Groupe de travail Réseau
Request for Comments : 4072
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

P. Eronen, éditeur, Nokia
T. Hiller, Lucent Technologies
G. Zorn, Cisco Systems
août 2005

Application Diameter du protocole d'authentification extensible (EAP)

Statut de ce mémoire
Le présent document spécifie un protocole Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et des suggestions pour son amélioration. Prière de se reporter à l'édition actuelle du STD 1 "Normes des protocoles officiels de l'Internet" pour connaître l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Le protocole d'authentification extensible (EAP, *Extensible Authentication Protocol*) donne un mécanisme standard pour la prise en charge de diverses méthodes d'authentification. Le présent document définit les codes de commandes et les AVP nécessaires pour porter les paquets EAP entre un serveur d'accès réseau (NAS, *Network Access Server*) et un serveur d'authentification de l'arrière.

Table des Matières

1. Introduction

Le protocole d'authentification extensible (EAP, *Extensible Authentication Protocol*) défini dans la [RFC3748], est un cadre d'authentification qui prend en charge de multiples mécanismes d'authentification. EAP peut être utilisé sur des liaisons dédiées, des circuits commutés, et aussi des liaisons sans fil.

Aujourd'hui, EAP a été mis en œuvre avec des hôtes et des routeurs qui se connectent via des circuits commutés sur des lignes de téléphonie en utilisant PPP [RFC1661], des commutateurs filaires IEEE 802 [IEEE-802.1X], et des points d'accès sans fil IEEE 802.11 [IEEE-802.11i]. EAP a aussi été adopté pour l'accès distant IPsec dans IKEv2 [RFC4306].

Le présent document spécifie l'application EAP Diameter qui porte les paquets EAP entre un serveur d'accès réseau (NAS, *Network Access Server*) agissant comme authentificateur EAP et un serveur d'authentification de l'arrière. L'application EAP Diameter se fonde sur l'application de serveur d'accès réseau Diameter [RFC4005] et est destinée à des environnements similaires à NASREQ.

Dans l'application EAP Diameter, l'authentification survient entre le client EAP et son serveur Diameter de rattachement. Cette authentification de bout en bout réduit la possibilité d'une authentification frauduleuse, comme des attaques en répétition et par interposition. L'authentification de bout en bout donne aussi une possibilité d'authentification mutuelle, qui n'est pas possible avec PAP et CHAP dans un environnement PPP d'itinérance.

L'application EAP Diameter s'appuie beaucoup sur la [RFC4005], et dans ses versions antérieures faisait partie de l'application Diameter NASREQ. Elle peut aussi être utilisée en conjonction avec NASREQ, en choisissant l'application sur la base du mécanisme d'authentification de l'usager (EAP ou PAP/CHAP). L'application EAP Diameter définit de nouveaux codes de commandes et paires d'attributs-valeur (AVP, *Attribute-Value Pair*) et peut fonctionner avec la prise en charge d'EAP par RADIUS [RFC3579].

1.1 Conventions utilisées dans le document

Dans le présent document, les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" sont à interpréter comme décrit dans le .BCP 14, RFC 2119.

2. Prise en charge du protocole d'authentification extensible dans Diameter

2.1 Annonce de la prise en charge de l'application

Les nœuds Diameter qui se conforment à la présente spécification DOIVENT annoncer leur soutien en incluant la valeur d'identifiant d'application EAP Diameter de 5 dans l'AVP Auth-Application-Id de la commande Demande/Réponse d'échange de capacités (Capabilities-Exchange-Request et Capabilities-Exchange-Answer) [RFC3588].

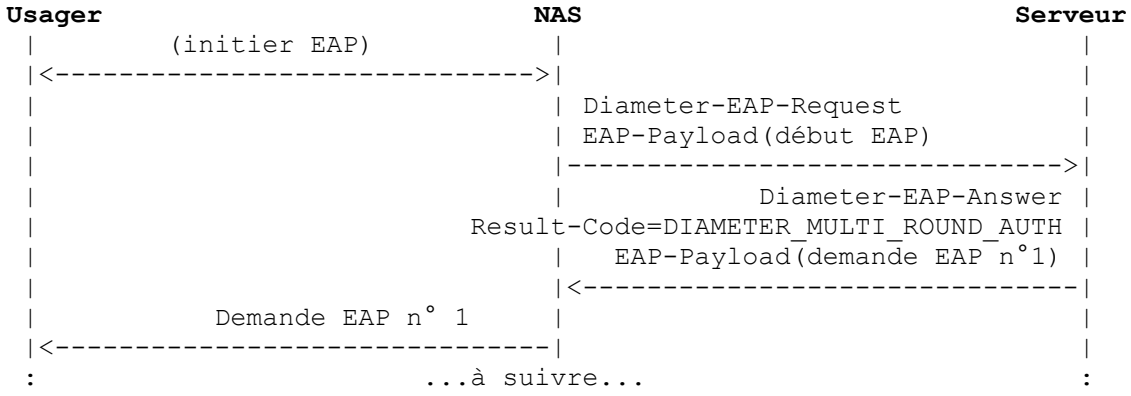
Si le NAS reçoit une réponse avec le code de résultat réglé à DIAMETER_APPLICATION_UNSUPPORTED *(application Diameter non prise en charge)* [RFC3588], cela indique que le serveur Diameter dans le domaine de rattachement ne prend pas en charge EAP. Si possible, l'appareil d'accès PEUT tenter de négocier un autre protocole d'authentification, comme PAP ou CHAP. Un appareil d'accès DEVRAIT faire attention quand il détermine si un protocole d'authentification moins sûr va être utilisé, car cela pourrait résulter d'une attaque en dégradation (voir le paragraphe 8.3).

2.2 Vue d'ensemble du protocole

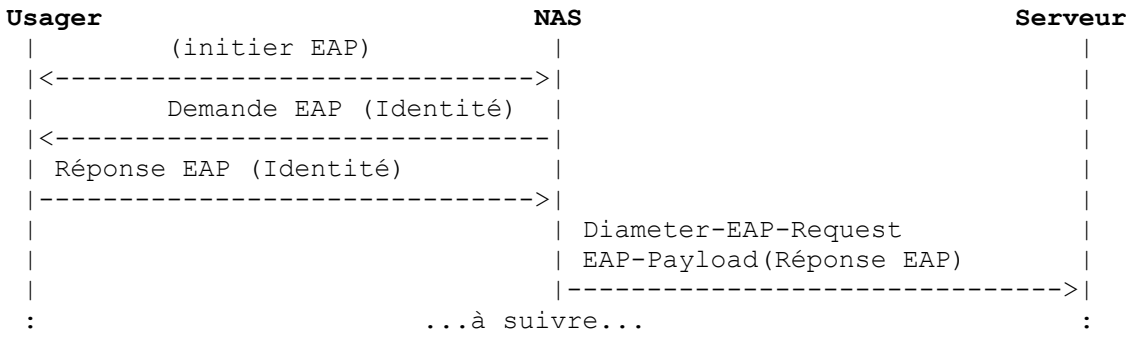
La conversation EAP entre les homologues qui s'authentifient et l'appareil d'accès commence avec l'initiation de EAP au sein d'une couche de liaison, comme PPP [RFC1661] ou IEEE 802.11i [IEEE-802.11i]. Une fois que EAP a été initié, l'appareil d'accès va normalement envoyer un message Diameter-EAP-Request avec une AVP EAP-Payload vide au serveur Diameter, signifiant EAP-Start *(début d'EAP)*.

Si le serveur Diameter de rattachement veut faire l'authentification EAP, il répond par un message Diameter-EAP-Answer contenant une AVP EAP-Payload qui comporte un paquet EAP encapsulé. L'AVP Result-Code dans le message sera réglée à DIAMETER_MULTI_ROUND_AUTH *(authentification Diameter en plusieurs tours)*, ce qui signifie qu'une demande

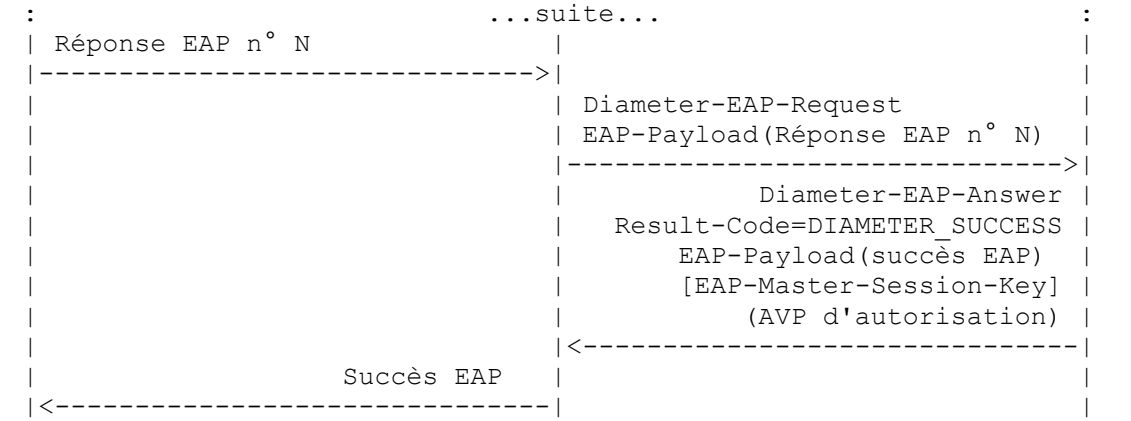
suivante est attendue. La charge utile EAP est transmise par l'appareil d'accès au client EAP. Ceci est illustré dans le diagramme suivant.



La réponse EAP Diameter initiale dans un échange à plusieurs tours inclut normalement une demande EAP d'identité (EAP-Request/Identity), demandant au client EAP de s'identifier. À réception de la réponse du client EAP (EAP-Response) l'appareil d'accès va alors produire un second message Diameter-EAP-Request, avec la charge utile EAP du client encapsulée dans l'AVP EAP-Payload.
L'approche préférée est que l'appareil d'accès produise le message EAP-Request/Identity au client EAP, et transmette le paquet EAP-Response/Identity encapsulé dans l'AVP EAP-Payload, comme une réponse Diameter-EAP-Request au serveur Diameter (voir le diagramme ci-dessous). Cette solution réduit le nombre d'allers-retours de messages Diameter. Lorsque le message EAP-Request/Identity est produit par l'appareil d'accès, il DEVRAIT interpréter le paquet EAP-Response/Identity retourné par l'homologue d'authentification, et copier sa valeur dans une AVP User-Name dans la demande EAP Diameter. Ceci est utile dans les environnements d'itinérance, car le domaine de destination est nécessaire pour l'acheminement. Noter que cette solution n'est pas d'utilisation universelle, car il y a des circonstances dans lesquelles l'identité d'un utilisateur n'est pas nécessaire (comme lorsque l'autorisation se fonde sur un numéro de téléphone appelant ou demandé).



La conversation continue jusqu'à ce que le serveur Diameter envoie une réponse EAP Diameter (Diameter-EAP-Answer) avec une AVP Result-Code indiquant le succès ou l'échec, et une AVP EAP-Payload facultative. L'AVP Result-Code est utilisée par l'appareil d'accès pour déterminer si le service est à fournir au client EAP. L'appareil d'accès NE DOIT PAS s'appuyer sur le contenu de la charge utile EAP facultative pour déterminer si le service est à fournir.



Si une autorisation était demandée, une réponse EAP Diameter avec le code de résultat réglé à DIAMETER_SUCCESS

DEVRAIT aussi inclure les AVP d'autorisation appropriées exigées pour le service demandé (voir la Section 5 et la [RFC4005]). Dans certains cas, le serveur de rattachement peut n'être pas capable de fournir toutes les AVP d'autorisation nécessaires ; dans ce cas, une étape d'autorisation séparée PEUT être utilisée comme décrit au paragraphe 2.3.3. Les messages de réponse EAP Diameter dont l'AVP Result-Code est réglée à DIAMETER_MULTI_ROUND_AUTH PEUVENT inclure des AVP d'autorisation.

Une réponse EAP Diameter avec un code de résultat de succès PEUT aussi inclure une AVP EAP-Master-Session-Key qui contient du matériel de chiffrement pour protéger la communication entre l'usager et le NAS. Comment exactement ce matériel de chiffrement est utilisé dépend de la couche de liaison en question, et sort du domaine d'application du présent document.

Un serveur Diameter de rattachement PEUT demander une réauthentification EAP en produisant le messages Re-Auth-Request [RFC3588] au client Diameter.

Si une session d'authentification EAP se trouvait interrompue suite à la défaillance d'un serveur de rattachement, la session POURRAIT être redirigée sur un serveur de remplacement, mais la session d'authentification devrait recommencer depuis le début.

2.3 Interaction des sessions et de NASREQ

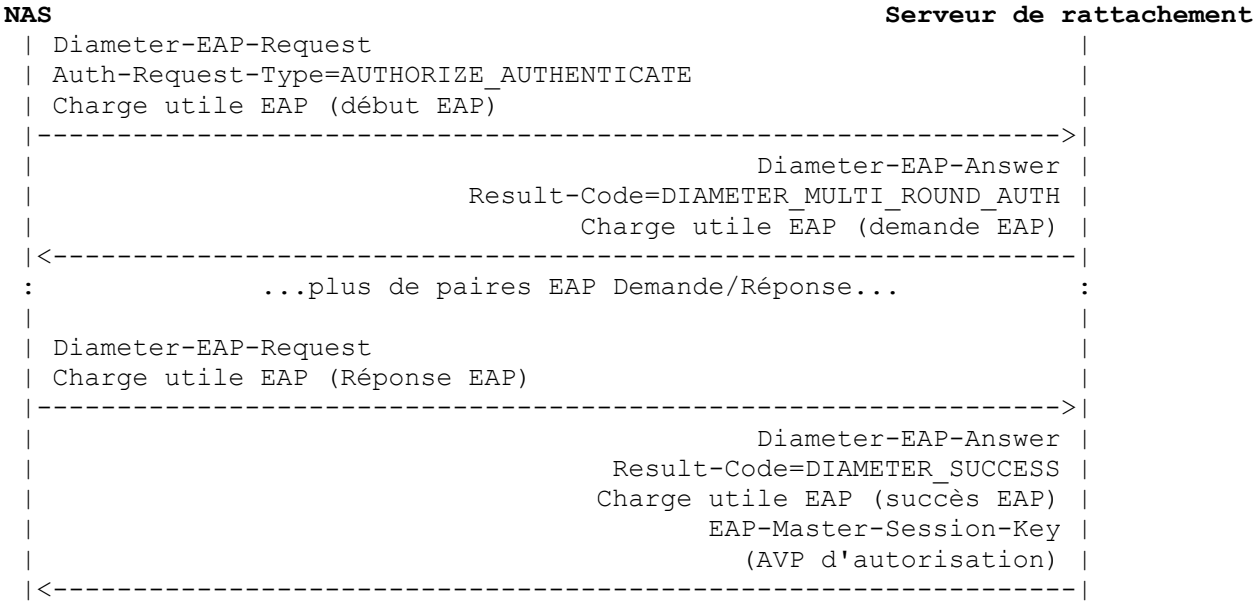
Le paragraphe précédent introduisait le protocole de base entre le NAS et le serveur de rattachement. Comme le message Diameter-EAP-Answer peut inclure une clé de session maîtresse (MSK, *Master Session Key*) pour protéger la communication entre l'utilisateur et le NAS, on doit s'assurer que cette clé ne tombe pas entre de mauvaises mains.

Les mécanismes de sécurité du Diameter de base (IPsec et TLS) protègent les messages Diameter bond par bond. Comme il n'y a actuellement pas de mécanisme de sécurité de bout en bout (du NAS au serveur de rattachement) défini pour Diameter, ce paragraphe décrit les scénarios possibles sur la façon dont les messages pourraient être protégés dans le transport en utilisant ces mécanismes bond par bond.

Cette liste de scénarios n'est pas destinée à être exhaustive, et il est possible de les combiner. Par exemple, le premier agent mandataire après le NAS pourrait utiliser des redirections comme dans le scénario 2 pour court-circuiter tous agents mandataires supplémentaires.

2.3.1 Scénario 1 : connexion directe

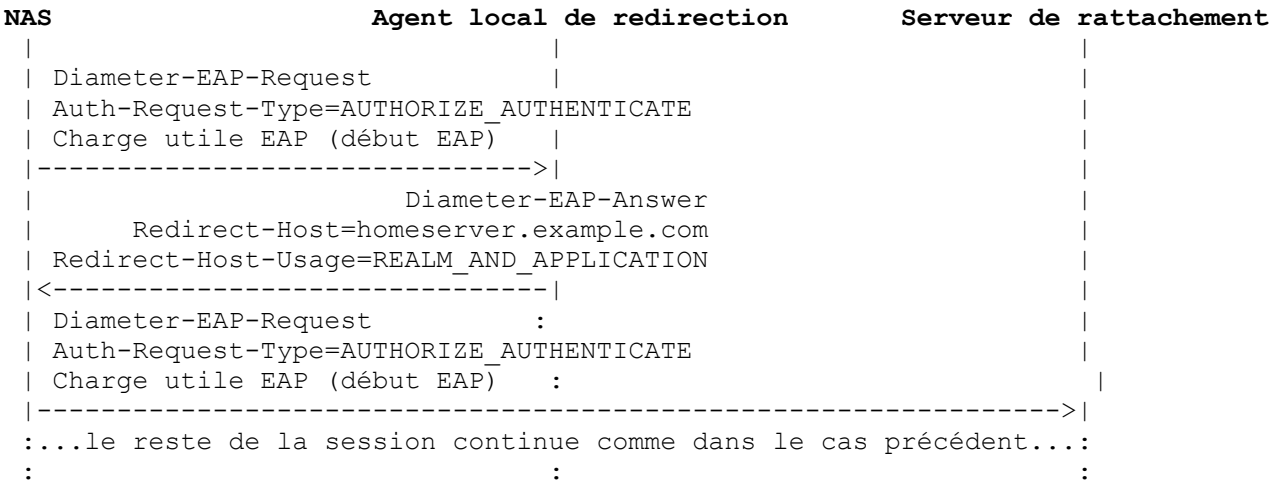
Le cas le plus simple est quand le NAS contacte le serveur de rattachement directement. Toutes les AVP d'autorisation et tout le matériel de chiffrement EAP sont livrés par le serveur de rattachement.



Ce scénario sera le plus probablement utilisé dans de petits réseaux, ou dans des cas où les agents Diameter ne sont pas nécessaires pour fournir des AVP d'acheminement ou d'autorisation supplémentaires.

2.3.2 Scénario 2 : Connexion directe avec redirections

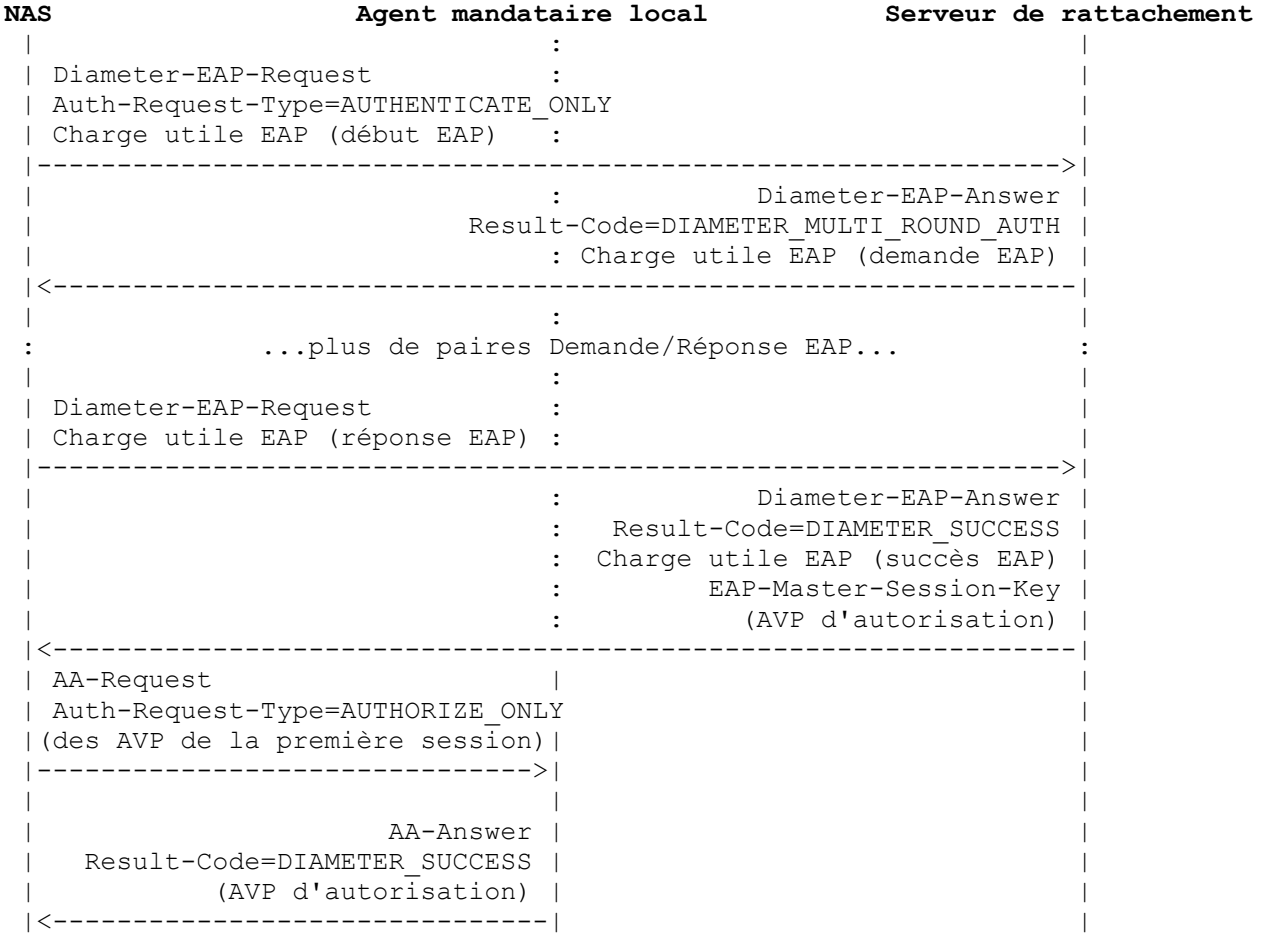
Dans ce scénario le NAS utilise un agent de redirection pour localiser le serveur de rattachement. Le reste de la session se poursuit comme précédemment.



L'avantage de ce scénario est que la connaissance du domaine et du serveur de rattachement est centralisée chez un agent de redirection, et il n'est pas nécessaire de modifier la configuration du NAS quand, par exemple, un nouvel accord d'itinérance est passé.

2.3.3 Scénario 3 : EAP direct, autorisation via les agents

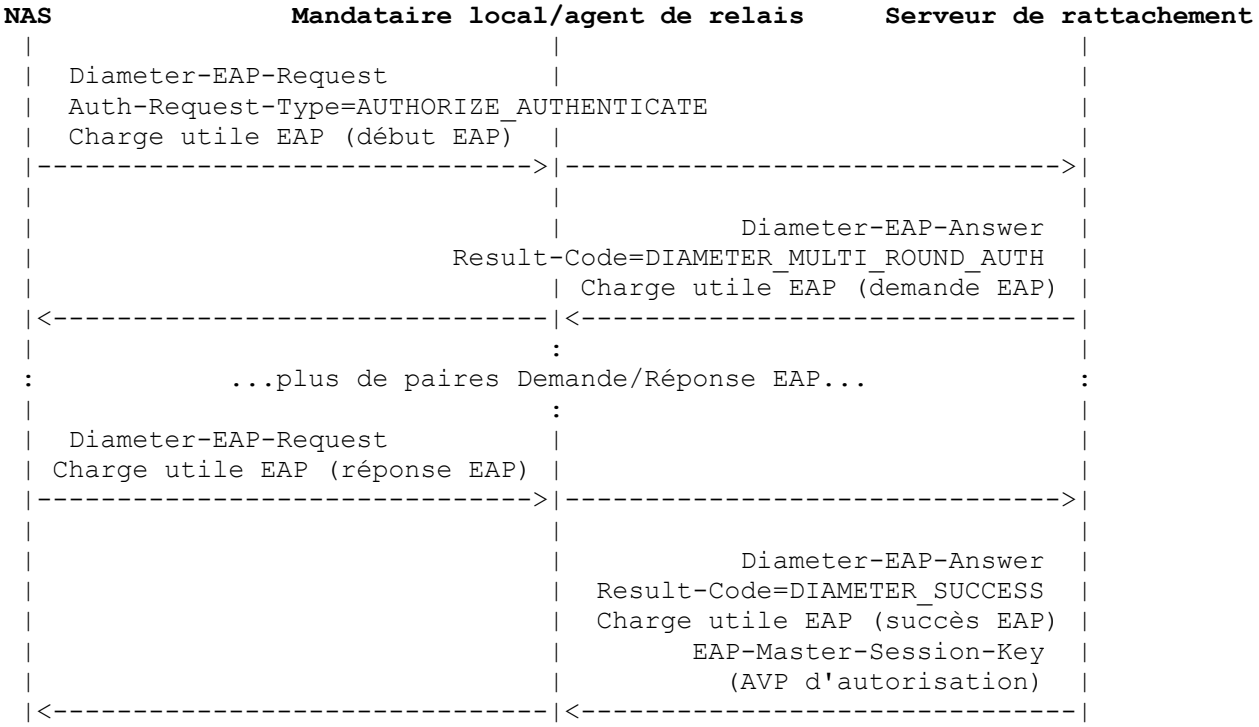
Dans ce scénario l'authentification EAP est faite directement avec le serveur de rattachement (avec Auth-Request-Type réglé à AUTHENTICATE_ONLY) et les AVP d'autorisation sont restituées des agents mandataires locaux. Ce scénario est destiné aux environnements dans lesquels le serveur de rattachement ne peut pas fournir toutes les AVP d'autorisation nécessaires au NAS.



L'application NASREQ est utilisée ici pour l'autorisation parce que le tableau d'acheminement spécifique du domaine prend en charge l'acheminement sur la base de l'application, et non des commandes Diameter.

2.3.4 Scénario 4 : agents mandataires

Ce scénario est le même que le scénario 1, mais le NAS contacte le serveur de rattachement à travers des mandataires. Noter que les mandataires peuvent voir les clés de session EAP, donc cela ne convient pas pour des environnements où les mandataires ne sont pas de confiance.



2.4 Paquets invalides

Lorsque il agit comme passeur, le NAS DOIT valider les champs d'en-tête EAP (Code, Identifiant, Longueur) avant de transmettre un paquet EAP au ou du serveur Diameter. À réception d'un paquet EAP de l'homologue, le NAS vérifie les champs Code (code 2 = réponse) et Longueur, et confronte la valeur de l'identifiant à celle fournie par le serveur Diameter dans la plus récente Demande EAP validée. À réception d'un paquet EAP du serveur Diameter (encapsulé dans une Diameter-EAP-Answer) le NAS vérifie les champs Code (code 1 = demande) et Longueur, puis met à jour la valeur d'identifiant courante. Les réponses EAP en cours qui ne correspondent pas à la valeur courante d'identifiant sont éliminées en silence par le NAS.

Comme les champs de méthode EAP (Type, Type-Data) ne sont normalement pas validés par un NAS fonctionnant comme passeur, en dépit de ces vérifications, il est possible qu'un NAS transmette un paquet EAP invalide au ou du serveur Diameter.

Un serveur Diameter qui reçoit une AVP EAP-Payload qu'il ne comprend pas DEVRAIT déterminer si l'erreur est fatale ou non sur la base du type EAP. Un serveur Diameter qui détermine qu'une erreur fatale s'est produite DOIT envoyer un message Diameter-EAP-Answer avec un code de résultat d'échec et une AVP EAP-Payload encapsulant un paquet EAP d'échec. Un serveur Diameter qui détermine qu'une erreur non fatale s'est produite DOIT envoyer un Diameter-EAP-Answer avec le code de résultat DIAMETER_MULTI_ROUND_AUTH, mais pas une AVP EAP-Payload. Pour simplifier la traduction de RADIUS, ce message DOIT aussi inclure une AVP EAP-Reissued-Payload encapsulant la demande EAP précédente envoyée par le serveur.

Lorsque il reçoit un Diameter-EAP-Answer sans AVP EAP-Payload (et le code de résultat DIAMETER_MULTI_ROUND_AUTH) le NAS DEVRAIT éliminer le paquet EAP-Response le plus récent transmis au serveur Diameter et vérifier si des paquets de réponse EAP supplémentaires qui correspondent à la valeur d'identifiant courante ont été reçus. Si il en est, un nouveau paquet de réponse EAP, si il en est de disponible, DOIT être envoyé au serveur Diameter au sein d'un Diameter-EAP-Request. Si aucun paquet de réponse EAP n'est disponible, la demande EAP précédente est envoyée à nouveau à l'homologue, et le temporisateur de retransmission est relancé.

Afin d'assurer la protection contre les attaques de déni de service (DoS) il est conseillé que le NAS alloue une mémoire tampon finie pour les paquets EAP reçus de l'homologue, et d'éliminer les paquets selon une politique appropriée une fois que la mémoire tampon est pleine. Aussi, il est conseillé que le serveur Diameter ne permette qu'un nombre modeste de paquets EAP invalides dans une seule session, avant de terminer la session avec le code de résultat DIAMETER_AUTHENTICATION_REJECTED. Par défaut, une valeur de 5 paquets EAP invalides est recommandée.

2.5 Retransmission

Comme noté dans la [RFC3748], si un paquet EAP est perdu dans le transit entre l'homologue qui s'authentifie et le NAS (ou vice versa), le NAS devra le retransmettre.

Il peut être nécessaire d'ajuster les stratégies de retransmission et les temporisations d'authentification dans certains cas. Par exemple, lorsque une carte à jeton est utilisée, du temps supplémentaire peut être nécessaire pour permettre à l'utilisateur de trouver la carte et entrer le jeton. Comme le NAS n'aura normalement pas connaissance des paramètres requis, ceci doit être assuré par le serveur Diameter.

Si une AVP Multi-Round-Time-Out [RFC3588] est présente dans un message Diameter-EAP-Answer qui contient aussi une AVP EAP-Payload, cette valeur sera utilisée pour régler le temporisateur de retransmission EAP pour cette seule demande EAP.

2.6 Fragmentation

En utilisant l'AVP EAP-Payload, il est possible au serveur Diameter 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 au serveur Diameter d'utiliser la découverte de MTU pour s'assurer de la MTU de la liaison, une AVP Framed-MTU peut être incluse dans un message Diameter-EAP-Request afin de fournir cette information au serveur Diameter.

Un serveur Diameter qui a reçu une AVP Framed-MTU dans un message Diameter-EAP-Request NE DOIT PAS envoyer de paquet ultérieur dans cette conversation EAP contenant une AVP EAP-Payload dont la longueur excède celle spécifiée par la valeur de Framed-MTU, en prenant en compte le type de liaison (spécifié par l'AVP NAS-Port-Type). Par exemple, comme noté au paragraphe 3.10 de la [RFC3580], pour une valeur de NAS-Port-Type de IEEE 802.11, le serveur RADIUS peut envoyer un paquet EAP aussi grand que Framed-MTU moins quatre (4) octets, en prenant en compte la redondance supplémentaire pour les champs Version IEEE 802.1X (1 octet), Type (1 octet) et Longueur de corps (2 octets).

2.7 Comptabilité

Lorsque un utilisateur a été authentifié à l'aide de EAP, le NAS PEUT inclure une AVP Accounting-Auth-Method [RFC4005] de valeur 5 (EAP) dans les messages Accounting-Request. Le présent document spécifie une AVP additionnelle pour les messages de comptabilité. Une ou plusieurs AVP Accounting-EAP-Auth-Method (voir au paragraphe 4.1.5) PEUVENT être incluses dans les messages Accounting-Request pour indiquer la ou les méthodes EAP utilisées pour authentifier l'utilisateur.

Si le NAS a authentifié l'utilisateur avec une méthode EAP mise en œuvre localement, il connaît la méthode utilisée et DEVRAIT l'inclure dans une AVP Accounting-EAP-Auth-Method.

Si l'authentification a été faite en utilisant des messages Diameter-EAP-Request/Answer, le serveur Diameter DEVRAIT inclure une ou plusieurs AVP Accounting-EAP-Auth-Method dans les paquets Diameter-EAP-Answer avec un code de résultat de succès. Dans ce cas, le NAS DEVRAIT inclure ces AVP dans les messages Accounting-Request.

2.8 Lignes directrices d'utilisation

2.8.1 AVP User-Name

Sauf si l'appareil d'accès interprète le paquet EAP-Response/Identity retourné par l'homologue qui s'authentifie, il n'aura pas accès à l'identité de l'utilisateur. De plus, certaines méthodes EAP prennent en charge la protection d'identité et l'identité réelle de l'utilisateur n'est pas incluse dans EAP-Response/Identity. Donc, le serveur Diameter DEVRAIT retourner l'identité de l'utilisateur en insérant une AVP User-Name aux messages Diameter-EAP-Answer qui ont un code de résultat de DIAMETER_SUCCESS. Un identifiant ou pseudonyme de facturation séparé PEUT être utilisé pour des raisons de confidentialité (voir au paragraphe 8.5). Si l'identité de l'utilisateur n'est pas disponible pour le NAS, l'AVP Session-Id PEUT être utilisée pour la comptabilité et la facturation ; cependant, le fonctionnement de ceci peut être très difficile à gérer.

2.8.2 Conflits d'AVP

Un message Diameter-EAP-Answer contenant une charge utile EAP de type EAP-Success ou EAP-Failure NE DOIT PAS avoir l'AVP Result-Code réglée à DIAMETER_MULTI_ROUND_AUTH.

Certaines couches inférieures supposent que la décision d'autorisation est prise par le serveur EAP, et donc l'homologue considère un succès EAP comme l'indication que l'accès a été accordé. Dans ce cas, le code de résultat DEVRAIT correspondre au paquet EAP contenu : un code de résultat de succès pour EAP-Success, et un code de résultat d'échec pour EAP-Failure. Si le paquet EAP encapsulé ne correspond pas au résultat impliqué par l'AVP Result-Code, la combinaison va probablement causer la confusion, parce que le NAS et l'homologue vont avoir des conclusions différentes sur le résultat de l'authentification. Par exemple, si le NAS reçoit un code de résultat d'échec avec un succès EAP encapsule, il ne va pas accorder l'accès à l'homologue. Cependant, à réception du succès EAP, l'homologue sera conduit à penser que l'accès a été accordé.

Cette situation peut être difficile à éviter lorsque les agents mandataires Diameter prennent des décisions d'autorisation (c'est à dire que des mandataires peuvent changer l'AVP Result-Code envoyée par le serveur de rattachement). Parce qu'il est de la responsabilité du serveur Diameter d'éviter les conflits, le NAS NE DOIT PAS "manufacturer" les paquets de résultat EAP afin de corriger les messages contradictoires qu'il reçoit. Ce comportement, rendu à l'origine obligatoire par [IEEE-802.1X], est maintenant déconseillé.

2.8.3 Messages affichables

L'AVP Reply-Message [RFC4005] NE DOIT PAS être incluse dans un message Diameter contenant une AVP EAP-Payload.

2.8.4 Inversion de rôle

Certains environnements dans lesquels EAP est utilisé, comme PPP, acceptent un fonctionnement d'homologue à homologue. Les deux parties agissent en même temps comme authentificateurs et comme authentifiés, dans deux conversations EAP simultanées et indépendantes.

La présente spécification est destinée aux communication entre l'authentificateur EAP (passeur) et le serveur d'authentification de l'extrémité arrière. Un client Diameter NE DOIT PAS envoyer de Diameter-EAP-Request encapsulant un paquet de demande EAP, et un serveur Diameter qui reçoit un tel paquet DOIT répondre par un code de résultat d'échec.

2.8.5 Espace d'identifiants

Dans EAP, chaque session a son propre espace d'identifiant univoque. Les mises en œuvre de serveur Diameter DOIVENT être capables de distinguer entre les paquets EAP qui ont le même identifiant existant au sein de sessions EAO distinctes et qui ont leur origine sur le même NAS. C'est fait en utilisant l'AVP Session-Id.

Si un NAS Diameter est au milieu d'un échange d'authentification à plusieurs tours, et si il détecte que la session EAP entre le client et le NAS s'est terminée, il DOIT choisir un nouvel identifiant de session Diameter pour toute session EAP ultérieure. Ceci est nécessaire afin de distinguer un processus d'authentification EAP redémarré de la continuation d'un processus en cours (par le même utilisateur sur les mêmes NAS et accès).

Dans RADIUS, la même fonctionnalité peut être réalisée par l'inclusion ou l'omission de l'attribut "State". Les règles de traduction de la [RFC4005] assurent qu'une demande d'accès sans l'attribut "State" se transpose en une nouvelle valeur d'AVP Session-Id Diameter. De plus, un agent de traduction va toujours inclure un attribut "State" dans les messages Access-Challenge, assurant que l'attribut State est disponible pour un NAS RADIUS.

3. Codes de commandes

Cette Section définit de nouvelles valeurs de code de commande qui DOIVENT être prises en charge par toutes les mises en œuvre Diameter qui se conforment à la présente spécification. Les commandes suivantes sont définies dans cette section :

Nom de commande	Abréviation	Code	Référence
Diameter-EAP-Request	DER	268	3.1
Diameter-EAP-Answer	DEA	268	3.2

Lorsque les commandes NASREQ AA-Request (AAR) ou AA-Answer (AAA) sont utilisées pour les messages AUTHORIZE_ONLY en conjonction avec EAP (voir au paragraphe 2.3.3) une valeur d'identifiant d'application de 1 (NASREQ) est utilisée, et les commandes suivent les règles et l'ABNF définis dans la [RFC4005].

Lorsque les commandes Re-Auth-Request (RAR), Re-Auth-Answer (RAA), Session-Termination-Request (STR), Session-Termination-Answer (STA), Abort-Session-Request (ASR), Abort-Session-Answer (ASA), Accounting-Request (ACR), et Accounting-Answer (ACA) sont utilisées avec l'application EAP Diameter, elles suivent les règles de la [RFC4005] et de la [RFC3588]. Les commandes de comptabilité utilisent la valeur d'identifiant d'application de 3 (comptabilité Diameter de base) ; les autres utilisent 0 (messages Diameter communs).

3.1 Commande Diameter-EAP-Request (DER)

La commande Diameter-EAP-Request (DER, *demande EAP Diameter*) indiquée par le champ Code de commande réglé à 268 et le bit 'R' établi dans le champ Fanions de commandes, est envoyée par un client Diameter à un serveur Diameter, et porte une réponse EAP provenant du client EAP. La commande Diameter-EAP-Request DOIT contenir une AVP EAP-Payload *(charge utile EAP)* contenant la charge utile EAP réelle. Une AVP EAP-Payload sans données PEUT être envoyée au serveur Diameter pour initier une session d'authentification EAP.

Le message DER PEUT résulter d'un échange d'authentification multi tours qui se produit lorsque le DEA est reçu avec l'AVP Result-Code réglée à DIAMETER_MULTI_ROUND_AUTH [RFC3588]. Un message DER suivant DOIT inclure toutes les AVP State *(état)* [RFC4005] qui étaient présentes dans le DEA. Pour la réauthentification, il est recommandé que la demande d'identité soit sautée afin de réduire le nombre d'allers-retours d'authentification. Ceci n'est possible que lorsque l'identité de l'utilisateur est déjà connue du serveur Diameter de rattachement.

Format de message : *(La présence des AVP entre accolades "{", "}" est obligatoire, celles entre crochets "[", "]" est facultative)*

```
<Diameter-EAP-Request> ::= < En-tête Diameter : 268, REQ, PXY >
                           < Session-Id >
                           { Auth-Application-Id }
                           { Origin-Host }
                           { Origin-Realm }
                           { Destination-Realm }
                           { Auth-Request-Type }
                           [ Destination-Host ]
                           [ NAS-Identifier ]
                           [ NAS-IP-Address ]
                           [ NAS-IPv6-Address ]
                           [ NAS-Port ]
                           [ NAS-Port-Id ]
                           [ NAS-Port-Type ]
                           [ Origin-State-Id ]
                           [ Port-Limit ]
                           [ User-Name ]
                           { EAP-Payload }
                           [ EAP-Key-Name ]
                           [ Service-Type ]
                           [ State ]
                           [ Authorization-Lifetime ]
                           [ Auth-Grace-Period ]
                           [ Auth-Session-State ]
                           [ Callback-Number ]
                           [ Called-Station-Id ]
                           [ Calling-Station-Id ]
                           [ Originating-Line-Info ]
                           [ Connect-Info ]
                         * [ Framed-Compression ]
                           [ Framed-Interface-Id ]
                           [ Framed-IP-Address ]
                         * [ Framed-IPv6-Prefix ]
                           [ Framed-IP-Netmask ]
                           [ Framed-MTU ]
                           [ Framed-Protocol ]
```

```
                * [ Tunneling ]
                * [ Proxy-Info ]
                * [ Route-Record ]
                * [ AVP ]
```

3.2 Commande Diameter-EAP-Answer (DEA)

Le message Diameter-EAP-Answer (DEA, *réponse EAP Diameter*) indiqué par le champ Code de commande réglé à 268 et bit 'R' à zéro dans le champ Fanions de commandes, est envoyé par le serveur Diameter au client pour une des raisons suivantes :

1. Le message fait partie d'un échange d'authentification multi tours, et le serveur attend une Diameter-EAP-Request à suivre. Ceci est indiqué par le réglage du code de résultat à DIAMETER_MULTI_ROUND_AUTH, et PEUT inclure zéro, une ou plusieurs AVP State.

2. Le client EAP a été authentifié et autorisé avec succès, auquel cas le message DOIT inclure l'AVP Result-Code indiquant le succès, et DEVRAIT inclure un type de charge utile EAP de EAP-Success. Cet événement DOIT causer la fourniture du service par l'appareil d'accès au client EAP.

3. Le client EAP n'a pas été authentifié et/ou autorisé, et l'AVP Result-Code est réglée pour indiquer l'échec. Ce message DEVRAIT inclure une AVP EAP-Payload, mais cette AVP n'est pas utilisée pour déterminer si le service doit être fourni.

Si le message provenant du client Diameter incluait une demande d'autorisation, une réponse de succès DOIT inclure les AVP d'autorisation qui sont pertinentes pour le service a fournir.

Format de message :

```
<Diameter-EAP-Answer> ::= < En-tête Diameter : 268, PXY >
                        < Session-Id >
                        { Auth-Application-Id }
                        { Auth-Request-Type }
                        { Result-Code }
                        { Origin-Host }
                        { Origin-Realm }
                        [ User-Name ]
                        [ EAP-Payload ]
                        [ EAP-Reissued-Payload ]
                        [ EAP-Master-Session-Key ]
                        [ EAP-Key-Name ]
                        [ Multi-Round-Time-Out ]
                        [ Accounting-EAP-Auth-Method ]
                        [ Service-Type ]
                       * [ Class ]
                       * [ Configuration-Token ]
                        [ Acct-Interim-Interval ]
                        [ Error-Message ]
                        [ Error-Reporting-Host ]
                       * [ Failed-AVP ]
                        [ Idle-Timeout ]
                        [ Authorization-Lifetime ]
                        [ Auth-Grace-Period ]
                        [ Auth-Session-State ]
                        [ Re-Auth-Request-Type ]
                        [ Session-Timeout ]
                        [ State ]
                       * [ Reply-Message ]
                        [ Origin-State-Id ]
                       * [ Filter-Id ]
                        [ Port-Limit ]
                        [ Callback-Id ]
                        [ Callback-Number ]
                        [ Framed-Appletalk-Link ]
```

```
* [ Framed-Appletalk-Network ]
  [ Framed-Appletalk-Zone ]
 * [ Framed-Compression ]
  [ Framed-Interface-Id ]
  [ Framed-IP-Address ]
 * [ Framed-IPv6-Prefix ]
  [ Framed-IPv6-Pool ]
 * [ Framed-IPv6-Route ]
  [ Framed-IP-Netmask ]
 * [ Framed-Route ]
  [ Framed-Pool ]
  [ Framed-IPX-Network ]
  [ Framed-MTU ]
  [ Framed-Protocol ]
  [ Framed-Routing ]
 * [ NAS-Filter-Rule ]
 * [ QoS-Filter-Rule ]
 * [ Tunneling ]
 * [ Redirect-Host ]
  [ Redirect-Host-Usage ]
  [ Redirect-Max-Cache-Time ]
 * [ Proxy-Info ]
 * [ AVP ]
```

4. Paires d'attribut-valeur

La présente Section définit de nouvelles AVP, spécifiques de l'application EAP Diameter, et décrit l'usage d'AVP définies ailleurs (si cet usage est notable dans l'application EAP).

4.1 Nouvelles AVP

4.1.1 AVP EAP-Payload

L'AVP EAP-Payload (code d'AVP 462) est du type OctetString et est utilisée pour encapsuler le paquet EAP réel qui est échangé entre le client EAP et le serveur Diameter de rattachement.

4.1.2 AVP EAP-Reissued-Payload

L'AVP EAP-Reissued-Payload (code d'AVP 463) est du type OctetString. L'utilisation de cette AVP est décrite au paragraphe 2.4.

4.1.3 AVP EAP-Master-Session-Key

L'AVP EAP-Master-Session-Key (code d'AVP 464) est du type OctetString. Elle contient le matériel de chiffrement pour protéger les communications entre l'utilisateur et le NAS. Comment ce matériel de chiffrement est exactement utilisé dépend de la couche de liaison en question, et sort du domaine d'application de ce document.

4.1.4 AVP EAP-Key-Name

L'AVP EAP-Key-Name (type d'attribut RADIUS 102) est du type OctetString. Elle contient un identifiant de clé opaque (nom) généré par la méthode EAP. Comment ce nom est exactement utilisé dépend de la couche de liaison en question, et sort du domaine d'application de ce document (voir les détails dans la [RFC5247]).

Noter que toutes les couches de liaison n'utilisent pas ce nom, et actuellement la plupart des méthodes EAP ne le génèrent pas. Comme le NAS fonctionne en mode passeur, il ne peut pas connaître la clé avant de la recevoir du serveur AAA. Par suite, une AVP Key-Name envoyée dans une demande EAP Diameter NE DOIT PAS contenir de données. Un serveur Diameter de rattachement qui reçoit une Diameter-EAP-Request avec une AVP Key-Name qui a des données non vides DOIT ignorer en silence cette AVP. De plus, le serveur Diameter de rattachement DEVRAIT n'inclure cette AVP dans le message Diameter-EAP-Answer que si une AVP EAP-Key-Name vide était présente dans la demande EAP Diameter.

4.1.5 AVP Accounting-EAP-Auth-Method

L'AVP Accounting-EAP-Auth-Method (code d'AVP 465) est du type Unsigned64. En cas de type expansé du paragraphe 5.7 de la [RFC3748], cette AVP contient la valeur ((Vendor-Id * 2^32) + Vendor-Type).

L'utilisation de cette AVP est décrite au paragraphe 2.7.

5. Tableaux d'occurrence des AVP

Les tableaux qui suivent utilisent ces symboles :
0 : l'AVP NE DOIT PAS être présente dans le message
0+ : zéro, une ou plusieurs instances de l'AVP PEUVENT être présentes dans le message
0-1 : zéro ou une instance de l'AVP PEUT être présente dans le message
1 : une instance de l'AVP DOIT être présente dans le message

Noter que les AVP qui peuvent seulement être présentes au sein d'une AVP Grouped ne sont pas représentées dans ces tableaux.

5.1 Tableau des AVP de commandes EAP

Le tableau qui suit fait la liste des AVP qui peuvent être présentes dans les commandes DER et DEA, comme défini dans le présent document ; les AVP sont définies ici et dans la [RFC4005].

	Code de commande	
Nom d'attribut	**DER**	**DEA**
Accounting-EAP-Auth-Method	0	0+
Acct-Interim-Interval [RFC3588]	0	0-1
Auth-Application-Id [RFC3588]	1	1
Auth-Grace-Period [RFC3588]	0-1	0-1
Auth-Request-Type [RFC3588]	1	1
Auth-Session-State [RFC3588]	0-1	0-1
Authorization-Lifetime [RFC3588]	0-1	0-1
Callback-Id [RFC4005]	0	0-1
Callback-Number [RFC4005]	0-1	0-1
Called-Station-Id [RFC4005]	0-1	0
Calling-Station-Id [RFC4005]	0-1	0
Class [RFC3588]	0	0+
Configuration-Token [RFC4005]	0	0+
Connect-Info [RFC4005]	0-1	0
Destination-Host [RFC3588]	0-1	0
Destination-Realm [RFC3588]	1	0
EAP-Master-Session-Key	0	0-1
EAP-Key-Name	0-1	0-1
EAP-Payload	1	0-1
EAP-Reissued-Payload	0	0-1
Error-Message [RFC3588]	0	0-1
Error-Reporting-Host [RFC3588]	0	0-1
Failed-AVP [RFC3588]	0	0+
Filter-Id [RFC4005]	0	0+
Framed-Appletalk-Link [RFC4005]	0	0-1
Framed-Appletalk-Network [RFC4005]	0	0+
Framed-Appletalk-Zone [RFC4005]	0	0-1
Framed-Compression [RFC4005]	0+	0+
Framed-Interface-Id [RFC4005]	0-1	0-1
Framed-IP-Address [RFC4005]	0-1	0-1
Framed-IP-Netmask [RFC4005]	0-1	0-1
Framed-IPv6-Prefix [RFC4005]	0+	0+
Framed-IPv6-Pool [RFC4005]	0	0-1
Framed-IPv6-Route [RFC4005]	0	0+

Framed-IPX-Network [RFC4005]	0	0-1
Framed-MTU [RFC4005]	0-1	0-1
Framed-Pool [RFC4005]	0	0-1
Framed-Protocol [RFC4005]	0-1	0-1
Framed-Route [RFC4005]	0	0+
Framed-Routing [RFC4005]	0	0-1
Idle-Timeout [RFC4005]	0	0-1
Multi-Round-Time-Out [RFC3588]	0	0-1
NAS-Filter-Rule [RFC4005]	0	0+
NAS-Identifier [RFC4005]	0-1	0
NAS-IP-Address [RFC4005]	0-1	0
NAS-IPv6-Address [RFC4005]	0-1	0
NAS-Port [RFC4005]	0-1	0
NAS-Port-Id [RFC4005]	0-1	0
NAS-Port-Type [RFC4005]	0-1	0
Originating-Line-Info [RFC4005]	0-1	0
Origin-Host [RFC3588]	1	1
Origin-Realm [RFC3588]	1	1
Origin-State-Id [RFC3588]	0-1	0-1
Port-Limit [RFC4005]	0-1	0-1
Proxy-Info [RFC3588]	0+	0+
QoS-Filter-Rule [RFC4005]	0	0+
Re-Auth-Request-Type [RFC3588]	0	0-1
Redirect-Host [RFC3588]	0	0+
Redirect-Host-Usage [RFC3588]	0	0-1
Redirect-Max-Cache-Time [RFC3588]	0	0-1
Reply-Message [RFC4005]	0	0+
Result-Code [RFC3588]	0	1
Route-Record [RFC3588]	0+	0+
Service-Type [RFC4005]	0-1	0-1
Session-Id [RFC3588]	1	1
Session-Timeout [RFC3588]	0	0-1
State [RFC4005]	0-1	0-1
Tunneling [RFC4005]	0+	0+
User-Name [RFC3588]	0-1	0-1

5.2 Tableau des AVP de comptabilité

Le tableau de ce paragraphe est utilisé pour représenter quelles AVP définies dans le présent document doivent être présentes dans les messages de comptabilité, comme défini dans la [RFC3588].

	Code de commande	
Nom d'attribut	**ACR**	**ACA**
Accounting-EAP-Auth-Method	0+	0

6. Interactions RADIUS/Diameter

La Section 9 de la [RFC4005] décrit les lignes directrices de base pour les agents de traduction qui assurent la traduction entre les protocoles RADIUS et Diameter. Ces lignes directrices DEVRAIENT être suivies aussi pour l'application EAP Diameter, avec quelques instructions supplémentaires données dans la présente Section. Noter que le présent document n'interdit pas aux mises en œuvre de créer des méthodes supplémentaires, pour autant que la fonction de traduction ne viole pas les protocoles RADIUS ou Diameter.

6.1 Demandes RADIUS transmises comme des demandes Diameter

Demande d'accès RADIUS à demande EAP Diameter :

- le ou les attributs RADIUS EAP-Message sont traduits en une AVP Diameter EAP-Payload. Si plusieurs attributs RADIUS EAP-Message sont présents, ils sont enchaînés et traduits en une seule AVP Diameter EAP-Payload.
- Un attribut RADIUS EAP-Message vide (de longueur 2) signifie EAP-Start, et est traduit en une AVP EAP-Payload vide.

Diameter-EAP-Answer à RADIUS Access-Accept/Reject/Challenge :
- o L'AVP Diameter EAP-Payload est traduite en attributs RADIUS EAP-Message. Si nécessaire, la valeur est partagée en plusieurs attributs RADIUS EAP-Message.
- o L'AVP Diameter EAP-Reissued-Payload est traduite en un message qui contient des attributs RADIUS EAP-Message, et un attribut RADIUS Error-Cause [RFC3576] de valeur 202 (en décimal), "paquet EAP invalide (ignoré)" [RFC3579].
- o Comme décrit dans la [RFC4005], si l'AVP Result-Code réglée à DIAMETER_MULTI_ROUND_AUTH et l'AVP Multi-Round-Time-Out sont présentes, elles sont traduites en l'attribut RADIUS Session-Timeout.
- o L'AVP Diameter EAP-Master-Session-Key peut être traduite en les attributs spécifiques de fabricant RADIUS MS-MPPE-Recv-Key et MS-MPPE-Send-Key [RFC2548]. Jusqu'aux 32 premiers octets de la clé sont mémorisés dans MS-MPPE-Recv-Key, et les 32 octets suivants (si ils sont présents) sont mémorisés dans MS-MPPE-Send-Key. Le chiffrement de cet attribut est décrit dans la [RFC2548].
- o Les AVP Diameter Accounting-EAP-Auth-Method, si elles sont présentes, sont éliminées.

6.2 Demandes Diameter transmises comme des demandes RADIUS

Diameter-EAP-Request à RADIUS Access-Request :
- o L'AVP Diameter EAP-Payload est traduite en attributs RADIUS EAP-Message.
- o Une AVP Diameter EAP-Payload vide signifie EAP-Start, et est traduite en un attribut RADIUS EAP-Message vide.
- o Le champ type (ou type étendu) de l'AVP EAP-Payload peut être sauvegardé dans un tableau d'état local, ou codé dans un attribut RADIUS Proxy-State. Cette information est nécessaire pour construire une AVP Accounting-EAP-Auth-Method pour le message de réponse (voir ci-dessous).

RADIUS Access-Accept/Reject/Challenge à Diameter-EAP-Answer :
- o Si le message RADIUS Access-Challenge ne contient pas d'attribut Error-Cause [RFC3576] de valeur 202 (en décimal), "paquet EAP invalide (ignoré)" [RFC3579], tous les attributs RADIUS EAP-Message sont traduits en une AVP Diameter EAP-Payload, en les enchaînant si plusieurs attributs sont présents.
- o Si l'attribut Error-Cause de valeur 202 est présent, tout attribut RADIUS EAP-Message est traduit en une AVP Diameter EAP-Reissued-Payload, en les enchaînant si plusieurs attributs sont présents.
- o Comme décrit dans la [RFC4005], si l'attribut Session-Timeout est présent dans un message RADIUS Access-Challenge, il est traduit en AVP Diameter Multi-Round-Time-Out.
- o Si les attributs RADIUS spécifiques de fabricant MS-MPPE-Recv-Key et/ou MS-MPPE-Send-Key [RFC2548] sont présents, ils peuvent être traduits en AVP Diameter EAP-Master-Session-Key. Les attributs doivent être déchiffrés avant la conversion, et les sous champs Sel, Longueur de clé et Bourrage sont éliminés. Les sous champs Clé sont enchaînés (d'abord MS-MPPE-Recv-Key, MS-MPPE-Send-Key ensuite) et la valeur enchaînée est mémorisée dans une AVP Diameter EAP-Master-Session-Key.
- o Si la réponse EAP Diameter a un code de résultat de succès, l'état sauvegardé (voir ci-dessus) peut être utilisé pour construire une AVP Accounting-EAP-Auth-Method.

6.3 Demandes de comptabilité

Dans les demandes de comptabilité, l'attribut RADIUS spécifique de fabricant MS-Acct-EAP-Type [RFC2548] peut être traduit en une AVP Diameter Accounting-EAP-Auth-Method, et vice versa.

Lors de la traduction de Diameter en RADIUS, noter que l'attribut MS-Acct-EAP-Type ne prend pas en charge les types EAP étendus. Les valeurs de type supérieures à 255 devraient être traduites en le type 254.

7. Considérations relatives à l'IANA

Les présent document ne crée aucun nouvel espace de noms que devrait tenir l'IANA, mais exige de nouvelles valeurs dans des espaces de noms qui ont été définis dans les spécifications du protocole Diameter de base et de RADIUS.

- o Le présent document définit une nouvelle commande Diameter (Section 3) dont le code de commande est alloué à partir de l'espace de noms de code de commandes défini dans la [RFC3588]. Le code de commande pour DER/DEA est 268.

- o Le présent document définit quatre nouvelles AVP dont les codes d'AVP sont alloués dans l'espace de noms de code d'AVP défini dans la [RFC3588] comme suit :
  462 pour EAP-Payload (définie au paragraphe 4.1.1),
  463 pour EAP-Reissued-Payload (définie au paragraphe 4.1.2),
  464 pour EAP-Master-Session-Key (définie au paragraphe 4.1.3), et

465 pour Accounting-EAP-Auth-Method (définie au paragraphe 4.1.5).

- Le présent document définit une nouvelle AVP (attribut) dont le code d'AVP (type d'attribut) est à allouer dans l'espace de noms Type d'attribut défini dans les [RFC2865] et [RFC3575]. Le type d'attribut RADIUS pour EAP-Key-Name (défini au paragraphe 4.1.4) est 102.

- Le présent document définit une nouvelle application Diameter (au paragraphe 2.1) dont l'identifiant d'application est à allouer dans l'espace de noms Identifiant d'application défini dans la [RFC3588]. L'identifiant d'application pour EAP Diameter est 5.

8. Considérations pour la sécurité

8.1 Vue d'ensemble

Les connexions Diameter d'homologue à homologue peuvent être protégées avec IPsec ou TLS. Ces mécanismes sont estimés fournir une protection suffisante sous le modèle normal de menaces de l'Internet, c'est-à-dire en supposant que les nœuds autorisés qui s'engagent dans le protocole n'ont pas été compromis, mais que l'attaquant a le contrôle complet des canaux de communication entre eux. Cela inclut l'espionnage, la modification de message, l'insertion, et les attaques par interposition et en répétition. Les détails et les considérations sur la sécurité qui s'y rapportent sont exposées dans la [RFC3588].

En plus de l'authentification fournie par IPsec ou TLS, l'autorisation est aussi requise. Ici, autorisation signifie de déterminer si un message Diameter reçu d'un homologue Diameter authentifié devrait être accepté (et non l'autorisation des utilisateurs demandant l'accès réseau au NAS). En d'autres termes, lorsque un serveur Diameter reçoit une demande EAP Diameter, il doit décider si le client est autorisé à agir comme NAS pour l'utilisateur spécifique, le type de service, et ainsi de suite. De même, lorsque un NAS contacte un serveur pour envoyer une demande EAP Diameter, il doit déterminer si le serveur est autorisé à agir comme serveur de rattachement pour le domaine en question.

L'autorisation peut impliquer des listes de contrôle d'accès (ACL, *Access Control List*) locales, des informations contenues dans les certificats, ou d'autres moyens. Voir dans la [RFC3588] un exposé plus complet et les considérations sur la sécurité qui s'y rapportent. Noter que les questions d'autorisation sont particulièrement pertinentes lorsque des redirections Diameter sont utilisées. Alors que la redirection réduit le nombre de nœuds qui ont accès au contenu des messages Diameter, un agent Diameter compromis ne peut pas fournir l'adresse du bon serveur de rattachement. Si le client Diameter est incapable de dire si ce serveur particulier est autorisé à agir comme serveur de rattachement pour cet utilisateur particulier, la sécurité des communications relève de l'agent de redirection.

Les mécanismes de sécurité bond par bond (IPsec et TLS) combinés à l'autorisation appropriée fournissent une bonne protection contre les attaques "de l'extérieur", sauf les attaques de déni de service. Le reste de cette section traite des attaques par des nœuds qui ont bien été autorisés (à fonctionner comme un NAS, un agent Diameter, ou un serveur Diameter) mais abusent de leur autorisation ou ont été compromis. En général, il n'est pas possible de se protéger complètement contre les attaques par des nœuds compromis, mais cette section propose de limiter l'étendue des dommages.

Les attaques qui impliquent l'espionnage ou la modification des messages EAP sortent du domaine d'application de ce document. Voir dans la [RFC3748] la discussion de ces considérations sur la sécurité (incluant la négociation de la méthode, les attaques de dictionnaire, et les questions de confidentialité). Bien que ces attaques puissent être menées par un attaquant entre le client et le NAS, les NAS et agents Diameter compromis sont naturellement aussi dans une bonne position pour modifier et espionner les messages EAP.

De même, les attaques qui impliquent le protocole de couche liaison utilisé entre le client et le NAS, comme PPP ou IEEE 802.11, sortent du domaine d'application de ce document.

8.2 Édition d'AVP

Les agents Diameter peuvent modifier, insérer, et supprimer des AVP. Les agents Diameter sont généralement destinés à modifier les AVP, et le protocole ne peut pas distinguer les modifications bien intentionnées des malveillantes (voir plus de détails dans la [RFC2607]). De même, un NAS ou serveur compromis peut naturellement inclure un ensemble d'AVP différent de celui attendu.

Donc, la question est que peut faire un attaquant qui a compromis un NAS, agent, ou serveur autorisé en utilisant les messages EAP Diameter ? Certaines des conséquences sont assez évidentes. Par exemple, un agent Diameter peut donner accès à des utilisateurs non autorisés en changeant le code de résultat en DIAMETER_SUCCESS. D'autres conséquences

sont moins évidentes et sont discutées ci-dessous et les attaques de négociation de méthode d'authentification sont discutées au paragraphe suivant.

En incluant les AVP convenables dans des messages AA-Answer/Diameter-EAP-Answer, un attaquant peut être capable (selon la mise en œuvre et les détails de configuration) de :
- o donner accès à des utilisateurs non autorisés, ou refuser l'accès à des utilisateurs autorisés (code de résultat) ;
- o donner à un attaquant une session connectée à un hôte par ailleurs protégé par des pare-feu, ou rediriger une session de connexion d'un utilisateur autorisé sur un hôte contrôlé par l'attaquant (Login-Host) ;
- o acheminer le trafic d'un utilisateur autorisé à travers un hôte contrôlé par l'attaquant (diverses AVP de tunnelage) ;
- o rediriger les demandes au DNS d'un utilisateur autorisé sur un serveur DNS malveillant (diverses AVP spécifiques de fabricant) ;
- o modifier les tableaux d'acheminement au NAS et donc rediriger les paquets destinés à quelqu'un d'autre (Framed-Route, Framed-Routing) ;
- o retirer les filtres de paquet et autres restrictions pour l'utilisateur (AVP Filter, Callback, et diverses spécifiques de fabricant) ;
- o causer l'appel d'un numéro par le NAS, éventuellement un numéro à forte tarification contrôlé par l'attaquant (AVP de rappel) ;
- o exécuter des commandes d'interface de ligne de commande (CLI, *Command Line Interface*) sur le NAS (divers attributs spécifiques de fabricant).

En modifiant une AA-Request/Diameter-EAP-Request, un attaquant peut être capable de :
- o changer le NAS-Identifier/NAS-Port/Origin-Host (ou autre attribut) afin qu'un utilisateur valide paraisse accéder au réseau à partir d'un NAS différent du NAS réel ;
- o modifier le Calling-Station-ID (pour cacher la vraie valeur, obtenir l'accès, ou tramer quelqu'un d'autre) ;
- o modifier des messages de changement de mot de passe (des attributs spécifiques de fabricant) ;
- o modifier des informations d'utilisation dans les messages de comptabilité ;
- o modifier le contenu des AVP Class et State.

Certaines de ces attaques peuvent être empêchées si le NAS ou serveur est configuré à ne pas accepter certaines AVP particulières, ou à ne les accepter que de certains nœuds.

8.3 Attaques sur la négociation

Ce paragraphe traite des attaques où le NAS, tout agent ou serveur Diameter, tente de causer le choix par l'utilisateur qui s'authentifie d'une méthode d'authentification autre que EAP, comme PAP ou CHAP (les attaques de négociation au sein de EAP sont discutées au paragraphe 7.8 de la [RFC3748]).

La vulnérabilité peut être atténuée via la mise en œuvre d'une politique par connexion par l'homologue qui s'authentifie, et une politique par utilisateur par le serveur Diameter. Pour l'homologue qui s'authentifie, la politique d'authentification devrait être réglée connexion par connexion.

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 de EAP est attendue. Par suite, on présume qu'un homologue qui s'authentifie en choisissant EAP exige ce niveau de sécurité. Si il ne peut pas être fourni, il y a probablement une mauvaise configuration, ou l'homologue qui s'authentifie peut être en train de contacter le mauvais serveur. Dans ce cas, l'homologue qui s'authentifie se déconnecte simplement.

De même, avec une politique par utilisateur, le serveur de rattachement ne va pas accepter des méthodes d'authentification autres que EAP pour des utilisateurs pour lesquels la prise en charge de EAP est attendue.

Pour un NAS, il peut n'être pas possible de déterminer si un homologue est obligé de s'authentifier avec EAP tant que l'identité de l'homologue n'est pas connue. Par exemple, pour les NAS en utilisation partagée, un revendeur peut mettre en œuvre EAP tandis qu'un autre ne le fait pas. Autrement, un certain homologue peut être authentifié en local par le NAS tandis que d'autres homologues sont authentifiés via Diameter. Dans ce cas, si un homologue du NAS DOIT faire EAP, le NAS DOIT tenter de négocier EAP pour toutes les sessions. Cela évite de forcer un homologue à prendre en charge plus d'un type d'authentification, ce qui pourrait affaiblir la sécurité.

8.4 Distribution des clés de session

Comme il n'y a actuellement aucun mécanisme de sécurité de bout en bout (du NAS au serveur de rattachement) spécifié pour Diameter, tous les agents qui traitent les messages Diameter-EAP-Answer peuvent voir le contenu de l'AVP EAP-

Master-Session-Key. Pour cette raison, la présente spécification recommande fortement d'éviter les agents Diameter qui ne sont pas de confiance pour garder les clés secrètes.

Dans des environnements où des agents sont présents, plusieurs facteurs devraient être pris en considération pour décider si les agents qui sont autorisés (et considérés comme "assez de confiance") à accorder l'accès aux utilisateurs et spécifier les diverses AVP d'autorisation et tunnelage sont aussi "assez de confiance" pour traiter les clés de session. Ces facteurs incluent le (mais ne se limitent pas au) type d'accès fourni (par exemple, Internet public ou internet d'entreprise) niveau de sécurité des agents, et les possibilités d'attaque du trafic de l'utilisateur après qu'il ait été déchiffré par le NAS.

Noter que les clés communiquées dans les messages Diameter sont généralement des clés de session à court terme (ou des clés maîtresses à court terme qui sont utilisées pour déduire les clés de session). Pour causer réellement des dommages, ces clés de session doivent tomber entre les mains d'un malveillant qui doit être capable d'espionner, modifier ou insérer du trafic entre l'utilisateur et le NAS pendant la durée de vie de ces clés (par exemple, dans 802.11i l'attaquant doit aussi espionner la "prise de contact en quatre phases").

8.5 Questions de confidentialité

Les messages Diameter peuvent contenir des AVP qui peuvent être utilisées pour identifier l'utilisateur (par exemple, le nom d'utilisateur) et approximer la localisation de l'utilisateur (par exemple, Origin-Host pour les points d'accès de WLAN, Calling-Station-Id pour les lignes de téléphone fixe). Donc, tout nœud Diameter qui traite les messages peut être capable de déterminer la localisation géographique des utilisateurs.

Noter que dans de nombreux cas, l'identité de l'utilisateur est aussi envoyée en clair dans les AVP EAP-Payload, et il est possible d'espionner cela entre l'utilisateur et le NAS.

Ceci peut être atténué un peu en utilisant les méthodes EAP qui fournissent la protection de l'identité (voir le paragraphe 7.3 de la [RFC3748]) et en utilisant l'identifiant de session ou des pseudonymes pour la comptabilité.

8.6 Note sur EAP et l'usurpation d'identité

Si la méthode EAP utilisée ne fournit pas l'authentification mutuelle, n'importe qui peut évidemment se faire passer pour le réseau aux yeux de l'utilisateur. Même lorsque l'authentification mutuelle EAP est utilisée, elle se produit entre l'utilisateur et le serveur de rattachement Diameter. Voir dans la [RFC5247] une discussion étendue des détails et leurs implications.

Une question vaut d'être soulignée ici. Comme décrit dans la [RFC5247], l'architecture EAP actuelle ne permet pas au serveur de rattachement de restreindre les paramètres ou identités de service (comme SSID ou BSSID dans les LAN sans fil 802.11) qui sont annoncés par le NAS au client. C'est-à-dire qu'un NAS compromis peut changer sa BSSID ou SSID, et donc apparaître comme offrant un service différent de celui attendu. Même si ces paramètres sont inclus dans les messages Diameter-EAP-Answer, le NAS peut dire des valeurs différentes au client.

Donc, la possession des clés de session par le NAS prouve que l'utilisateur est en train de parler à un NAS autorisé, mais un NAS compromis peut mentir sur son identité réelle. Voir dans la [RFC5247] la discussion sur la façon dont les méthodes EAP individuelles peuvent fournir l'authentification des paramètres et identités de service de NAS.

Noter que l'utilité de cette authentification peut être assez limitée dans de nombreux environnements. Par exemple, dans les LAN sans fil l'utilisateur ne sait généralement pas de façon sûre l'identité (comme un BSSID) du "bon" point d'accès ; il est simplement ramassé à partir du message d'une balise qui a le SSID correct et la bonne force de signal (quelque chose qu'il est facile d'imiter). Donc, simplement authentifier l'identité peut ne pas permettre à l'utilisateur de distinguer le "bon" point d'accès de tous les autres.

9. Remerciements

La présente application Diameter s'appuie fortement sur les travaux sur l'application NASREQ Diameter [RFC4005] et la prise en charge d'EAP par RADIUS [RFC3579]. Beaucoup des matériaux de la présente spécification ont été copiés dans ces documents.

Les auteurs tiennent aussi à remercier les personnes suivantes de leurs contributions à ce document : Bernard Aboba, Jari Arkko, Julien Bournelle, Pat Calhoun, Henry Haverinen, John Loughney, Yoshihiro Ohba, et Joseph Salowey.

10. Références

10.1 Références normatives

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

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

[RFC3748] B. Aboba et autres, "Protocole extensible d'authentification (EAP)", juin 2004. *(P.S., MàJ par* RFC5247)

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

10.2 Références pour information

[IEEE-802.1X] Institute of Electrical and Electronics Engineers, "Local and Metropolitan Area Networks: Port-Based Network Access Control", IEEE Standard 802.1X, septembre 2001.

[IEEE-802.11i] Institute of Electrical and Electronics Engineers, "IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements", IEEE Standard 802.11i-2004, juillet 2004.

[RFC1661] W. Simpson, éditeur, "Protocole point à point (PPP)", STD 51, juillet 1994. *(MàJ par la* RFC2153)

[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.)*

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

[RFC3575] B. Aboba, "Considérations relatives à l'IANA pour le service d'authentification distante d'utilisateur appelant (RADIUS)", juillet 2003. (*MàJ* RFC2865) *(P.S.)*

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

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

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

[RFC4306] C. Kaufman, "Protocole d'échange de clés sur Internet (IKEv2)", décembre 2005. *(Obsolète, voir la* RFC5996)

[RFC5247] B. Aboba et autres, "Cadre de gestion des clés du protocole d'authentification extensible (EAP)", août 2008. (*MàJ* RFC3748) *(P.S.)*

Adresse des auteurs

Pasi Eronen (editor)
Nokia Research Center
P.O. Box 407
FIN-00045 Nokia Group
Finland
mél : pasi.eronen@nokia.com

Tom Hiller
Lucent Technologies
1960 Lucent Lane
Naperville, IL 60566
USA
téléphone : +1 630 979 7673
mél : tomhiller@lucent.com

Glen Zorn
Cisco Systems
500 108th Avenue N.E., Suite 500
Bellevue, WA 98004
USA
téléphone : +1 425 344 8113
mél : gwz@cisco.com

Déclaration complète de droits de reproduction

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