attribut Framed-AppleTalk-Zone.)

3. Autres matériaux très spécifiques de NAS comme le nom du NAS, et des informations de "bourrage intelligent" *(smartbuffering)*. (Le "bourrage intelligent" est un mécanisme ARAP pour remplacer des datagrammes AppleTalk courants par de petits jetons, pour améliorer les performances de liaisons lentes dans quelques situations de trafic courantes.)

4. Informations de "liste de zone" pour cet utilisateur. La spécification ARAP définit un champ "compte de zone" qui est actuellement non utilisé.

RADIUS prend en charge les modules de sécurité ARAP de la manière suivante :

Après l'achèvement de l'authentification DES, le serveur RADIUS peut donner pour instruction au NAS ARAP de faire fonctionner un ou plusieurs modules de sécurité pour l'usager appelant. Bien que le protocole sous-jacent prenne en charge l'exécution en série de plusieurs modules de sécurité, en pratique, toutes les mises en œuvre courantes ne permettent d'en exécuter qu'une seule. Par l'utilisation de plusieurs demandes Access-Challenge, plusieurs modules peuvent être pris en charge, mais cette facilité ne sera probablement jamais utilisée.

On suppose aussi que, bien que ARAP permette un dialogue de forme libre entre modules de sécurité sur chaque extrémité de la liaison point à point, dans la pratique actuelle tous les modules de sécurité peuvent être réduits à un simple cycle de défi/réponse.

Si le serveur RADIUS souhaite donner pour instruction au NAS ARAP de faire fonctionner un module de sécurité, il devrait envoyer un paquet Access-Challenge au NAS avec (facultativement) l'attribut State, plus le ARAP-Challenge-Response, le ARAP-Features, et deux attributs de plus :

ARAP-Security : une signature de module de sécurité de quatre octets, contenant un type OST Macintosh,

ARAP-Security-Data : une chaîne portant le défi/réponse réel du module de sécurité.

Lorsque le module de sécurité a fini de s'exécuter, la réponse du module de sécurité est passée dans un attribut ARAP-Security-Data du NAS au serveur RADIUS dans une seconde Access-Request, incluant aussi l'état provenant du Access-Challenge. Le champ Authentificateur ne contient aucune information particulière dans ce cas, et ceci peut être discerné par la présence de l'attribut State.

2.3 Prise en charge par RADIUS du protocole d'authentification extensible (EAP)

Le protocole extensible d'authentification (EAP, *Extensible Authentication Protocol*) décrit dans la [RFC2284], fournit un mécanisme normalisé pour prendre en charge des méthodes d'authentification supplémentaires dans PPP. Par l'usage de EAP, la prise en charge d'un certain nombre de schémas d'authentification peut être ajoutée, incluant des cartes à mémoire, Kerberos, une clé publique, des mots de passe à utilisation unique, et autres. Afin d'assurer la prise en charge de EAP dans RADIUS, deux nouveaux attributs, EAP-Message et Message-Authenticator, sont introduits dans le présent document. Ce paragraphe décrit comment ces nouveaux attributs peuvent être utilisés pour assurer la prise en charge d'EAP dans RADIUS.

Dans le schéma proposé, le serveur RADIUS est utilisé pour porter les paquets EAP encapsulés dans RADIUS entre le NAS et un serveur de sécurité arrière. Bien que la conversation entre le serveur RADIUS et le serveur de sécurité arrière se

produise normalement en utilisant un protocole propriétaire développé par le fabricant du serveur de sécurité arrière, il est aussi possible d'utiliser EAP encapsulé dans RADIUS via l'attribut EAP-Message. Cela a l'avantage de permettre que le serveur RADIUS prenne en charge EAP sans qu'il soit besoin d'un code spécifique d'authentification, qui peut à la place résider sur le serveur de sécurité arrière.

2.3.1 Vue d'ensemble du protocole

La conversation EAP entre l'homologue qui s'authentifie (usager appelant) et le NAS commence par la négociation de EAP dans LCP. Une fois que EAP a été négocié, le NAS DOIT envoyer un message EAP-Request/Identity à l'homologue qui s'authentifie, sauf si l'identité est déterminée via d'autres moyens tels que Called-Station-Id ou Calling-Station-Id. L'homologue va alors répondre par une EAP-Response/Identity que le NAS va transmettre au serveur RADIUS dans l'attribut EAP-Message d'un paquet RADIUS Access-Request. Le serveur RADIUS va normalement utiliser EAP-Response/Identity pour déterminer quel type EAP est à appliquer à l'usager.

Afin de permettre à des mandataires RADIUS sans capacité EAP de transmettre le paquet Access-Request, si le NAS envoie la EAP-Request/Identity, le NAS DOIT copier le contenu de EAP-Response/Identity dans l'attribut User-Name et DOIT inclure la EAP-Response/Identity dans l'attribut User-Name dans chaque Access-Request suivante. NAS-Port ou NAS-Port-Id DEVRAIT être inclus dans les attributs produits par le NAS dans le paquet Access-Request, et NAS-Identifier ou NAS-IP-Address DOIT être inclus. Afin de permettre la transmission de la Access-Reply par les mandataires sans capacité EAP, si un attribut User-Name était inclus dans une Access-Request, le serveur RADIUS DOIT inclure l'attribut User-Name dans les paquets Access-Accept suivants. Sans l'attribut User-Name, la comptabilité et la facturation deviennent très difficiles à gérer.

Si l'identité est déterminée via d'autres moyens tels que Called-Station-Id ou Calling-Station-Id, le NAS DOIT inclure ces attributs d'identification dans chaque Access-Request.

Bien que cette approche économise un aller-retour, elle ne peut pas être universellement employée. Il y a des circonstances où l'identité de l'usager n'est pas nécessaire (comme lorsque l'authentification et la comptabilité sont traitées sur la base de Called-Station-Id ou Calling-Station-Id) et donc un paquet EAP-Request/Identity n'est pas nécessairement produit par le NAS pour l'homologue qui s'authentifie. Dans les cas où un paquet EAP-Request/Identity n'est pas envoyé, le NAS va envoyer au serveur RADIUS un paquet RADIUS Access-Request contenant un attribut EAP-Message signifiant EAP-Start. EAP-Start est indiqué par l'envoi d'un attribut EAP-Message d'une longueur de 2 (pas de données). Cependant, on notera que comme aucun attribut User-Name n'est inclus dans la Access-Request, cette approche n'est pas compatible avec RADIUS comme spécifié dans la [RFC2865], ni ne peut être facilement appliquée dans des situations où des mandataires sont déployés, comme en cas d'itinérance ou de réseau à utilisation partagée.

Si le serveur RADIUS prend en charge EAP, il DOIT répondre avec un paquet Access-Challenge contenant un attribut EAP-Message. Si le serveur RADIUS ne prend pas en charge EAP, il DOIT répondre avec un Access-Reject. L'attribut EAP-Message inclut un paquet EAP encapsulé qui est ensuite passé à l'homologue qui s'authentifie. Dans le cas où le NAS n'a pas envoyé initialement un message EAP-Request/Identity à l'homologue, le Access-Challenge va normalement contenir un attribut EAP-Message encapsulant un message EAP-Request/Identity, qui demande que l'usager appelant s'identifie. Le NAS va alors répondre avec un paquet RADIUS Access-Request contenant un attribut EAP-Message encapsulant une EAP-Response. La conversation continue jusqu'à ce que soit reçu un paquet RADIUS Access-Reject ou Access-Accept.

La réception d'un paquet RADIUS Access-Reject, avec ou sans un attribut EAP-Message encapsulant une EAP-Failure, DOIT avoir pour résultat que le NAS produit une demande LCP Terminate à l'homologue qui s'authentifie. Un paquet RADIUS Access-Accept avec un attribut EAP-Message encapsulant un EAP-Success termine avec succès la phase d'authentification. Le paquet RADIUS Access-Accept/EAP-Message/EAP-Success DOIT contenir tous les attributs attendus qui sont actuellement retournés dans un paquet Access-Accept.

Le scénario ci-dessus crée une situation dans laquelle le NAS n'a jamais besoin de manipuler un paquet EAP. Une solution de remplacement peut être utilisée dans des situations où un message EAP-Request/Identity va toujours être envoyé par le NAS à l'homologue qui s'authentifie.

Pour les demandes RADIUS qui passent par un mandataire , il y a deux méthodes de traitement. Si le domaine est déterminé sur la base du Called-Station-Id, le serveur RADIUS peut déléguer à un mandataire le Access-Request/EAP-Start RADIUS initial. Si le domaine est déterminé sur la base de l'identité de l'usager, le serveur RADIUS local DOIT répondre avec un paquet RADIUS Access-Challenge/EAP-Identity. La réponse de l'homologue qui s'authentifie DOIT être mandatée au serveur d'authentification final.

Pour les demandes RADIUS mandatées, le NAS peut recevoir un paquet Access-Reject en réponse à son paquet Access-

Request/EAP-Identity. Cela va se produire si le message a été mandaté à un serveur RADIUS qui ne prend pas en charge l'extension EAP-Message. À réception d'un Access-Reject, le NAS DOIT envoyer une demande LCP Terminate à l'homologue qui s'authentifie, et se déconnecter.

2.3.2 Retransmission

Comme noté dans la [RFC2284], l'authentificateur EAP (NAS) est chargé de la retransmission des paquets entre l'homologue authentifiant et le NAS. Donc si un paquet EAP est perdu dans le transit entre l'homologue qui s'authentifie et le NAS (ou vice versa) le NAS va retransmettre. Comme dans RADIUS [RFC2865], le client RADIUS est chargé de la retransmission des paquets entre le client RADIUS et le serveur RADIUS.

Noter qu'il peut être nécessaire d'ajuster les stratégies de retransmission et les temporisations d'authentification dans certains cas. Par exemple, lorsque une carte à jetons est utilisée, du temps supplémentaire peut être nécessaire pour permettre à l'usager de trouver la carte et entrer le jeton. Comme le NAS ne va normalement pas avoir connaissance des paramètres requis, ils doivent être fournis par le serveur RADIUS. Ceci peut se faire en incluant les attributs Session-Timeout et Password-Retry dans le paquet Access-Challenge.

Si Session-Timeout est présent dans un paquet Access-Challenge qui contient aussi un EAP-Message, la valeur de Session-Timeout donne au NAS le nombre maximum de secondes qu'il devrait attendre une EAP-Response avant de retransmettre le message EAP à l'usager appelant.

2.3.3 Fragmentation

En utilisant l'attribut EAP-Message, il est possible au serveur RADIUS d'encapsuler un paquet EAP qui est plus grand que la MTU sur la liaison entre le NAS et l'homologue. Comme il n'est pas possible que le serveur RADIUS utilise la découverte de MTU pour s'assurer de la MTU de la liaison, l'attribut Framed-MTU peut être inclus dans un paquet Access-Request contenant un attribut EAP-Message afin de fournir cette information au serveur RADIUS.

2.3.4 Exemples

L'exemple ci-dessous montre la conversation entre l'homologue qui s'authentifie, le NAS, et le serveur RADIUS, pour le cas d'une authentification par mot de passe à utilisation unique (OTP, *One Time Password*). OTP est seulement utilisé à des fins d'illustration ; d'autres protocoles d'authentification pourraient aussi être utilisés, mais ils présenteraient un comportement un peu différent.

Homologue s'authentifiant **NAS** **Serveur RADIUS**

<- auth PPP LCP Request-EAPauth PPP LCP ACK-EAP ->
<- PPP EAP-Request/Identity
PPP EAP-Response/Identity (MyID) ->
RADIUS Access-Request/EAP-Message/EAP-Response/(MyID) ->
<- RADIUS Access-Challenge/EAP-Message/EAP-Request OTP/défi OTP
<- PPP EAP-Request/OTP/défi OTP
PPP EAP-Response/OTP, OTPpw ->
RADIUS Access-Request/EAP-Message/EAP-Response/OTP, OTPpw ->
<- RADIUS Access-Accept/EAP-Message/ EAP-Success (autres attributs)
<- PPP EAP-Success
Phase d'authentification PPP achevée, début de phase NCP

Dans le cas où le NAS envoie d'abord un paquet EAP-Start au serveur RADIUS, la conversation apparaîtrait comme suit :

Homologue s'authentifiant **NAS** **Serveur RADIUS**

<- auth PPP LCP Request-EAP
auth PPP LCP ACK-EAP ->
RADIUS Access-Request/ EAP-Message/Start ->
<- RADIUS Access-Challenge/ EAP-Message/Identity
<- PPP EA-Request/Identity
PPP EAP-Response/Identity (MyID) ->
RADIUS Access-Request/EAP-Message/EAP-Response/(MyID) ->
<- RADIUS Access-Challenge/EAP-Message/EAP-Request OTP/défi OTP

<- PPP EAP-Request/OTP/OTP Challenge
PPP EAP-Response/OTP, OTPpw ->
RADIUS Access-Request/EAP-Message/EAP-Response/OTP, OTPpw ->
<- RADIUS Access-Accept/EAP-Message/EAP-Success
(autres attributs)
<- PPP EAP-Success
Phase d'authentification PPP achevée, début de phase NCP

Dans le cas où le client échoue à l'authentification EAP, la conversation apparaîtra comme suit :

Homologue s'authentifiant NAS Serveur RADIUS
<- auth PPP LCP Request-EAP
auth PPP LCP ACK-EAP ->
Access-Request/EAP-Message/Start ->
<- RADIUS Access-Challenge/EAP-Message/Identity
<- PPP EAP-Request/Identity
PPP EAP-Response/Identity (MyID) ->
RADIUS Access-Request/EAP-Message/EAP-Response/(MyID) ->
<- RADIUS Access-Challenge/EAP-Message/EAP-Request/OTP/défi OTP
<- PPP EAP-Request/OTP/OTP Challenge
PPP EAP-Response/OTP, OTPpw ->
RADIUS Access-Request/EAP-Message/EAP-Response/OTP, OTPpw ->
<- RADIUS Access-Reject/EAP-Message/EAP-Failure
<- PPP EAP-Failure (client déconnecté)

Dans le cas où le serveur ou mandataire RADIUS ne prend pas en charge EAP-Message, la conversation va apparaître comme suit :

Homologue s'authentifiant NAS Serveur RADIUS
<- auth PPP LCP Request-EAP
auth PPP LCP ACK-EAP ->
RADIUS Access-Request/EAP-Message/Start ->
<- RADIUS Access-Reject
<- PPP LCP Terminate (usager déconnecté)

Dans le cas où le serveur RADIUS local prend en charge EAP-Message, mais où le serveur RADIUS distant ne le fait pas, la conversation va apparaître comme suit :

Homologue s'authentifiant NAS Serveur RADIUS
<- auth PPP LCP Request-EAP
auth PPP LCP ACK-EAP ->
RADIUS Access-Request/EAP-Message/Start ->
<- RADIUS Access-Challenge/EAP-Message/Identity
<- PPP EAP-Request/Identity
PPP EAP-Response/Identity(MyID) ->
RADIUS Access-Request/EAP-Message/EAP-Response/(MyID) ->
<- RADIUS Access-Reject (mandaté par le serveur RADIUS distant)
<- PPP LCP Terminate (usager déconnecté)

Dans le cas où l'homologue qui s'authentifie ne prend pas en charge EAP, mais où EAP est exigé pour cet usager, la conversation va apparaître comme suit :

Homologue s'authentifiant NAS Serveur RADIUS
<- auth PPP LCP Request-EAP
auth PPP LCP NAK-EAP ->
<- auth PPP LCP Request-CHAP
auth PPP LCP ACK-CHAP ->
<- PPP CHAP Challenge
PPP CHAP Response ->
RADIUS Access-Request/User-Name, CHAP-Password ->
<- RADIUS Access-Reject
<- PPP LCP Terminate (usager déconnecté)

Dans le cas où le NAS ne prend pas en charge EAP, mais où EAP est exigé pour cet usager, la conversation va apparaître comme suit :

Homologue s'authentifiant	**NAS**	**Serveur RADIUS**
	<- auth PPP LCP Request-CHAP	
auth PP LCP ACK-CHAP ->		
	<- PPP CHAP Challenge	
PPP CHAP Response ->		
	RADIUS Access-Request/User-Name, CHAP-Password ->	
		<- RADIUS Access-Reject
	<- PPP LCP Terminate (usager déconnecté)	

2.3.5 Autres utilisations

Actuellement, la conversation entre le serveur de sécurité de l'arrière et le serveur RADIUS n'est pas normalisée. Afin d'augmenter la normalisation et assurer l'interopérabilité entre les fabricants RADIUS et les fabricants de sécurité arrière, il est recommandé que EAP encapsulé dans RADIUS soit utilisé pour cette conversation.

Cela présente l'avantage de permettre au serveur RADIUS de prendre en charge EAP sans avoir besoin de code spécifique d'authentification au sein du serveur RADIUS. Le code spécifique de l'authentification peut alors résider plutôt sur un serveur de sécurité arrière.

Dans le cas où EAP encapsulé dans RADIUS est utilisé dans une conversation entre un serveur RADIUS et un serveur de sécurité de l'arrière, celui-ci va normalement retourner un message Access-Accept/EAP-Success sans inclusion des attributs attendus actuellement retournés dans un Access-Accept. Cela signifie que le serveur RADIUS DOIT ajouter ces attributs avant d'envoyer un message Access-Accept/EAP-Success au NAS.

3. Format de paquet

Le format de paquet est identique à celui défini dans les [RFC2865] et [RFC2866].

4. Types de paquet

Les types de paquet sont identiques à ceux définis dans les [RFC2865] et [RFC2866].

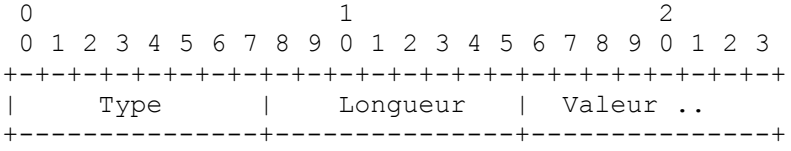
Voir au "Tableau des attributs" ci-dessous comment déterminer quels types de paquets peuvent contenir quels attributs définis ici.

5. Attributs

Les attributs RADIUS portent les détails spécifiques d'authentification, autorisation et comptabilité pour les demandes et réponses. Certains attributs PEUVENT être inclus plus d'une fois. L'effet en est spécifique de l'attribut, et est spécifié dans chaque description d'attribut. L'ordre des attributs de même type DEVRAIT être préservé. Il n'est pas obligé de préserver l'ordre des attributs de types différents.

La fin de la liste des attributs est indiquée par la longueur du paquet RADIUS.

Un sommaire du format des attributs, qui est le même que dans la [RFC2865] est inclus ici pour faciliter la référence. Les champs sont transmis de gauche à droite.



Type : le champ Type fait un octet. Les valeurs à jour du champ RADIUS Type sont spécifiées dans la plus récente RFC "Numéros alloués" [RFC1700]. Les valeurs 192 à 223 sont réservées pour les utilisations expérimentales, les valeurs 224 à 240 sont réservées pour les utilisations spécifiques de la mise en œuvre, et les valeurs 241 à 255 sont réservées et ne devraient pas être utilisées. La présente spécification concerne les valeurs suivantes :

1 à 39 (voir la [RFC2865], "RADIUS")
40 à 51 (voir la [RFC2866], "comptabilité RADIUS")
52 : Acct-Input-Gigawords *(grand mot d'entrée de comptabilité)*
53 : Acct-Output-Gigawords *(grand mot de résultat de comptabilité)*
54 : non utilisé
55 : Event-Timestamp *(horodatage d'événement)*
56-59 : non utilisé
60 à 63 : (voir la [RFC2865], "RADIUS")
64 à 67 : (voir la [RFC2868])
68 : (voir la [RFC2867])
69 : (voir la [RFC2868])
70 : ARAP-Password *(mot de passe ARAP)*
71 : ARAP-Features *(caractéristiques ARAP)*
72 : ARAP-Zone-Access *(accès de zone ARAP)*
73 : ARAP-Security *(sécurité ARAP)*
74 : ARAP-Security-Data *(données de sécurité ARAP)*
75 : Password-Retry *(nouvel essai du mot de passe)*
76 : Prompt *(invite)*
77 : Connect-Info *(informations de connexion)*
78 : Configuration-Token *(jeton de configuration)*
79 : EAP-Message *(message EAP)*
80 : Message-Authenticator *(authentificateur de message)*
81 à 83 : (voir la [RFC2868])
84 : ARAP-Challenge-Response *(défi-réponse ARAP)*
85 : Acct-Interim-Interval *(intervalle entre messages intérimaires de comptabilité)*
86 : (voir la [RFC2867])
87 : NAS-Port-Id *(identifiant d'accès de NAS)*
88 : Framed-Pool *(réservoir tramé)*
89 : non utilisé
90-91 : (voir la [RFC2868])
92 à 191 : non utilisé

Longueur : le champ Longueur fait un octet, et indique la longueur de cet attribut, incluant les champs Type, Longueur et Valeur. Si un attribut est reçu dans un paquet avec une longueur invalide, la demande entière devrait être éliminée en silence.

Valeur : le champ Valeur fait zéro, un ou plusieurs octets et contient des informations spécifiques de l'attribut. Le format et la longueur du champ Valeur sont déterminés par les champs Type et Longueur. Noter que dans RADIUS aucun de ces types ne se termine par un NUL (hex 00). En particulier, les types "text" et "string" dans RADIUS ne se terminent pas par un NUL (hex 00). L'attribut a un champ Longueur et n'utilise pas de terminaison. Text contient des caractères ISO 10646 codés en UTF-8 [RFC2279] et String contient des données binaires de 8 bits. Les serveurs et les clients DOIVENT être capables de traiter des nuls incorporés. Les mises en œuvre de RADIUS qui utilisent le langage C ne doivent pas utiliser strcpy() lors du traitement de chaînes. Le format du champ Valeur est un parmi cinq types de données. Noter que le type "text" est un sous ensemble du type "string."

text : 1 à 253 octets contenant des caractères ISO 10646 codés en UTF-8 [RFC2279]. Un texte de longueur zéro (0) NE DOIT PAS être envoyé ; il faut à la place omettre l'attribut entier.

string : 1 à 253 octets contenant des données binaires (valeurs 0 à 255 inclus, en décimal,). Les chaînes de longueur zéro (0) NE DOIVENT PAS être envoyées ; il faut à la place omettre l'attribut entier.

adresse : valeur de 4 octets non signés, octet de poids fort en premier.

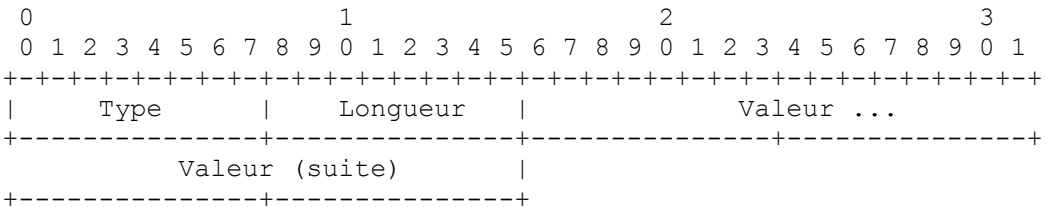
entier : valeur de 4 octets non signés, octet de poids fort en premier.

time : valeur de 4 octets non signés, octet de poids fort en premier -- secondes depuis le 1er janvier 1970 à 00:00:00 UTC.

5.1 Acct-Input-Gigawords

Description : cet attribut indique combien de fois le compteur Acct-Input-Octets est revenu de 2^32 à zéro pendant le cours de la fourniture de ce service, et ne peut être présent que dans les enregistrements de demande de comptabilité où le type Acct-Status-Type est réglé à Stop ou Interim-Update.

Un sommaire du format de l'attribut Acct-Input-Gigawords est montré ci-dessous. Les champs sont transmis de gauche à droite.



Type : 52 pour Acct-Input-Gigawords.

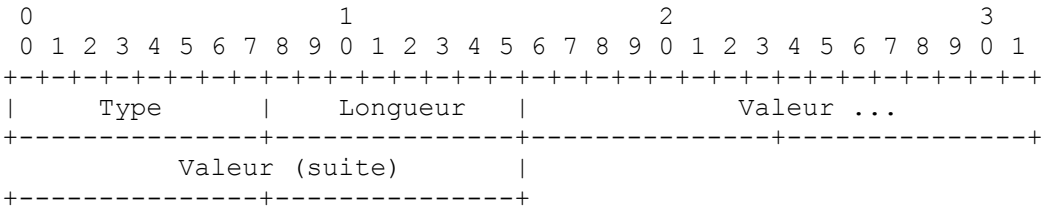
Longueur : 6

Valeur : le champ Valeur fait quatre octets.

5.2 Acct-Output-Gigawords

Description : cet attribut indique combien de fois le compteur Acct-Output-Octets est revenu de 2^32 à zéro dans le cours de la livraison de ce service, et peut seulement être présent dans les enregistrements Accounting-Request où le Acct-Status-Type est réglé à Stop ou Interim-Update.

Un sommaire du format d'attribut de Acct-Output-Gigawords est montré ci-dessous. Les champs sont transmis de gauche à droite.



Type : 53 pour Acct-Output-Gigawords.

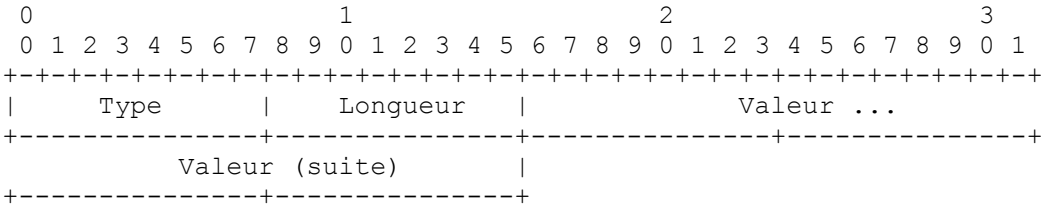
Longueur : 6

Valeur : le champ Valeur fait quatre octets.

5.3 Event-Timestamp

Description : cet attribut est inclus dans un paquet Accounting-Request pour enregistrer l'heure à laquelle cet événement s'est produit au NAS, en secondes depuis le 1er janvier 1970 à 00:00 UTC.

Un sommaire du format d'attribut Event-Timestamp est montré ci-dessous. Les champs sont transmis de gauche à droite.



Type : 55 pour Event-Timestamp

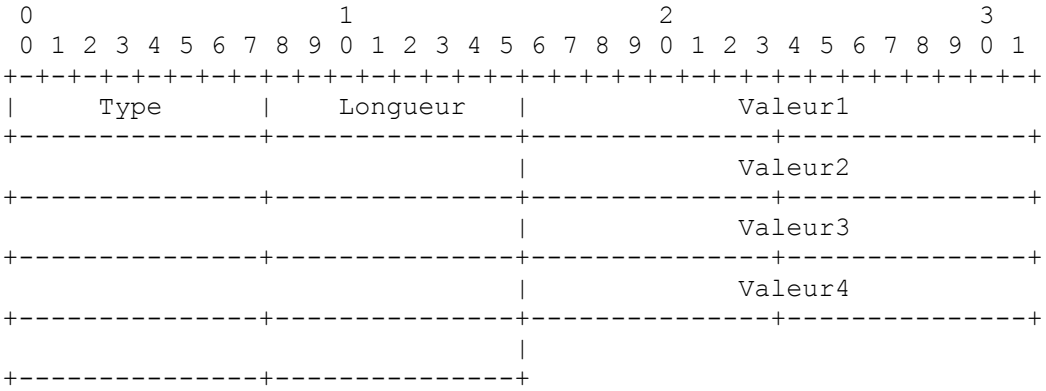
Longueur : 6

Valeur : le champ Valeur fait quatre octets codant un entier non signé du nombre de secondes depuis le 1er janvier 1970 à 00:00 UTC.

5.4 ARAP-Password

Description : cet attribut est seulement présent dans un paquet Access-Request contenant un Framed-Protocol de ARAP. Un seul de User-Password, CHAP-Password, ou ARAP-Password a besoin d'être présent dans une Access-Request, ou un ou plusieurs messages EAP.

Un sommaire du format d'attribut ARAP-Password est montré ci-dessous. Les champs sont transmis de gauche à droite.



Type : 70 pour ARAP-Password.

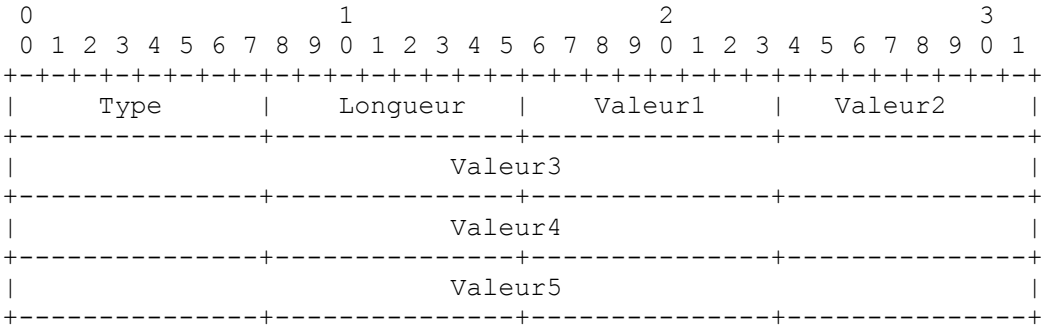
Longueur : 18

Valeur : cet attribut contient une chaîne de 16 octets, utilisée pour porter la réponse de l'usager appelant au défi du NAS et le propre défi du client au NAS. Les octets de poids fort (Valeur1 et Valeur2) contiennent le défi de l'usager appelant au NAS (2 nombres de 32 bits, 8 octets) et les octets de moindre poids (Valeur3 et Valeur4) contiennent la réponse de l'usager appelant au défi du NAS (2 nombres de 32 bits, 8 octets).

5.5 ARAP-Features

Description : cet attribut est envoyé dans un paquet Access-Accept avec le Framed-Protocol de ARAP, et inclut des informations de mot de passe que le NAS devrait envoyer à l'usager dans un paquet ARAP "fanions de caractéristiques".

Un sommaire du format d'attribut ARAP-Features est montré ci-dessous. Les champs sont transmis de gauche à droite.



Type : 71 pour ARAP-Features.

Longueur : 16

Valeur : le champ Valeur est une chaîne composée contenant des informations que le NAS devrait envoyer à l'usager dans le paquet ARAP "fanions de caractéristiques".

Valeur1 : Si elle est zéro, l'usager ne peut pas changer son mot de passe. Sinon, il le peut. (RADIUS ne traite pas le changement de mot de passe , juste l'attribut qui indique si ARAP indique qu'il le peut.)

Valeur2 : longueur minimum acceptable du mot de passe, de 0 à 8.

Valeur3: date de création du mot de passe en format Macintosh, défini comme 4 octets non signés qui représentent les secondes depuis le 1er janvier 1904 à minuit GMT.

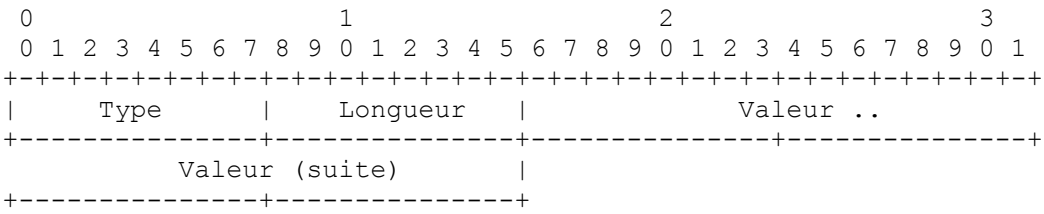
Valeur4 : différence de date d'expiration du mot de passe depuis la date de création en secondes.

Valeur5 : heure RADIUS actuelle en format Macintosh.

5.6 ARAP-Zone-Access

Description : cet attribut est inclus dans un paquet Access-Accept avec le Framed-Protocol de ARAP pour indiquer comment la liste de zones ARAP pour l'usager devrait être utilisée.

Un sommaire du format d'attribut ARAP-Zone-Access est montré ci-dessous. Les champs sont transmis de gauche à droite.



Type : 72 pour ARAP-Zone-Access.

Longueur : 6

Valeur : le champ Valeur fait quatre octets codants un entier avec une des valeurs suivantes :
1 : ne permet l'accès qu'à la zone par défaut
2 : utilise inclusivement le filtre de zone4 : utilise exclusivement le filtre de zone.

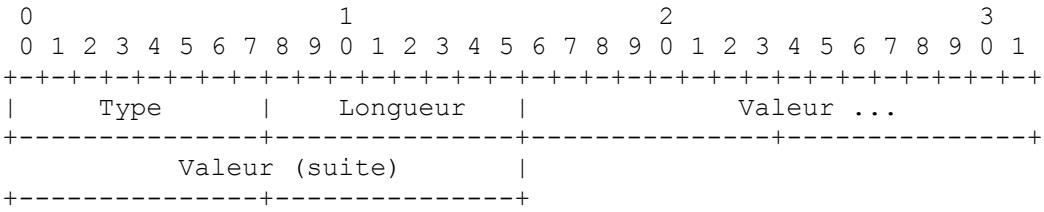
La valeur 3 est sautée, non parce qu'il y a des bits fanions, mais parce que 3 dans certaines mises en œuvre ARAP signifie "toutes les zones" ce qui est la même chose que ne pas spécifier du tout de liste dans RADIUS.

Si cet attribut est présent et si la valeur est 2 ou 4, un Filter-Id doit alors être aussi présent pour désigner un filtre de liste de zones à appliquer au fanion d'accès.

5.7 ARAP-Security

Description : cet attribut identifie le module de sécurité ARAP à utiliser dans un paquet Access-Challenge.

Un sommaire du format d'attribut ARAP-Security est montré ci-dessous. Les champs sont transmis de gauche à droite.



Type : 73 for ARAP-Security.

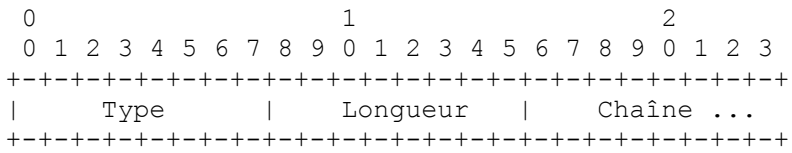
Longueur : 6

Valeur : le champ Valeur fait quatre octets, contenant un entier qui spécifie la signature du module de sécurité, qui est un OSType Macintosh. (Les OSTypes Macintosh sont 4 caractères ASCII présentés comme un entier de 32 bits.)

5.8 ARAP-Security-Data

Description : cet attribut contient le défi ou réponse réel du module de sécurité, et se trouve dans les paquets Access-Challenge et Access-Request.

Un sommaire du format d'attribut ARAP-Security-Data est montré ci-dessous. Les champs sont transmis de gauche à droite.



Type : 74 pour ARAP-Security-Data.

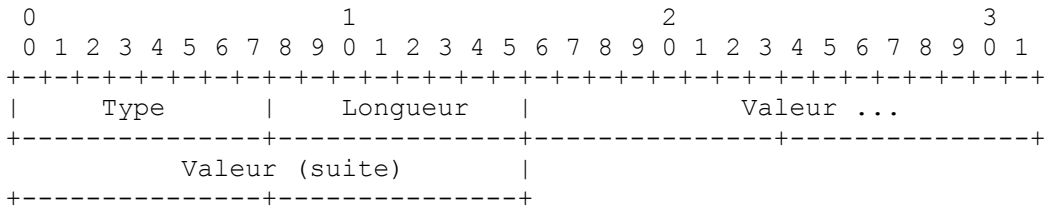
Longueur : ≥ 3

Chaîne : le champ String contient le défi ou réponse du module de sécurité associé au module de sécurité ARAP spécifié dans ARAP-Security.

5.9 Password-Retry

Description : cet attribut PEUT être inclus dans un Access-Reject pour indiquer combien de tentatives d'authentification peuvent être permises à un usager avant d'être déconnecté. Il est principalement destiné à l'utilisation dans l'authentification ARAP.

Un sommaire du format d'attribut Password-Retry est montré ci-dessous. Les champs sont transmis de gauche à droite.



Type : 75 pour Password-Retry.

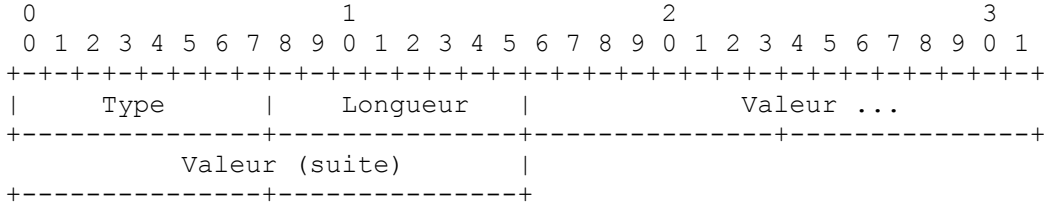
Longueur : 6

Valeur : le champ Valeur fait quatre octets, contenant un entier qui spécifie le nombre de tentatives d'entrée de mot de passe permises à l'usager.

5.10 Prompt

Description : cet attribut est utilisé seulement dans les paquets Access-Challenge, et indique au NAS si il devrait faire écho à la réponse de l'usager lorsque il est entré, ou non.

Un sommaire du format d'attribut Prompt est montré ci-dessous. Les champs sont transmis de gauche à droite.



Type : 76 pour Prompt.

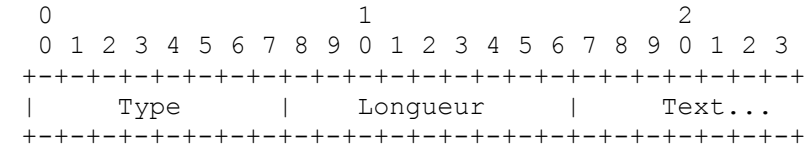
Longueur : 6

Valeur : le champ Valeur fait quatre octets.
0 : pas d'écho
1 : écho

5.11 Connect-Info

Description : cet attribut est envoyé du NAS pour indiquer la nature de la connexion de l'usager. Le NAS PEUT envoyer cet attribut dans une Access-Request ou Accounting-Request pour indiquer la nature de la connexion de l'usager.

Un sommaire du format d'attribut Connect-Info est montré ci-dessous. Les champs sont transmis de gauche à droite.



Type : 77 pour Connect-Info.

Longueur : ≥ 3

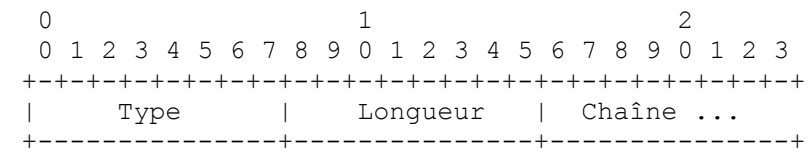
Text : le champ Text consiste en caractères ISO 10646 codés en UTF-8 [RFC2279]. La vitesse de connexion DEVRAIT être incluse au début du premier attribut Connect-Info dans le paquet. Si les vitesses de connexion d'émission et de réception diffèrent, elles peuvent être toutes deux incluses dans le premier attribut avec la vitesse d'émission en premier (la vitesse du modem du NAS émet à), une barre oblique (/), la vitesse de réception, puis facultativement d'autres informations.
Par exemple, "28800 V42BIS/LAPM" ou "52000/31200 V90"

Plus d'un attribut Connect-Info peuvent être présents dans un paquet Accounting-Request pour s'accommoder des efforts attendus de l'UIT pour que les modems rapportent plus d'informations de connexion en format standard, qui pourraient excéder 252 octets.

5.12 Configuration-Token

Description : cet attribut est à utiliser dans de grands réseaux d'authentification répartie fondés sur le mandataire. Il est envoyé d'un serveur mandataire RADIUS à un client mandataire RADIUS dans une Access-Accept pour indiquer un type de profil d'utilisateur à utiliser. Il ne devrait pas être envoyé à un NAS.

Un sommaire du format d'attribut Configuration-Token est montré ci-dessous. Les champs sont transmis de gauche à droite.



Type : 78 pour Configuration-Token.
Longueur : ≥ 3
Chaîne : le champ Chaîne fait un ou plusieurs octets. Le format réel des informations est spécifique du site ou de l'application, et une mise en œuvre robuste DEVRAIT prendre en charge le champ comme des octets indistincts.

La codification de la gamme des usages permis de ce champ sort du domaine d'application de la présente spécification.

5.13 EAP-Message

Description : cet attribut encapsule les paquets du protocole d'accès étendu [RFC2284] afin de permettre au NAS d'authentifier les usagers appelants via EAP sans avoir à comprendre le protocole EAP.

Le NAS place tous messages EAP reçus de l'usager dans un ou plusieurs attributs EAP et les transmet au serveur RADIUS au titre de la Access-Request, qui peut retourner les messages EAP dans des paquets Access- Challenge, Access-Accept et Access-Reject.
Un serveur RADIUS qui reçoit des messages EAP qu'il ne comprend pas DEVRAIT retourner un Access-Reject.

Le NAS place les messages EAP reçus de l'homologue qui s'authentifie dans un ou plusieurs attributs EAP-Message et les transmet au serveur RADIUS dans un message Access-Request. Si plusieurs messages EAP sont contenus dans un paquet Access-Request ou Access-Challenge, ils DOIVENT être dans l'ordre et ils DOIVENT être des attributs consécutifs dans le paquet Access-Request ou Access-Challenge. Les paquets Access-Accept et Access-Reject DEVRAIENT seulement avoir UN attribut EAP-Message, contenant EAP-Success ou EAP-Failure.

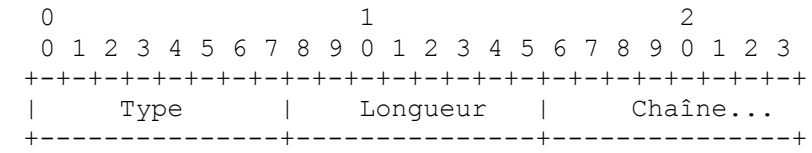
On s'attend à ce que EAP soit utilisé pour mettre en œuvre diverses méthodes d'authentification, incluant des méthodes impliquant un chiffrement fort. Afin d'empêcher des attaquants de subvertir EAP en attaquant RADIUS/EAP, (par exemple, en modifiant les paquets EAP-Success ou EAP-Failure) il est nécessaire que RADIUS/EAP fournisse une protection de l'intégrité au moins aussi forte que celle utilisée dans les méthodes EAP elles-mêmes.

Donc, 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.

Les paquets Access-Request qui incluent un attribut EAP-Message sans un attribut Message-Authenticator DEVRAIENT être éliminés en silence par le serveur RADIUS. Un serveur RADIUS qui prend en charge EAP-Message DOIT calculer la valeur correcte de Message-Authenticator et éliminer en silence le paquet si il ne correspond pas à la valeur envoyée. Un serveur RADIUS qui ne prend pas en charge EAP-Message DOIT retourner un Access-Reject si il reçoit une Access-Request contenant un attribut EAP-Message. Un serveur RADIUS qui reçoit un attribut EAP-Message qu'il ne comprend pas DOIT retourner un Access-Reject.

Les paquets Access-Challenge, Access-Accept, ou Access-Reject qui incluent un attribut EAP-Message sans un attribut Message-Authenticator DEVRAIENT être éliminés en silence par le NAS. Un NAS qui prend en charge EAP-Message DOIT calculer la valeur correcte du Message-Authenticator et éliminer en silence le paquet si il ne correspond pas à la valeur envoyée.

Un sommaire du format d'attribut EAP-Message est montré ci-dessous. Les champs sont transmis de gauche à droite.



Type : 79 pour EAP-Message.

Longueur : ≥ 3

Chaîne : le champ Chaîne contient des paquets EAP, comme défini dans la [RFC2284]. Si plusieurs attributs EAP-Message sont présents dans un paquet, leurs valeurs devraient être enchaînées ; cela permet à RADIUS de passer des paquets EAP plus longs que 253 octets.

5.14 Message-Authenticator

Description : cet attribut PEUT être utilisé pour signer les Access-Request pour empêcher l'usurpation des demandes d'accès en utilisant les méthodes d'authentification CHAP, ARAP ou EAP. Il PEUT être utilisé dans toute Access-Request. Il DOIT être utilisé dans tout Access-Request, Access-Accept, Access-Reject ou Access-Challenge qui inclut un attribut EAP-Message.

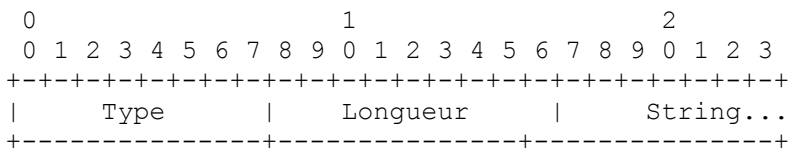
Un serveur RADIUS qui reçoit une Access-Request avec un attribut Message-Authenticator présent DOIT calculer la valeur correcte du Message-Authenticator et éliminer en silence le paquet si il ne correspond pas à la valeur envoyée.

Un client RADIUS qui reçoit un Access-Accept, Access-Reject ou Access-Challenge avec un attribut Message-Authenticator présent DOIT calculer la valeur correcte du Message-Authenticator et éliminer en silence le paquet si il ne correspond pas à la valeur envoyée.

Les projets antérieurs du présent mémoire utilisaient "Signature" comme nom de cet attribut, mais Message-Authenticator

est plus précis. Son fonctionnement n'a pas changé.

Un sommaire du format d'attribut Message-Authenticator est montré ci-dessous. Les champs sont transmis de gauche à droite.



Type : 80 pour Message-Authenticator

Longueur : 18

Chaîne : lorsque présent dans un paquet Access-Request, Message-Authenticator est une somme de contrôle HMAC-MD5 [RFC2104] du paquet Access-Request entier, incluant les champs Type, ID, Longueur et Authentificateur, en utilisant le secret partagé comme clé, comme suit .

Message-Authenticator = HMAC-MD5 (Type, Identifiant, Longueur, Authentificateur de demande, Attributs)

Lorsque la somme de contrôle est calculée, la chaîne Signature devrait être considérée comme seize octets de zéros.

Pour les paquets Access-Challenge, Access-Accept, et Access-Reject, le Message-Authenticator est calculé comme suit, en utilisant le Request-Authenticator provenant de la Access-Request auquel ce paquet répond :

Message-Authenticator = HMAC-MD5 (Type, Identifiant, Longueur, Authentificateur de demande, Attributs)

Lorsque la somme de contrôle est calculée, la chaîne Signature devrait être considérée comme seize octets de zéros. Le secret partagé est utilisé comme clé pour le hachage HMAC-MD5. Il est calculé et inséré dans le paquet avant que l'authentificateur de réponse soit calculé.

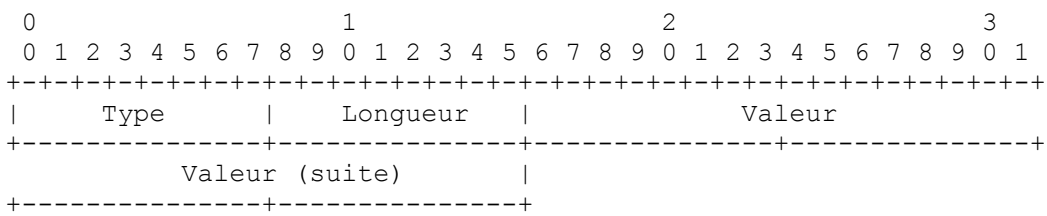
Cet attribut n'est pas nécessaire si l'attribut User-Password est présent, mais il est utile pour empêcher des attaques sur d'autres types d'authentification. Cet attribut est destiné à déjouer les tentatives où un attaquant établit un NAS "félon" , et effectue des attaques de dictionnaire en ligne contre le serveur RADIUS. Il n'assure pas la protection contre des attaques "hors ligne" où l'attaquant intercepte des paquets contenant (par exemple) le défi et réponse CHAP, et effectue une attaque de dictionnaire hors ligne contre ces paquets.

IPsec rendra finalement cet attribut inutile, de sorte qu'il devrait être considéré comme une mesure intérimaire.

5.15 ARAP-Challenge-Response

Description : cet attribut est envoyé dans un paquet Access-Accept avec le Framed-Protocol de ARAP, et contient la réponse au défi du client appelant.

Un sommaire du format d'attribut ARAP-Challenge-Response est montré ci-dessous. Les champs sont transmis de gauche à droite.



Type : 84 pour ARAP-Challenge-Response.

Longueur : 10

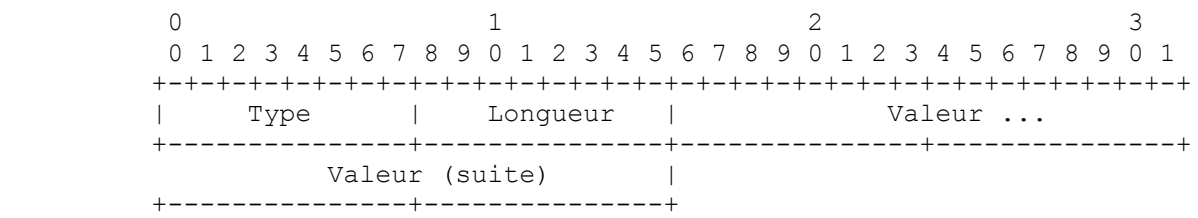
Valeur : le champ Valeur contient une réponse de 8 octets au défi du client appelant. Le serveur RADIUS calcule cette valeur en prenant le défi du client sur les huit octets de poids fort de l'attribut ARAP-Password et en effectuant le

chiffrement DES sur cette valeur avec le mot de passe de l'usager qui s'authentifie comme clé. Si le mot de passe de l'usager fait moins de 8 octets, le mot de passe est bourré à la fin d'octets NUL jusqu'à la longueur de 8 avant de l'utiliser comme clé.

5.16 Acct-Interim-Interval

Description : cet attribut indique le nombre de secondes entre chaque mise à jour intermédiaire en secondes pour cette session spécifique. Cette valeur peut seulement apparaître dans le message Access-Accept.

Un sommaire du format d'attribut Acct-Interim-Interval est montré ci-dessous. Les champs sont transmis de gauche à droite.



Type : 85 pour Acct-Interim-Interval.

Longueur : 6

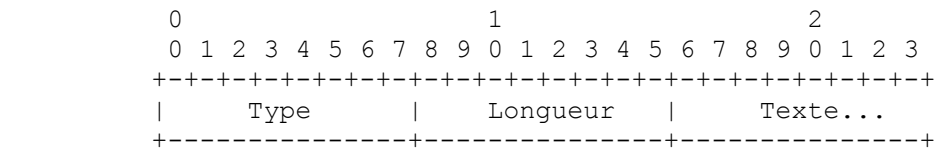
Valeur : le champ Valeur contient le nombre de secondes entre chaque mise à jour intermédiaire à envoyer du NAS pour cette session. La valeur NE DOIT PAS être inférieure à 60. La valeur NE DEVRAIT PAS être inférieure à 600, et une considération particulière devrait être apportée quant à son impact sur le trafic réseau.

5.17 NAS-Port-Id

Description : cet attribut contient une chaîne de texte identifiant l'accès du NAS qui authentifie l'usager. Il est seulement utilisé dans les paquets Access-Request et Accounting-Request. Noter qu'il utilise "accès" au sens d'une connexion physique sur le NAS, non au sens d'un numéro d'accès TCP ou UDP.

NAS-Port ou NAS-Port-Id DEVRAIT être présent dans un paquet Access-Request, si le NAS différencie ses accès. NAS-Port-Id est destiné à être utilisé par les NAS qui ne peuvent pas numéroter leur accès de façon convenable.

Un sommaire du format d'attribut NAS-Port-Id est montré ci-dessous. Les champs sont transmis de gauche à droite.



Type : 87 pour NAS-Port-Id.

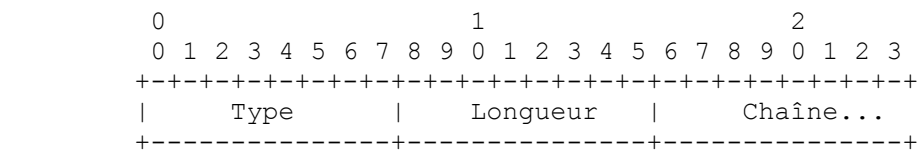
Longueur : ≥ 3

Texte : le champ Text contient le nom de l'accès en utilisant des caractères ISO 10646 codés en UTF-8 [RFC2279].

5.18 Framed-Pool

Description : cet attribut contient le nom d'un réservoir d'adresses allouées qui DEVRAIT être utilisé pour allouer une adresse à l'usager. Si un NAS ne prend pas en charge les réservoirs d'adresses multiples, il devrait ignorer cet attribut. Les réservoirs d'adresses sont généralement utilisés pour les adresses IP, mais peuvent être utilisés pour d'autres protocoles si le NAS prend en charge les réservoirs pour ces protocoles.

Un sommaire du format d'attribut Framed-Pool est montré ci-dessous. Les champs sont transmis de gauche à droite.



Type : 88 pour Framed-Pool

Longueur : ≥ 3

Chaîne : le champ Chaîne contient le nom d'un réservoir d'adresses allouées configuré sur le NAS.

5.19 Tableau des attributs

Le tableau suivant donne une indication sur les attributs qui peuvent être trouvés dans les divers types de paquets. Acct-Input-Gigawords, Acct-Output-Gigawords, Event-Timestamp, et NAS-Port-Id peuvent avoir 0-1 instance dans un paquet Accounting-Request. Connect-Info peut avoir 0+ instances dans un paquet Accounting-Request. Les autres attributs ajoutés dans le présent document ne doivent pas être présents dans une Accounting-Request.

Request	Accept	Reject	Challenge	n°	Attribut
0-1	0	0	0	70	ARAP-Password [Note]
0	0-1	0	0-1	71	ARAP-Features
0	0-1	0	0	72	ARAP-Zone-Access
0-1	0	0	0-1	73	ARAP-Security
0+	0	0	0+	74	ARAP-Security-Data
0	0	0-1	0	75	Password-Retry
0	0	0	0-1	76	Prompt
0-1	0	0	0	77	Connect-Info
0	0+	0	0	78	Configuration-Token
0+	0+	0+	0+	79	EAP-Message [Note]
0-1	0-1	0-1	0-1	80	Message-Authenticator [Note]
0	0-1	0	0-1	84	ARAP-Challenge-Response
0	0-1	0	0	85	Acct-Interim-Interval
0-1	0	0	0	87	NAS-Port-Id
0	0-1	0	0	88	Framed-Pool

[Note] une Access-Request qui contient un User-Password ou CHAP-Password ou ARAP-Password ou un ou plusieurs attributs EAP-Message NE DOIT PAS contenir plus d'un type de ces quatre attributs. Si elle ne contient aucun de ces quatre attributs, elle DEVRAIT contenir un Message-Authenticator. Si un type de paquet contient un attribut EAP-Message, il DOIT aussi contenir un Message-Authenticator.

Légende des entrées du tableau ci-dessus :
0 : cet attribut NE DOIT PAS être présent
0+ : zéro, une ou plusieurs instances de cet attribut PEUVENT être présentes
0-1 : zéro ou une instance de cet attribut PEUNT être présente
1 : exactement une instance de cet attribut DOIT être présente

6. Considérations relatives à l'IANA

Les codes de type de paquet, les types d'attribut, et les valeurs d'attribut définis dans le présent document sont enregistrés par l'autorité d'allocation des numéros de l'Internet (IANA, *Internet Assigned Numbers Authority*) dans l'espace de noms RADIUS comme décrit dans les "Considérations relatives à l'IANA" de la [RFC2865], conformément au BCP 26 [RFC2434].

7. Considérations sur la sécurité

Les attributs autres que Message-Authenticator et EAP-Message dans ce document ne présentent pas d'autre problème de sécurité que ceux déjà identifiés dans la [RFC2865].

7.1 Sécurité de Message-Authenticator

Les paquets de demande d'accès avec un mot de passe d'utilisateur établissent l'identité de l'usager et du NAS qui envoie la Access-Request, à cause de la façon dont le secret partagé est utilisé entre NAS et serveur RADIUS. Les paquets Access-Request avec un CHAP-Password ou EAP-Message n'ont pas d'attribut User-Password, et donc l'attribut Message-Authenticator devrait être utilisé dans les paquets de demande d'accès qui n'ont pas de User-Password, afin d'établir l'identité du NAS qui envoie la demande.

7.2 Sécurité de EAP

Comme l'objet de EAP est de fournir une sécurité améliorée pour l'authentification PPP, il est critique que RADIUS prenne en charge la sécurité d'EAP. En particulier, les questions suivantes doivent être traitées :

Séparation du serveur EAP et de l'authentificateur PPP
Capture de connexion
Attaques par interposition
Bases de données multiples
Attaques de la négociation

7.2.1 Séparation du serveur EAP et de l'authentificateur PPP

Il est possible que les points d'extrémité EAP s'authentifient mutuellement, négocient une suite de chiffrement, et déduisent une clé de session pour l'utiliser ultérieurement dans le chiffrement PPP.

Cela ne pose pas de problème à l'homologue, car l'homologue et le client EAP résident sur la même machine ; tout ce qui est exigé est que le module client EAP passe la clé de session au module de chiffrement PPP.

La situation est plus complexe lorsque EAP est utilisé avec RADIUS, car l'authentificateur PPP ne va normalement pas résider sur la même machine que le serveur EAP. Par exemple, le serveur EAP peut être un serveur de sécurité arrière, ou un module résidant sur le serveur RADIUS.

Dans le cas où le serveur EAP et l'authentificateur PPP résident sur des machines différentes, il y a plusieurs implications pour la sécurité. D'abord, l'authentification mutuelle va se faire entre l'homologue et le serveur EAP, et non entre l'homologue et l'authentificateur. Cela signifie qu'il n'est pas possible à l'homologue de valider l'identité du NAS ou du tunnel serveur auquel il parle.

Comme décrit plus haut, lorsque EAP/RADIUS est utilisé pour encapsuler les paquets EAP, l'attribut Message-Authenticator est exigé dans les demandes d'accès EAP/RADIUS envoyées du NAS ou du serveur tunnel au serveur RADIUS. Comme l'attribut Message-Authenticator implique un hachage HMAC-MD5, il est possible au serveur RADIUS de vérifier l'intégrité de la demande d'accès ainsi que l'identité du NAS ou serveur tunnel. De même, les paquets Access-Challenge envoyés du serveur RADIUS au NAS sont aussi authentifiés et protégés en intégrité en utilisant un hachage HMAC-MD5, permettant au NAS ou serveur tunnel de déterminer l'intégrité du paquet et de vérifier l'identité du serveur RADIUS. De plus, les paquets EAP envoyés via des méthodes qui contiennent leur propre protection d'intégrité ne peuvent pas être modifiés avec succès par un NAS ou serveur tunnel félon.

Le second problème qui se pose dans le cas d'un serveur EAP et d'un authentificateur PPP résidant sur des machines différentes est que la clé de session négociée entre l'homologue et le serveur EAP va devoir être transmise à l'authentificateur. Donc, un mécanisme doit être fourni pour transmettre la clé de session du serveur EAP à l'authentificateur ou serveur tunnel qui doit utiliser la clé. La spécification de ce mécanisme de transit sort du domaine d'application du présent document.

7.2.2 Capture de connexion

Dans cette forme d'attaque, l'attaquant tente d'injecter des paquets dans la conversation entre le NAS et le serveur RADIUS, ou entre le serveur RADIUS et le serveur de sécurité arrière. RADIUS ne prend pas en charge le chiffrement, et comme décrit dans la [RFC2865], seuls les paquets Access-Reply et Access-Challenge sont protégés en intégrité. De plus, le mécanisme de protection de l'intégrité décrit dans la [RFC2865] est plus faible que celui probablement utilisé par certaines méthodes EAP, rendant possible de subvertir ces méthodes en attaquant EAP/RADIUS.

Afin d'assurer l'authentification de tous les paquets dans l'échange EAP, tous les paquets EAP/RADIUS DOIVENT être authentifiés en utilisant l'attribut Message-Authenticator, comme décrit plus haut.

7.2.3 Attaques par interposition

Comme la sécurité de RADIUS se fonde sur des secrets partagés, la sécurité de bout en bout n'est pas assurée dans le cas où l'authentification ou les paquets de comptabilité sont transmis le long d'une chaîne de mandataires. Par suite, des attaquants qui prennent le contrôle d'un mandataire RADIUS seront capables de modifier les paquets EAP en transit.

7.2.4 Bases de données multiples

Dans de nombreux cas, un serveur de sécurité d'extrémité arrière sera déployé avec un serveur RADIUS afin de fournir des services EAP. Si le serveur de sécurité d'extrémité arrière fonctionne aussi comme serveur RADIUS, deux bases de données d'utilisateur séparées vont exister, contenant chacune des informations sur les exigences de sécurité pour l'usager. Cela représente une faiblesse, car la sécurité peut être compromise par une attaque réussie sur un des serveurs, ou leur bases de données d'extrémité arrière. Avec plusieurs bases de données d'utilisateur, l'ajout d'un nouvel usager peut exiger plusieurs opérations, augmentant les chances d'erreur. Les problèmes sont augmentés dans le cas où les informations d'utilisateur sont aussi conservées dans un serveur LDAP. Dans ce cas, il peut exister trois mémorisations des informations de l'utilisateur.

Pour contrer ces menaces, la consolidation des bases de données est recommandée. Ceci peut se faire en ayant le serveur RADIUS et le serveur de sécurité d'extrémité arrière qui mémorisent les informations dans la même base de données d'arrière, en ayant le serveur de sécurité d'extrémité arrière qui fournit une pleine mise en œuvre RADIUS, ou en consolidant les deux serveur RADIUS et de sécurité arrière sur la même machine.

7.2.5 Attaques de la négociation

Dans une attaque de la négociation, un NAS, un serveur tunnel, un mandataire RADIUS ou un serveur RADIUS félon fait que l'homologue qui s'authentifie choisit une méthode d'authentification moins sûre afin de faciliter l'obtention du mot de passe de l'usager. Par exemple, une session qui serait normalement authentifiée avec EAP va à la place s'authentifier via CHAP ou PAP ; autrement, une connexion qui serait normalement authentifiée via un type EAP se fait via un type EAP moins sûr, comme MD5. La menace que font peser des appareils félons, considérée autrefois comme lointaine, a gagné en force grâce à des systèmes de commutation de compagnie de téléphone compromis, comme ceux décrits dans [Slatalla].

La protection contre les attaques de la négociation exige l'élimination des négociations vers l'aval. Cela peut se faire via la mise en œuvre d'une politique par connexion de la part de l'homologue qui s'authentifie, et d'une politique par usager de la part du serveur RADIUS.

Pour l'homologue qui s'authentifie, la politique d'authentification devrait être établie sur la base de la connexion. Une politique par connexion permet à un homologue qui s'authentifie de négocier EAP lorsque il invoque un service, tout en négociant CHAP pour un autre service, même si les deux services sont accessibles via le même numéro de téléphone.

Avec une politique par connexion, un homologue qui s'authentifie va seulement tenter de négocier EAP pour une session dans laquelle la prise en charge d'EAP est attendue. Par suite, il y a une présomption qu'un homologue qui s'authentifie en choisissant EAP exige ce niveau de sécurité. Si iee ne peut pas être fourni, il est probable qu'il y a une mauvaise configuration, ou même que l'homologue qui s'authentifie contacte le mauvais serveur. Si le NAS n'était pas capable de négocier EAP, ou si la EAP-Request envoyée par le NAS était d'un différent type EAP que celui attendu, l'homologue qui s'authentifie DOIT se déconnecter. Un homologue qui s'authentifie s'attendant à ce que EAP soit négocié pour une session NE DOIT PAS négocier CHAP ou PAP.

Pour un NAS, il peut n'être pas possible de déterminer si un usager est obligé de s'authentifier avec EAP jusqu'à ce que l'identité de l'usager soit connue. Par exemple, pour les NAS à utilisation partagée, il est possible qu'un revendeur mette en œuvre EAP tandis qu'un autre ne le fait pas; Dans de tels cas, si un usager du NAS DOIT faire EAP, le NAS DOIT alors tenter de négocier EAP pour chaque appel. Cela évite de forcer un client à capacité EAP de faire plus d'une authentification, ce qui affaiblit la sécurité.

Si CHAP est négocié, le NAS va passer les attributs User-Name et CHAP-Password au serveur RADIUS dans un paquet Access-Request. Si l'usager n'est pas obligé d'utiliser EAP, le serveur RADIUS va alors répondre avec un paquet Access-Accept ou Access-Reject comme approprié. Cependant, si CHAP a été négocié mais si EAP est requis, le serveur RADIUS DOIT répondre par un Access-Reject, plutôt qu'un paquet Access-Challenge/EAP-Message/EAP-Request. L'homologue qui s'authentifie DOIT refuser de renégocier l'authentification, même si la renégociation est de CHAP à EAP.

Si EAP est négocié mais n'est pas pris en charge par le mandataire ou serveur RADIUS, le serveur ou mandataire DOIT alors répondre avec un Access-Reject. Dans ces cas, le NAS DOIT envoyer un LCP-Terminate et déconnecter l'usager. C'est le comportement correct car l'homologue qui s'authentifie s'attend à ce que EAP soit négocié, et cette attente ne peut pas être satisfaite. Un homologue à capacité EAP qui s'authentifie DOIT refuser de renégocier le protocole d'authentification si EAP a été initialement négocié. Noter que des problèmes avec un mandataire RADIUS sans capacité

EAP peuvent se révéler difficiles à diagnostiquer, car un usager qui appelle d'un endroit (avec un mandataire à capacité EAP) peut être capable de s'authentifier avec succès via EAP, tandis que le même usager appelant d'un autre endroit (et qui rencontre un mandataire sans capacité EAP) peut être systématiquement déconnecté.

8. Références

[RFC1700] J. Reynolds et J. Postel, "Numéros alloués", STD 2, octobre 1994. *(Historique, voir www.iana.org)*)

[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.

[RFC2279] F. Yergeau, "UTF-8, un format de transformation de la norme ISO 10646", janvier 1998. (*Obsolète, voir* RFC3629) *(D.S.)*

[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)

[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)*

[Slatalla] Slatalla, M., et Quittner, J., "Masters of Deception." HarperCollins, New York, 1995.

9. Remerciements

RADIUS et RADIUS Accounting ont été à l'origine développés par Livingston Enterprises (qui fait maintenant partie de Lucent Technologies) pour leur série PortMaster de serveurs d'accès réseau. La section sur ARAP a été adoptée avec la permission de "Using RADIUS to Authenticate Apple Remote Access Connections" par Ward Willats de Cyno Technologies (ward@cyno.com). La section sur Acct-Interim-Interval a été adoptée avec la permission des auteurs d'un travail en cours antérieur, Pat Calhoun de Sun Microsystems, Mark Beadles de Compuserve, et Alex Ratcliffe de UUNET Technologies. La section sur EAP a été adoptée avec la permission des auteurs d'un travail en cours antérieur, Pat Calhoun de Sun Microsystems, Allan Rubens de Merit Network, et Bernard Aboba de Microsoft. Merci aussi à Dave Dawson et Karl Fox de Ascend, et Glen Zorn et Narendra Gidwani de Microsoft pour d'utiles discussions sur ces problèmes.

10. Adresse du président

Le groupe de travail RADIUS peut être contacté via son président actuel :
Carl Rigney
Livingston Enterprises
4464 Willow Road
Pleasanton, California 94588
USA
téléphone : +1 925 737 2100
mél : cdr@telemancy.com

11. Adresse des auteurs

Les questions sur le présent mémoire peuvent aussi être adressées à : Carl Rigney (cf supra)
Les questions sur ARAP et RADIUS peuvent être adressées à :
Ward Willats
Cyno Technologies
1082 Glen Echo Ave
San Jose, CA 95125
USA
téléphone : +1 408 297 7766
mél : ward@cyno.com

Les questions sur EAP et RADIUS peuvent être adressées à :

Pat R. Calhoun
Network et Security Research Center
Sun Microsystems, Inc.
15 Network Circle
Menlo Park, CA 94025
téléphone : +1 650 786 7733
mél : pcalhoun@eng.sun.com

Allan C. Rubens
Tut Systems, Inc.
220 E. Huron, Suite 260
Ann Arbor, MI 48104
téléphone : +1 734 995 1697
mél : arubens@tutsys.com

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