Internet Engineering Task Force (IETF)
Request for Comments : 7155
RFC rendue obsolète : 4005
Catégorie : En cours de normalisation
ISSN: 2070-1721

G. Zorn, éditeur
Network Zen
avril 2014
Traduction Claude Brière de L'Isle

Application de serveur d'accès réseau Diameter

Résumé
Le présent document décrit l'application du protocole Diameter qui est utilisée pour les services d'authentification, autorisation, et comptabilité dans l'environnement de serveur d'accès réseau (NAS, *Network Access Server*) ; il rend obsolète la RFC 4005. Lorsque combiné avec les spécifications du protocole Diameter de base, du profil de transport, et du protocole extensible d'authentification, la présente spécification d'application satisfait aux exigences normales des services d'accès réseau.

Statut de ce mémoire
Ceci est un document de l'Internet en cours de normalisation.

Le présent document a été produit par l'équipe d'ingénierie de l'Internet (IETF). Il représente le consensus de la communauté de l'IETF. Il a subi une révision publique et sa publication a été approuvée par le groupe de pilotage de l'ingénierie de l'Internet (IESG). Plus d'informations sur les normes de l'Internet sont disponibles à la Section 2 de la [RFC5741].

Les informations sur le statut actuel du présent document, tout errata, et comment fournir des réactions sur lui peuvent être obtenues à http://www.rfc-editor.org/info/rfc7155

Table des Matières

1. Introduction

Le présent document décrit l'application de protocole Diameter utilisée pour l'authentification, l'autorisation, et la comptabilité dans l'environnement de serveur d'accès réseau (NAS, *Network Access Server*). Lorsque combiné avec les spécifications du protocole de base Diameter [RFC6733], du profil de transport [RFC3539], et du protocole d'authentification extensible (EAP, *Extensible Authentication Protocol*) [RFC4072], la présente spécification satisfait aux exigences relatives aux NAS définies dans les [RFC2989] et [RFC3169].

D'abord, le présent document décrit le fonctionnement d'une application de NAS Diameter. Puis il définit les codes de commande du message Diameter. Les sections qui suivent font la liste des AVP utilisées dans ces messages, groupées par usage commun. Ce sont l'identification de session, l'authentification, l'autorisation, le tunnelage, et la comptabilité. Les AVP d'autorisation sont de plus subdivisées par type de service.

1.1 Changements par rapport à la RFC 4005

Le présent document rend obsolète la [RFC4005] et avec laquelle il n'est pas rétro compatible. Un survol des changements majeurs est fait ci-dessous.

- Tout ce qui concerne les interactions RADIUS/Diameter a été supprimé ; cependant, lorsque les AVP sont dérivées des attributs RADIUS, la gamme et le format de ces valeurs d'attribut ont été conservés pour faciliter la transition.

- Le format de code de commande (CCF, *Command Code Format*) [RFC6733] pour les messages Demande/Réponse de comptabilité a été changé pour exiger explicitement l'inclusion de l'AVP Acct-Application-Id et exclure l'AVP Vendor-Specific-Application-Id. Normalement, ce type de changement devrait exiger l'allocation d'un nouveau code de commande (voir au paragraphe 1.3.3 de la [RFC6733]) et par conséquent, un nouvel identifiant d'application. Cependant, la présence d'une instance de l'AVP Acct-Application-Id était aussi exigée dans la [RFC4005] : le message Accounting-Request (ACR) [RFC3588] est envoyé par le NAS pour rapporter ses informations de session à un serveur cible en aval. L'AVP Acct-Application-Id ou l'AVP Vendor-Specific-Application-Id DOIT être présente. Si l'AVP groupée Vendor-Specific-Application-Id est présente, elle doit avoir une AVP Acct-Application-Id en son sein. Donc, bien que la syntaxe des commandes ait changé, la sémantique est restée la même (avec l'avertissement que l'AVP Acct-Application-Id ne peut plus être contenue dans l'AVP Vendor-Specific-Application-Id).

- Les listes de valeurs d'attributs RADIUS ont été supprimées en faveur de références aux registres IANA appropriés.

- Le modèle comptable à utiliser est maintenant spécifié (paragraphe 1.6).

Il y a de nombreuses autres corrections diverses qui ont été introduites dans le présent document qui peuvent n'être pas considérées comme significatives, mais elles sont néanmoins utiles. Des exemples en sont les corrections aux exemples

d'adresses IP, l'ajout de références à des éclaircissements, etc. Les Errata à l'égard de la [RFC4005] au moment de cette rédaction ont été incorporés en tant que de besoin. On ne fait pas ici pour des raisons pratiques une liste complète des corrections.

1.2 Terminologie

Le paragraphe 1.2 de la spécification du protocole de base Diameter [RFC6733] définit l'essentiel de la terminologie utilisée dans le présent document. Les termes et acronymes suivants sont utilisés dans cette application :

Serveur d'accès réseau (NAS, *Network Access Server*) : Appareil qui fournit un service d'accès à l'utilisateur d'un réseau. Le service peut être une connexion réseau ou un service à valeur ajoutée comme une émulation de terminal [RFC2881].

Protocole point à point (PPP, *Point-to-Point Protocol*) : Liaison de données en série multi protocoles. PPP est la principale liaison de données IP pour le service de connexion de NAS commuté [RFC1661].

Protocole d'authentification par dialogue à énigme (CHAP, *Challenge Handshake Authentication Protocol*) : Processus d'authentification utilisé dans PPP [RFC1994].

Protocole d'authentification par mot de passe (PAP, *Password Authentication Protocol*) : Processus d'authentification déconseillé dans PP, mais souvent utilisé pour la rétro compatibilité [RFC1334].

Protocole Internet de ligne en série (SLIP, *Serial Line Internet Protocol*) : Liaison de données en série qui ne prend en charge que IP. Un concept d'avant PPP.

Protocole d'accès distant AppleTalk (ARAP, *AppleTalk Remote Access Protocol*) : Liaison de données en série pour accéder aux réseaux AppleTalk [ARAP].

Échange de paquets inter réseaux (IPX, *Internetwork Packet Exchange*) : Protocole réseau utilisé par les réseaux NetWare [IPX].

Protocole de tunnelage de couche 2 (L2TP, *Layer Two Tunneling Protocol*) : L2TP [RFC3931] fournit un mécanisme dynamique pour tunneler les "circuits" de couche 2 à travers un réseau de données en mode paquet.

Concentrateur d'accès L2TP (LAC, *L2TP Access Concentrator*) : Point d'extrémité de connexion de contrôle L2TP utilisé pour interconnecter une session L2TP directement à une liaison de données [RFC3931].

Transport de zone locale (LAT, *Local Area Transport*) : Protocole de LAN de Digital Equipment Corp. pour les services de terminaux [LAT].

Protocole de contrôle de liaison (LCP, *Link Control Protocol*) : Un des trois composants majeurs de PPP [RFC1661]. LCP est utilisé pour s'accorder automatiquement sur les options de format d'encapsulation, traiter les variations de limites des tailles de paquets, détecter une liaison en boucle et autres erreurs courantes de configuration, et terminer la liaison. D'autres facilités facultatives fournies sont l'authentification de l'identité de l'homologue sur la liaison, et la détermination de quand la liaison fonctionne correctement et quand elle est défaillante.

Protocole de tunnelage de point à point (PPTP, *Point-to-Point Tunneling Protocol*) : Protocole qui permet à PPP d'être tunnelé à travers un réseau IP [RFC2637].

Réseau privé virtuel (VPN, *Virtual Private Network*) : Dans le présent document, ce terme est utilisé pour décrire les services d'accès qui utilisent des méthodes de tunnelage.

1.3 Langage des exigences

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

L'utilisation de "DOIT" et "NE DOIT PAS" dans les colonnes Règles de fanions d'AVP des tableaux d'AVP de la Section 4 du présent document se réfère aux fanions d'AVP (au paragraphe 4.1 de la [RFC6733]) qui :

- DOIVENT être réglés à 1 dans l'en-tête d'AVP (colonne "DOIT") et
- NE DOIVENT PAS être réglés à 1 (colonne "NE DOIT PAS")

1.4 Annonce de la prise en charge d'application

Les nœuds Diameter qui se conforment à la présente spécification DOIVENT annoncer la prise en charge de l'application en incluant la valeur de un (1) dans le champ Auth-Application-Id du message de demande d'échange de capacités (CER, *Capabilities-Exchange-Request*) [RFC6733].

1.5 Identification d'application d'authentification

Lorsque elle est utilisée dans la présente application, l'AVP Auth-Application-Id *(identifiant d'application d'autorisation)* DOIT être réglée à la valeur un (1) dans les messages suivants :

- AA-Request *(demande d'authentification-autorisation)* (paragraphe 3.1)
- Re-Auth-Request *(demande de réautorisation)* (paragraphe 3.3)
- Session-Termination-Request *(demande de terminaison de sessiion)* (paragraphe 3.5)
- Abort-Session-Request *(demande d'interruption de session)* (paragraphe 3.7)

1.6 Modèle de comptabilité

Il est RECOMMANDÉ que le modèle de comptabilité couplé du paragraphe 9.3 de la [RFC6733] soit utilisé avec cette application ; donc, la valeur de l'AVP Acct-Application-Id dans les messages Demande de comptabilité *(Accounting-Request)* (paragraphe 3.9) et Réponse de comptabilité *(Accounting-Answer)* (paragraphe 3.10) DEVRAIT être de un (1).

2. Appels, accès et session de NAS

L'arrivée d'un nouvel appel ou connexion de service à un accès d'un serveur d'accès réseau (NAS, *Network Access Server*) commence par un échange de messages d'application de NAS Diameter. Les informations sur l'appel, l'identité de l'utilisateur, et les informations d'authentification de l'utilisateur sont mises en paquets dans des messages Diameter de demande d'authentification et autorisation (AAR, *AA-Request*) et envoyées à un serveur.

Le serveur traite les informations et répond par un message Diameter de réponse d'authentification et autorisation (AAA, *AA-Answer*) qui contient les informations d'autorisation pour le NAS ou un code d'échec (AVP Result-Code). Une valeur de DIAMETER_MULTI_ROUND_AUTH indique un échange d'authentification supplémentaire, et plusieurs messages AAR et AAA peuvent être échangés jusqu'à ce que la transaction s'achève.

2.1 Établissement de session Diameter

Lorsque l'échange d'authentification ou autorisation s'achève avec succès, l'application de NAS DEVRAIT commencer un contexte de session. Si le code de résultat DIAMETER_MULTI_ROUND_AUTH est retourné, l'échange se poursuit jusqu'à ce que soit retourné un succès ou une erreur.

Si la comptabilité est active, l'application DOIT aussi envoyer un message Accounting [RFC6733]. Un type d'enregistrement de comptabilité *(Accounting-Record-Type)* de START_RECORD *(début d'enregistrement)* est envoyé pour une nouvelle session. Si une session ne réussit pas à débuter, le message EVENT_RECORD *(événement d'enregistrement)* est envoyé avec la description de la raison de l'échec.

Noter que le retour d'une valeur de Accounting-Realtime-Required *(comptabilité en temps réel exigée)* [RFC6733] non prise en charge résultera en un échec d'établissement de la session.

2.2 Réauthentification ou réautorisation de session Diameter

Le protocole Diameter de base permet aux utilisateurs d'être périodiquement réauthentifiés et/ou réautorisés. Dans de telles instances, l'AVP Session-Id *(identifiant de session)* dans le message AAR DOIT être la même que celle présente dans le message d'authentification/autorisation d'origine.

Un serveur Diameter informe le NAS du délai maximum permis avant la réauthentification ou réautorisation via l'AVP Authorization-Lifetime *(durée de vie d'autorisation)* [RFC6733]. Un NAS PEUT être réauthentifié et/ou réautorisé avant la fin, mais un NAS DOIT se réauthentifier et/ou se réautoriser à la fin de la période donnée par l'AVP Authorization-Lifetime. L'échec d'un échange de réauthentification va terminer le service.

De plus, il est possible aux serveurs Diameter de produire une demande non sollicitée de réauthentification et/ou réautorisation (par exemple, un message Re-Auth-Request (RAR) [RFC6733]) au NAS. À réception d'un tel message, le NAS DOIT répondre à la demande par un message Re-Auth-Answer (RAA) [RFC6733].

Si le message RAR identifie correctement une session active, le NAS va initier une nouvelle séquence locale de réauthentification ou d'autorisation comme indiqué par la valeur du Re-Auth-Request-Type *(type de demande de réauthentification)*. Cela va causer l'envoi par le NAS d'un nouveau message AAR utilisant l'identifiant de session existant. Le serveur va répondre par un message AAA pour spécifier les nouveaux paramètres de service.

Si la comptabilité est active, chaque changement d'authentification ou d'autorisation DEVRAIT générer un message de comptabilité. Si le service de NAS est la continuation d'un contexte d'utilisateur antérieur, un Accounting-Record-Type de INTERIM_RECORD indiquant les nouveaux attributs de session et l'état cumulatif sera alors approprié. Si un nouvel utilisateur ou un changement significatif de l'autorisation est détecté par le NAS, le service peut alors envoyer deux messages des types STOP_RECORD et START_RECORD. La comptabilité peut changer les identifiants de sous session (Acct-Session-Id, ou Acct-Sub-Session-Id) pour indiquer de telles sous sessions. Un service peut aussi utiliser une valeur différente d'identifiant de session pour la comptabilité (voir le paragraphe 9.6 de la [RFC6733]).

Cependant, la valeur d'AVP Session-Id Diameter utilisée pour l'échange initial d'autorisation DOIT être utilisée pour générer un message STR lorsque le contexte de la session est terminé.

2.3 Terminaison de session Diameter

Lorsque un NAS reçoit une indication que la session d'un utilisateur est en train d'être déconnectée par le client (par exemple, un message LCP Terminate-Request [RFC1661] est reçu) ou une commande administrative, le NAS DOIT produire un message Demande de terminaison de session (STR, *Session-Termination-Request*) [RFC6733] à son serveur Diameter. Cela va assurer que toutes les ressources conservées sur les serveurs seront libérée convenablement.

De plus, un NAS qui reçoit un message Demande d'interruption de session (ASR, *Abort-Session-Request*) [RFC6733] DOIT produire une réponse d'interruption de session (ASA, *Abort-Session-Answer*) si la session identifiée est active et déconnecter la session PPP (ou le tunnelage).

Si la comptabilité est active, un message de comptabilité STOP_RECORD *(arrêt d'enregistrement)* [RFC6733] DOIT être envoyé dès la terminaison du contexte de session.

Plus d'informations sur la terminaison de session Diameter se trouvent aux paragraphes 8.4 et 8.5 de la [RFC6733].

3. Messages d'application de NAS Diameter

La présente Section définit les valeurs de code de commande de message Diameter [RFC6733] qui DOIVENT être prises en charge par toutes les mises en œuvre Diameter conformes à la présente spécification. Les codes de commande sont comme suit :

Nom de commande	**Abréviation**	**Code**	**Référence**
AA-Request *(demande AA)*	AAR	265	paragraphe 3.1
AA-Answer *(réponse AA)*	AAA	265	paragraphe 3.2
Re-Auth-Request *(demande de réauthentification)*	RAR	258	paragraphe 3.3
Re-Auth-Answer *(réponse de réauthentification)*	RAA	258	paragraphe 3.4
Session-Termination-Request *(demande de terminaison de session)*	STR	275	paragraphe 3.5
Session-Termination-Answer *(réponse de terminaison de session)*	STA	275	paragraphe 3.6
Abort-Session-Request *(demande d'interruption de session)*	ASR	274	paragraphe 3.7
Abort-Session-Answer *(réponse d'interruption de session)*	ASA	274	paragraphe 3.8
Accounting-Request *(demande de comptabilité)*	ACR	271	paragraphe 3.9
Accounting-Answer *(réponse de comptabilité)*	ACA	271	paragraphe 3.10

Noter que les formats de message dans les paragraphes qui suivent utilisent le format standard de code de commande Diameter du paragraphe 3.2 de la [RFC6733].

3.1 Commande AA-Request (AAR)

La commande AA-Request (AAR), qui est indiquée par le réglage du champ Code de commande à 265 et le bit 'R' dans le champ Fanions de commande, est utilisée pour demander l'authentification et/ou l'autorisation pour un certain NAS utilisateur. Le type de demande est identifié par l'AVP Auth-Request-Type [RFC6733]. La valeur recommandée pour la plupart des situations est AUTHORIZE_AUTHENTICATE.

Si l'authentification est demandée, l'attribut User-Name *(nom d'utilisateur)* DEVRAIT être présent, ainsi que toutes AVP d'authentification supplémentaires qui porteraient des informations de mot de passe. Une demande d'autorisation DEVRAIT inclure seulement les informations à partir desquelles l'autorisation sera effectuée, comme les AVP User-Name, Called-Station-Id, ou Calling-Station-Id. Toutes les demandes DEVRAIENT contenir des AVP identifiant de façon univoque la source de l'appel, comme Origin-Host *(hôte d'origine)* et NAS-Port *(accès de NAS)*. Certains réseaux PEUVENT utiliser des AVP différentes pour les besoins d'autorisation. Une demande d'autorisation inclura certaines des AVP définies au paragraphe 4.4.

Il est possible qu'une seule session soit autorisée d'abord et qu'ensuite une demande d'authentification suive.

Ce message AA-Request PEUT être le résultat d'un échange d'authentification à plusieurs tours, qui se produit lorsque le message AA-Answer est reçu avec l'AVP Result-Code réglée à DIAMETER_MULTI_ROUND_AUTH. Un message AAR DEVRAIT être ensuite envoyé, avec l'AVP User-Password *(mot de passe d'utilisateur)* qui comporte la réponse de l'utilisateur à l'invite et DOIT inclure toutes les AVP d'état qui étaient présentes dans le message AAA.

(Note du traducteur : la présence des AVP figurant entre des accolades "{" "}" est obligatoire ; celles des AVP entre crochets "[" "]" est facultative, conformément au paragraphe 3.2 de la RFC 6733.)

Format de message :

<AA-Request> ::= < En-tête Diameter : 265, REQ, PXY >
< Session-Id > *(identifiant de session)*
{ Auth-Application-Id } *(identifiant d'application d'authentification)*
{ Origin-Host } *(hôte d'origine)*
{ Origin-Realm } *(domaine d'origine)*
{ Destination-Realm } *(domaine de destination)*
{ Auth-Request-Type } *(type de demande d'authentification)*
[Destination-Host] *(hôte de destination)*
[NAS-Identifier] *(identifiant de NAS)*
[NAS-IP-Address] *(Adresse IP de NAS)*
[NAS-IPv6-Address] *(adresse IPv6 de NAS)*
[NAS-Port] *(accès de NAS)*
[NAS-Port-Id] *(identifiant d'accès de NAS)*
[NAS-Port-Type] *(type d'accès de NAS)*
[Origin-AAA-Protocol] *(protocole AAA d'origine)*
[Origin-State-Id] *(identifiant d'état d'origine)*
[Port-Limit] *(limite d'accès)*
[User-Name] *(nom d'utilisateur)*
[User-Password] *(mot de passe d'utilisateur)*
[Service-Type] *(type de service)*
[State] *(état)*
[Authorization-Lifetime] *(durée de vie d'autorisation)*
[Auth-Grace-Period] *(période de grâce d'autorisation)*
[Auth-Session-State] *(état de session d'autorisation)*
[Callback-Number] *(numéro de rappel)*
[Called-Station-Id] *(identifiant de la station demandée)*
[Calling-Station-Id] *(identifiant de la station appelante)*
[Originating-Line-Info] *(informations sur la ligne appelante)*
[Connect-Info] *(informations de connexion)*
[CHAP-Auth] *(authentification CHAP)*
[CHAP-Challenge] *(défi CHAP)*
* [Framed-Compression] *(compression tramée)*
[Framed-Interface-Id] *(identifiant d'interface tramée)*
[Framed-IP-Address] *(adresse IP tramée)*
* [Framed-IPv6-Prefix] *(préfixe IPv6 tramé)*
[Framed-IP-Netmask] *(réseau IP tramé)*

[Framed-MTU] *(MTU tramée)*
[Framed-Protocol] *(protocole tramé)*
[ARAP-Password] *(mot de passe ARAP)*
[ARAP-Security] (*sécurité ARAP)*
* [ARAP-Security-Data] *(données de sécurité ARAP)*
* [Login-IP-Host] *(hôte IP se connectant)*
* [Login-IPv6-Host] *(hôte IPv6 se connectant)*
[Login-LAT-Group] *(groupe LAT se connectant)*
[Login-LAT-Node] *(nœud LAT se connectant)*
[Login-LAT-Port] *(accès LAT se connectant)*
[Login-LAT-Service] *(service LAT se connectant)*
* [Tunneling] *(tunnelage)*
* [Proxy-Info] *(informations sur le mandataire)*
* [Route-Record] *(enregistrement de chemin)*
* [AVP]

3.2 Commande AA-Answer (AAA)

Le message AA-Answer (AAA) est indiqué par le réglage du champ Code de commande à 265 et en mettant à zéro le bit 'R' dans le champ Fanions de commande. Il est envoyé en réponse à un message AA-Request (AAR). Si l'autorisation a été demandée, une réponse de succès va inclure les AVP d'autorisation appropriées pour le service fourni, comme défini au paragraphe 4.4.

Pour les échanges d'authentification qui exigent plus d'un seul aller-retour, le serveur DOIT régler l'AVP Result-Code à DIAMETER_MULTI_ROUND_AUTH. *(authentification Diameter en plusieurs tours).*

Un message AAA avec ce code de résultat PEUT inclure un Reply-Message ou plus et PEUT inclure zéro ou une AVP State.

Si l'AVP Reply-Message était présente, le serveur d'accès réseau DEVRAIT envoyer le texte au client d'utilisateur pour l'afficher à l'utilisateur, en donnant pour instruction au client d'inviter l'utilisateur à répondre. Par exemple, cela peut être fait dans PPP via PAP. Si il est impossible de livrer le texte de l'invite à l'utilisateur, le client d'application NAS Diameter DOIT traiter le AA-Answer (AAA) avec l'AVP Reply-Message comme une erreur et refuser l'accès.

Format de message :

<AA-Answer> ::= < En-tête Diameter : 265, PXY >
< Session-Id >
{ Auth-Application-Id }
{ Auth-Request-Type }
{ Result-Code }
{ Origin-Host }
{ Origin-Realm }
[User-Name]
[Service-Type]
* [Class]
* [Configuration-Token] *(jeton de configuration)*
[Acct-Interim-Interval] *(intervalle de comptabilité intermédiaire)*
[Error-Message] *(message d'erreur)*
[Error-Reporting-Host] *(jeton de configuration)*
* [Failed-AVP]
[Idle-Timeout] *(temporisation d'inactivité)*
[Authorization-Lifetime]
[Auth-Grace-Period]
[Auth-Session-State]
[Re-Auth-Request-Type]
[Multi-Round-Time-Out]
[Session-Timeout]
[State]
* [Reply-Message]
[Origin-AAA-Protocol]
[Origin-State-Id]

```
* [ Filter-Id ]
  [ Password-Retry ]
  [ Port-Limit ]
  [ Prompt ]
  [ ARAP-Challenge-Response ]
  [ ARAP-Features ]
  [ ARAP-Security ]
* [ ARAP-Security-Data ]
  [ ARAP-Zone-Access ]
  [ 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 ]
* [ Login-IP-Host ]
* [ Login-IPv6-Host ]
  [ Login-LAT-Group ]
  [ Login-LAT-Node ]
  [ Login-LAT-Port ]
  [ Login-LAT-Service ]
  [ Login-Service ]
  [ Login-TCP-Port ]
* [ NAS-Filter-Rule ]
* [ QoS-Filter-Rule ]
* [ Tunneling ]
* [ Redirect-Host ]
  [ Redirect-Host-Usage ]
  [ Redirect-Max-Cache-Time ]
* [ Proxy-Info ]
* [ AVP ]
```

3.3 Commande Re-Auth-Request (RAR)

Un serveur Diameter peut initier la réauthentification et/ou réautorisation pour une certaine session en produisant un message Re-Auth-Request (RAR) [RFC6733].

Par exemple, pour des services prépayés, le serveur Diameter qui a à l'origine autorisé une session peut avoir besoin d'une confirmation que l'utilisateur utilise toujours le service.

Si un NAS reçoit un message RAR avec Session-Id égal à une session actuellement active et un Re-Auth-Type qui inclut l'authentification, il DOIT initier une réauthentification de l'utilisateur, si le service prend en charge cette caractéristique particulière.

Format de message :

```
<RA-Request>  ::= < En-tête Diameter : 258, REQ, PXY >
                  < Session-Id >
                  { Origin-Host }
                  { Origin-Realm }
```

```
                { Destination-Realm }
                { Destination-Host }
                { Auth-Application-Id }
                { Re-Auth-Request-Type }
                [ User-Name ]
                [ Origin-AAA-Protocol ]
                [ Origin-State-Id ]
                [ NAS-Identifier ]
                [ NAS-IP-Address ]
                [ NAS-IPv6-Address ]
                [ NAS-Port ]
                [ NAS-Port-Id ]
                [ NAS-Port-Type ]
                [ Service-Type ]
                [ Framed-IP-Address ]
                [ Framed-IPv6-Prefix ]
                [ Framed-Interface-Id ]
                [ Called-Station-Id ]
                [ Calling-Station-Id ]
                [ Originating-Line-Info ]
                [ Acct-Session-Id ]
                [ Acct-Multi-Session-Id ]
                [ State ]
              * [ Class ]
                [ Reply-Message ]
              * [ Proxy-Info ]
              * [ Route-Record ]
              * [ AVP ]
```

3.4 Commande Re-Auth-Answer (RAA)

Le message Re-Auth-Answer (RAA) [RFC6733] est envoyé en réponse à RAR. L'AVP Result-Code DOIT être présente et indique la disposition de la demande.

Une transaction RAA réussie DOIT être suivie par un message AAR.

Format de message :

```
<RA-Answer>  ::= < En-tête Diameter : 258, PXY >
                 < Session-Id >
                 { Result-Code }
                 { Origin-Host }
                 { Origin-Realm }
                 [ User-Name ]
                 [ Origin-AAA-Protocol ]
                 [ Origin-State-Id ]
                 [ Error-Message ]
                 [ Error-Reporting-Host ]
               * [ Failed-AVP ]
               * [ Redirected-Host ]
                 [ Redirected-Host-Usage ]
                 [ Redirected-Host-Cache-Time ]
                 [ Service-Type ]
               * [ Configuration-Token ]
                 [ Idle-Timeout ]
                 [ Authorization-Lifetime ]
                 [ Auth-Grace-Period ]
                 [ Re-Auth-Request-Type ]
                 [ State ]
               * [ Class ]
               * [ Reply-Message ]
                 [ Prompt ] (invite)
```

```
                * [ Proxy-Info ]
                * [ AVP ]
```

3.5 Commande Session-Termination-Request (STR)

Le message Session-Termination-Request (STR) [RFC6733] est envoyé par le NAS pour informer le serveur Diameter : qu'une session authentifiée et/ou autorisée se termine.

Format de message :

```
<ST-Request> ::= < En-tête Diameter : 275, REQ, PXY >
                 < Session-Id >
                 { Origin-Host }
                 { Origin-Realm }
                 { Destination-Realm }
                 { Auth-Application-Id }
                 { Termination-Cause }
                 [ User-Name ]
                 [ Destination-Host ]
                * [ Class ]
                 [ Origin-AAA-Protocol ]
                 [ Origin-State-Id ]
                * [ Proxy-Info ]
                * [ Route-Record ]
                * [ AVP ]
```

3.6 Commande Session-Termination-Answer (STA)

Le message Session-Termination-Answer (STA) [RFC6733] est envoyé par le serveur Diameter pour accuser réception de la notification qu'une session s'est terminée. L'AVP Result-Code DOIT être présente et PEUT contenir une indication qu'une erreur s'est produite pendant que le STR était en cours de traitement.

À l'envoi du STA, le serveur Diameter DOIT libérer toutes les ressources pour la session indiquée par l'AVP Session-Id. Tout serveur intermédiaire dans la chaîne de mandataires PEUT aussi libérer toutes les ressources, si nécessaire.

Format de message :

```
<ST-Answer>  ::= < En-tête Diameter : 275, PXY >
                 < Session-Id >
                 { Result-Code }
                 { Origin-Host }
                 { Origin-Realm }
                 [ User-Name ]
                * [ Class ]
                 [ Error-Message ]
                 [ Error-Reporting-Host ]
                * [ Failed-AVP ]
                 [ Origin-AAA-Protocol ]
                 [ Origin-State-Id ]
                * [ Redirect-Host ]
                 [ Redirect-Host-Usage ]
                 [ Redirect-Max-Cache-Time ]
                * [ Proxy-Info ]
                * [ AVP ]
```

3.7 Commande Abort-Session-Request (ASR)

Le message Abort-Session-Request (ASR) [RFC6733] peut être envoyé par tout serveur Diameter au NAS qui fournit le service de session pour demander que la session identifiée par ce Session-Id soit arrêtée.

Format de message :

<AS-Request> ::= < En-tête Diameter : 274, REQ, PXY >
< Session-Id >
{ Origin-Host }
{ Origin-Realm }
{ Destination-Realm }
{ Destination-Host }
{ Auth-Application-Id }
[User-Name]
[Origin-AAA-Protocol]
[Origin-State-Id]
[NAS-Identifier]
[NAS-IP-Address]
[NAS-IPv6-Address]
[NAS-Port]
[NAS-Port-Id]
[NAS-Port-Type]
[Service-Type]
[Framed-IP-Address]
[Framed-IPv6-Prefix]
[Framed-Interface-Id]
[Called-Station-Id]
[Calling-Station-Id]
[Originating-Line-Info]
[Acct-Session-Id]
[Acct-Multi-Session-Id]
[State]
* [Class]
* [Reply-Message]
* [Proxy-Info]
* [Route-Record]
* [AVP]

3.8 Commande Abort-Session-Answer (ASA)

Le message ASA [RFC6733] est envoyé en réponse à ASR. L'AVP Result-Code DOIT être présente et indique la disposition de la demande.

Si la session identifiée par l'identifiant de session dans l'ASR a été terminée avec succès, le code de résultat est réglé à DIAMETER_SUCCESS. Si la session n'est pas actuellement active, l'AVP Result-Code est réglée à DIAMETER_UNKNOWN_SESSION_ID. Si l'appareil d'accès n'arrête pas la session pour une autre raison, l'AVP Result-Code est réglée à DIAMETER_UNABLE_TO_COMPLY.

Format de message :
<AS-Answer> ::= < En-tête Diameter : 274, PXY >
< Session-Id >
{ Result-Code }
{ Origin-Host }
{ Origin-Realm }
[User-Name]
[Origin-AAA-Protocol]
[Origin-State-Id]
[State]
[Error-Message]
[Error-Reporting-Host]
* [Failed-AVP]
* [Redirected-Host] *(hôte de redirection)*
[Redirected-Host-Usage]
[Redirected-Max-Cache-Time]
* [Proxy-Info]
* [AVP]

3.9 Commande Accounting-Request (ACR)

Le message ACR [RFC6733] est envoyé par le NAS pour rapporter ses informations de session à un serveur cible en aval.

L'AVP Acct-Application-Id DOIT être présente.

Les AVP dont la liste figure dans la spécification du protocole Diameter de base [RFC6733] DOIVENT être supposées présentes, comme approprié. Les AVP de comptabilité spécifiques du service de NAS DEVRAIENT être présentes comme décrit au paragraphe 4.6 et dans le reste de la présente spécification.

Format de message :

<AC-Request> ::= < En-tête Diameter : 271, REQ, PXY >
< Session-Id >
{ Origin-Host }
{ Origin-Realm }
{ Destination-Realm }
{ Accounting-Record-Type } *(type d'enregistrement de comptabilité)*
{ Accounting-Record-Number } *(nombre d'enregistrements de comptabilité)*
{ Acct-Application-Id } *(identifiant d'application de comptabilité)*
[User-Name]
[Accounting-Sub-Session-Id] *(identifiant de sous session de comptabilité)*
[Acct-Session-Id]
[Acct-Multi-Session-Id]
[Origin-AAA-Protocol]
[Origin-State-Id]
[Destination-Host]
[Event-Timestamp] *(horodatage d'événement)*
[Acct-Delay-Time]
[NAS-Identifier]
[NAS-IP-Address]
[NAS-IPv6-Address]
[NAS-Port]
[NAS-Port-Id]
[NAS-Port-Type]
* [Class]
[Service-Type]
[Termination-Cause]
[Accounting-Input-Octets]
[Accounting-Input-Packets]
[Accounting-Output-Octets]
[Accounting-Output-Packets]
[Acct-Authentic]
[Accounting-Auth-Method]
[Acct-Link-Count]
[Acct-Session-Time]
[Acct-Tunnel-Connection]
[Acct-Tunnel-Packets-Lost]
[Callback-Id]
[Callback-Number]
[Called-Station-Id]
[Calling-Station-Id]
* [Connection-Info]
[Originating-Line-Info]
[Authorization-Lifetime]
[Session-Timeout]
[Idle-Timeout]
[Port-Limit]
[Accounting-Realtime-Required]
[Acct-Interim-Interval]
* [Filter-Id]
* [NAS-Filter-Rule]
* [QoS-Filter-Rule]
[Framed-Appletalk-Link]

```
                [ Framed-Appletalk-Network ]
                [ Framed-Appletalk-Zone ]
                [ Framed-Compression ]
                [ Framed-Interface-Id ]
                [ Framed-IP-Address ]
                [ Framed-IP-Netmask ]
               * [ Framed-IPv6-Prefix ]
                [ Framed-IPv6-Pool ]
               * [ Framed-IPv6-Route ]
                [ Framed-IPX-Network ]
                [ Framed-MTU ]
                [ Framed-Pool ]
                [ Framed-Protocol ]
               * [ Framed-Route ]
                [ Framed-Routing ]
               * [ Login-IP-Host ]
               * [ Login-IPv6-Host ]
                [ Login-LAT-Group ]
                [ Login-LAT-Node ]
                [ Login-LAT-Port ]
                [ Login-LAT-Service ]
                [ Login-Service ]
                [ Login-TCP-Port ]
               * [ Tunneling ]
               * [ Proxy-Info ]
               * [ Route-Record ]
               * [ AVP ]
```

3.10 Commande Accounting-Answer (ACA)

Le message ACA [RFC6733] est utilisé pour accuser réception d'une commande Accounting-Request. La commande Accounting-Answer contient le même identifiant de session que la demande.

Seul le serveur Diameter cible ou le serveur Diameter de rattachement DEVRAIT répondre avec la commande Accounting-Answer.

L'AVP Acct-Application-Id DOIT être présente.

Les AVP dont la liste figure dans la spécification du protocole Diameter de base [RFC6733] DOIVENT être supposées présentes, comme approprié. Les AVP de comptabilité spécifiques du service de NAS DEVRAIENT être présentes comme décrit au paragraphe 4.6 et dans le reste de la présente spécification.

Format de message :

```
<AC-Answer> ::= < En-tête Diameter : 271, PXY >
                < Session-Id >
                { Result-Code }
                { Origin-Host }
                { Origin-Realm }
                { Accounting-Record-Type }
                { Accounting-Record-Number }
                { Acct-Application-Id }
                [ User-Name ]
                [ Accounting-Sub-Session-Id ]
                [ Acct-Session-Id ]
                [ Acct-Multi-Session-Id ]
                [ Event-Timestamp ]
                [ Error-Message ]
                [ Error-Reporting-Host ]
               * [ Failed-AVP ]
                [ Origin-AAA-Protocol ]
                [ Origin-State-Id ]
                [ NAS-Identifier ]
```

[NAS-IP-Address]
[NAS-IPv6-Address]
[NAS-Port]
[NAS-Port-Id]
[NAS-Port-Type]
[Service-Type]
[Termination-Cause]
[Accounting-Realtime-Required]
[Acct-Interim-Interval]
* [Class]
* [Proxy-Info]
* [AVP]

4. AVP d'application de NAS Diameter

Les paragraphes qui suivent définissent un nouveau format de données d'AVP déduit, définissent un ensemble d'AVP spécifiques d'application, et décrivent l'utilisation des AVP définies dans d'autres documents par l'application de NAS Diameter.

4.1 Formats de données d'AVP déduits

4.1.1 QoSFilterRule

Le format QosFilterRule *(règle de filtre de qualité de service)* est dérivé du format de base d'AVP OctetString *(chaîne d'octet)*. Il utilise le jeu de caractères US-ASCII. Les paquets peuvent être marqués ou mesurés sur la base des informations suivantes :

- o Direction (entrante ou sortante)
- o Adresses IP de source et destination (éventuellement masquées)
- o Protocole
- o Accès de source et de destination (listes ou gammes)
- o Valeurs de codet de service différencié (DSCP, *Differentiated Services Code Point*) (pas de gamme ou gabarit)

Les règles pour la direction appropriée sont évaluées dans l'ordre; la première règle qui correspond termine l'évaluation. Chaque paquet est évalué une fois. Si aucune règle ne correspond, le paquet est traité au mieux. Un appareil d'accès qui n'est pas capable d'interpréter ou appliquer une règle de qualité de service (QS) NE DEVRAIT PAS terminer la session.

Les filtres QoSFilterRule DOIVENT respecter le format suivant : action dir proto de src à dst [options]
où :
action :
- tag : marque le paquet avec un DSCP spécifique [RFC2474]
- meter : mesure le trafic

dir : le format est comme décrit sous IPFilterRule [RFC6733]
proto : le format est comme décrit sous IPFilterRule [RFC6733]
src et dst : le format est comme décrit sous IPFilterRule [RFC6733]
Les options sont décrites au paragraphe 4.4.9.

La syntaxe de règle est un sous ensemble modifié de ipfw(8) provenant de FreeBSD, et le code ipfw.c peut fournir une base utile pour les mises en œuvre.

4.2 AVP de session de NAS

Diameter réserve les codes d'AVP 0 à 255 pour les attributs RADIUS qui sont mis en œuvre dans Diameter.

4.2.1 Information d'appel et de session

Ce paragraphe décrit les AVP spécifiques des applications Diameter qui sont nécessaires pour identifier le contexte d'appel et de session et les informations d'état. Sur une demande, ces informations permettent au serveur de qualifier la session.

Ces AVP sont utilisées en plus des AVP suivantes provenant de la spécification du protocole Diameter de base [RFC6733] :

Session-Id, Auth-Application-Id, Origin-Host, Origin-Realm, Auth-Request-Type, Termination-Cause
Le tableau suivant donne les valeurs de fanions possibles pour les AVP de niveau session. *(Voir au paragraphe 4.1 de la RFC6733 la signification de "M" et de "V".)*

		Règles de fanion d'AVP	
Nom d'attribut	**§**	**Doit**	**Ne doit pas**
NAS-Port	4.2.2	M	V
NAS-Port-Id	4.2.3	M	V
NAS-Port-Type	4.2.4	M	V
Called-Station-Id	4.2.5	M	V
Calling-Station-Id	4.2.6	M	V
Connect-Info	4.2.7	M	V
Originating-Line-Info	4.2.8	M	V
Reply-Message	4.2.9	M	V

4.2.2 AVP NAS-Port

L'AVP NAS-Port (code d'AVP 5) est du type Unsigned32 et contient le numéro d'accès physique ou virtuel du NAS, qui authentifie l'utilisateur. Noter que "accès" est pris dans le sens de connexion de service sur le NAS, non au sens d'un identifiant de protocole IP ; donc, le format et le contenu de la chaîne qui identifie l'accès sont spécifiques de la mise en œuvre de NAS.

L'AVP NAS-Port ou l'AVP NAS-Port-Id (paragraphe 4.2.3) DEVRAIT être présente dans la commande AA-Request (AAR) (paragraphe 3.1) si le NAS différencie ses accès.

4.2.3 AVP NAS-Port-Id

L'AVP NAS-Port-Id (code d'AVP 87) est du type UTF8String et consiste en 7 bits de texte US-ASCII identifiant l'accès du NAS qui authentifie l'utilisateur. Noter que "accès" est pris dans le sens de connexion de service sur le NAS, non au sens d'un identifiant de protocole IP.

L'AVP NAS-Port-Id ou l'AVP NAS-Port AVP (paragraphe 4.2.2) DEVRAIT être présente dans la commande AA-Request (AAR) (paragraphe 3.1) si le NAS différencie ses accès . NAS-Port-Id est destinée à être utilisée par les NAS qui ne peuvent pas numéroter facilement leurs accès.

4.2.4 AVP NAS-Port-Type

L'AVP NAS-Port-Type (code d'AVP 61) est du type Enumerated et contient le type de l'accès sur lequel le NAS authentifie l'utilisateur. Cette AVP DEVRAIT être présente si le NAS utilise concurremment les mêmes gammes de numéro d'accès de NAS pour les différents types de service.

La liste des valeurs actuellement acceptées de l'AVP NAS-Port-Type figure dans [RADIUS-ATT].

4.2.5 AVP Called-Station-Id

L'AVP Called-Station-Id (code d'AVP 30) est du type UTF8String et contient une chaîne de 7 bits en US-ASCII envoyée par le NAS pour décrire l'adresse de couche 2 de l'utilisateur contacté dans la demande. Pour un accès commuté, ce peut être un numéro de téléphone obtenu en utilisant le service d'identification du numéro composé (DNIS, *Dialed Number Identification Service*) ou une technologie similaire. Noter que ceci peut être différent du numéro de téléphone sur lequel est venu l'appel. Pour l'utilisation avec un accès IEEE 802, l'AVP Called-Station-Id PEUT contenir une adresse de contrôle de support d'accès (MAC, *Media Access Control*) formatée comme décrit dans la [RFC3580].

Si l'AVP Called-Station-Id est présente dans un message AAR, l'AVP Auth-Request-Type est réglée à AUTHORIZE_ONLY, et si l'AVP User-Name est absente, le serveur Diameter PEUT effectuer l'autorisation sur la base de cette AVP. Cela peut être utilisé par un NAS pour demander si il devrait répondre à un appel sur la base du résultat DNIS.

La codification du contenu permis pour ce champ et son usage sortent du domaine d'application de cette spécification.

4.2.6 AVP Calling-Station-Id

L'AVP Calling-Station-Id (code d'AVP 31) est du type UTF8String et contient une chaîne de 7 bits en US-ASCII envoyée par le NAS pour décrire l'adresse de couche 2 à partir de laquelle l'utilisateur a connecté la demande. Pour un accès commuté, c'est le numéro de téléphone d'où vient l'appel, en utilisant l'identification automatique du numéro (ANI, *Automatic Number Identification*) ou une technologie similaire. Pour l'utilisation avec un accès IEEE 802, l'AVP Calling-Station-Id PEUT contenir une adresse MAC, formatée comme décrit dans la RFC 3580.

Si l'AVP Calling-Station-Id est présente dans un message AAR, l'AVP Auth-Request-Type réglée à AUTHORIZE_ONLY, et l'AVP User-Name absente, le serveur Diameter PEUT effectuer l'autorisation sur la base de la valeur de cette AVP. Ceci peut être utilisé par un NAS pour demander si on devrait répondre à un appel sur la base de l'adresse de couche 2 (ANI, adresse MAC, etc.).

La codification du contenu admis pour ce champ et son utilisation sortent du domaine d'application de cette spécification.

4.2.7 AVP Connect-Info

L'AVP Connect-Info (code d'AVP 77) est du type UTF8String et est envoyée dans le message AA-Request ou un message ACR avec la valeur de l'AVP Accounting-Record-Type réglée à STOP. Lorsque envoyée dans AA-Request, elle indique la nature de la connexion de l'utilisateur. La vitesse de connexion DEVRAIT être incluse au début de la première AVP Connect-Info dans le message. Si les vitesses des connexions d'émission et de réception diffèrent, elles peuvent être incluses toutes les deux dans la première AVP avec la vitesse d'émission (la vitesse de transmission du modem du NAS) figurant en premier, puis une barre oblique (/), puis la vitesse de réception, et ensuite les autres informations facultatives.

Par exemple : "28800 V42BIS/LAPM" ou "52000/31200 V90"

Si elle est envoyée dans un message ACR avec la valeur de l'AVP Accounting-Record-Type réglée à STOP, cet attribut peut reprendre des statistiques relatives à la qualité de la session. Par exemple, dans IEEE 802.11, l'AVP Connect-Info peut contenir des informations sur le nombre de retransmissions de couche liaison. Le format exact de cet attribut est spécifique de la mise en œuvre.

4.2.8 AVP Originating-Line-Info

L'AVP Originating-Line-Info (code d'AVP 94) est du type OctetString et est envoyée par le système de NAS pour convoyer les informations sur l'origine de l'appel provenant du système de signalisation n° 7 (SS7).

L'élément Informations de ligne génératrice (OLI, *Originating Line Information*) indique la nature et/ou les caractéristiques de la ligne d'où l'appel a son origine (par exemple, une cabine, un hôtel, un téléphone cellulaire). Les compagnies de téléphone commencent à offrir OLI à leurs clients comme option sur le service principal. Les fournisseurs d'accès Internet (FAI) peuvent utiliser OLI en plus des attributs Called-Station-Id et Calling-Station-Id pour différencier les appels des abonnés et pour définir des services différents.

Le champ Valeur contient deux octets (00 - 99). ANSI T1.113 et BELLCORE 394 peuvent être utilisés pour des informations supplémentaires sur ces valeurs et leur utilisation. Pour des informations sur les valeurs actuellement allouées, voir [ANITypes].

4.2.9 AVP Reply-Message

L'AVP Reply-Message (code d'AVP 18) est du type UTF8String et contient un texte qui PEUT être affiché à l'utilisateur. Lorsque utilisée dans un message AA-Answer avec une AVP Result-Code de succès, elle indique le succès. Lorsque elle se trouve dans un message AAA avec un Result-Code autre que DIAMETER_SUCCESS, l'AVP contient un message d'échec.

L'AVP Reply-Message PEUT contenir un texte pour inviter l'utilisateur a faire une autre tentative de AA-Request. Lorsque utilisée dans un message AA-Answer contenant une AVP Result-Code avec la valeur DIAMETER_MULTI_ROUND_AUTH ou dans un message Re-Auth-Request, elle PEUT contenir un texte invitant l'utilisateur à une réponse.

4.3 AVP d'authentification de NAS

Cette section définit les AVP nécessaires pour porter les informations d'authentification dans le protocole Diameter. La fonctionnalité définie ici fournit un service d'authentification, autorisation, et comptabilité de style RADIUS [RFC2865] sur un transport plus fiable et sûr, comme défini dans le protocole Diameter de base [RFC6733].

Le tableau suivant donne les valeurs de fanions possibles pour les AVP de niveau session.

		Règles de fanion d'AVP	
Nom d'attribut	**§**	**Doit**	**Ne doit pas**
User-Password	4.3.1	M	V
Password-Retry	4.3.2	M	V
Prompt	4.3.3	M	V
CHAP-Auth	4.3.4	M	V
CHAP-Algorithm	4.3.5	M	V
CHAP-Ident	4.3.6	M	V
CHAP-Response	4.3.7	M	V
CHAP-Challenge	4.3.8	M	V
ARAP-Password	4.3.9	M	V
ARAP-Challenge-Response	4.3.10	M	V
ARAP-Security	4.3.11	M	V
ARAP-Security-Data	4.3.12	M	V

4.3.1 AVP User-Password

L'AVP User-Password (code d'AVP 2) est du type OctetString et contient le mot de passe de l'utilisateur à authentifier ou l'entrée de l'utilisateur dans un échange d'authentification à plusieurs tours.

L'AVP User-Password contient un mot de passe d'utilisateur ou un mot de passe à utilisation unique et donc représente des informations sensibles. Comme exigé par le protocole Diameter de base [RFC6733], les messages Diameter sont chiffrés en utilisant IPsec [RFC4301] ou la sécurité de couche transport (TLS, *Transport Layer Security*) [RFC5246]. Sauf si cette AVP est utilisée pour des mots de passe à utilisation unique, l'AVP User-Password NE DEVRAIT PAS être utilisée dans des environnements de mandataires non de confiance sans la chiffrer en utilisant des techniques de sécurité de bout en bout.

Le mot de passe en clair (avant le chiffrement) NE DOIT PAS faire plus de 128 octets.

4.3.2 AVP Password-Retry

L'AVP Password-Retry (code d'AVP 75) est du type Unsigned32 et PEUT être incluse dans le message AA-Answer si le code de résultat indique un échec d'authentification. La valeur de cette AVP indique combien de tentatives d'authentification sont permises à un utilisateur avant d'être déconnecté. Cette AVP est principalement destinée à être utilisée lorsque l'AVP Framed-Protocol (paragraphe 4.4.10.1) est réglée à ARAP.

4.3.3 AVP Prompt

L'AVP Prompt (code d'AVP 76) est du type Enumerated et PEUT être présente dans le message AA-Answer. Lorsque présente, elle est utilisée par le NAS pour déterminer si il devrait être fait écho à la réponse de l'utilisateur, lorsque elle est entrée. Les valeurs acceptées figurent dans [RADIUS-ATT].

4.3.4 AVP CHAP-Auth

L'AVP CHAP-Auth (code d'AVP 402) est du type Grouped et contient les informations nécessaires pour authentifier un utilisateur qui utilise le protocole PPP d'authentification par dialogue à énigmes (CHAP) [RFC1994]. Si l'AVP CHAP-Auth se trouve dans un message, l'AVP CHAP-Challenge (paragraphe 4.3.8) DOIT être présente aussi. Les AVP facultatives qui contiennent la réponse CHAP dépendent de la valeur de l'AVP CHAP-Algorithm (paragraphe 4.3.8). L'AVP groupée a la grammaire ABNF [RFC5234] suivante :

```
CHAP-Auth  ::= < En-tête d'AVP : 402 >
               { CHAP-Algorithm }
               { CHAP-Ident }
               [ CHAP-Response ]
             * [ AVP ]
```

4.3.5 AVP CHAP-Algorithm

L'AVP CHAP-Algorithm (code d'AVP 403) est du type Enumerated et contient l'identifiant d'algorithme utilisé pour le

calcul de la réponse CHAP [RFC1994]. Les valeurs suivantes sont actuellement acceptées : CHAP avec MD5 : 5
La réponse CHAP est calculée en utilisant la procédure décrite dans la [RFC1994]. Cet algorithme exige que l'AVP CHAP-Response (paragraphe 4.3.7) soit présente dans l'AVP CHAP-Auth (paragraphe 4.3.4).

4.3.6 AVP CHAP-Ident

L'AVP CHAP-Ident (code d'AVP 404) est du type OctetString et contient l'identifiant CHAP de un octet utilisé pour le calcul de la réponse CHAP [RFC1994].

4.3.7 AVP CHAP-Response

L'AVP CHAP-Response (code d'AVP 405) est du type OctetString et contient les 16 octets de données d'authentification fournies par l'utilisateur dans la réponse au défi CHAP [RFC1994].

4.3.8 AVP CHAP-Challenge

L'AVP CHAP-Challenge (code d'AVP 60) est du type OctetString et contient le défi CHAP envoyé par le NAS à l'homologue CHAP [RFC1994].

4.3.9 ARAP-Password

L'AVP ARAP-Password (code d'AVP 70) est du type OctetString et n'est présente que lorsque l'AVP Framed-Protocol (paragraphe 4.4.10.1) est incluse dans le message et est réglée à ARAP. Cette AVP NE DOIT PAS être présente si l'AVP User-Password ou l'AVP CHAP-Auth est présente. Voir dans la [RFC2869] plus d'informations sur le contenu de cette AVP.

4.3.10 AVP ARAP-Challenge-Response

L'AVP ARAP-Challenge-Response (code d'AVP 84) est du type OctetString et n'est présente que lorsque l'AVP Framed-Protocol (paragraphe 4.4.10.1) est incluse dans le message et est réglée à ARAP. Cette AVP contient une réponse de 8 octets au défi du client appelant. Le serveur Diameter calcule cette valeur en prenant le défi du client appelant à partir des 8 octets de poids fort de l'AVP ARAP-Password et en effectuant le chiffrement DES sur cette valeur avec comme clé le mot de passe de l'utilisateur qui s'authentifie. Si le mot de passe de l'utilisateur fait moins de 8 octets, le mot de passe est bourré à la fin avec des octets NUL jusqu'à ce qu'il en fasse 8 avant de l'utiliser comme clé.

4.3.11 AVP ARAP-Security

L'AVP ARAP-Security (code d'AVP 73) est du type Unsigned32 et PEUT être présente dans le message AA-Answer si l'AVP Framed-Protocol (paragraphe 4.4.10.1) est réglée à la valeur de ARAP, et l'AVP Result-Code ([RFC6733], paragraphe 7.1) est réglée à DIAMETER_MULTI_ROUND_AUTH. Voir la RFC 2869 pour plus d'informations sur le contenu de cette AVP.

4.3.12 AVP ARAP-Security-Data

L'AVP ARAP-Security-Data (code d'AVP 74) est du type OctetString et PEUT être présente dans le message AA-Request ou AA-Answer si l'AVP Framed-Protocol (paragraphe 4.4.10.1) est réglée à la valeur de ARAP et l'AVP Result-Code ([RFC6733], paragraphe 7.1) est réglée à DIAMETER_MULTI_ROUND_AUTH. Cette AVP contient le défi ou la réponse du module de sécurité associé au module de sécurité ARAP spécifié dans l'AVP ARAP-Security (paragraphe 4.3.11).

4.4 AVP d'autorisation de NAS

Ce paragraphe contient les AVP d'autorisation prises en charge dans l'application de NAS. L'AVP Service-Type DEVRAIT être présente dans tous les messages et, sur la base de sa valeur, des AVP supplémentaires définies dans ce paragraphe et au paragraphe 4.5 PEUVENT être présentes.

Le tableau suivant donne les valeurs de fanions possibles pour les AVP de niveau session.

		Règles de fanion d'AVP	
Nom d'attribut	**§**	**Doit**	**Ne doit pas**
Service-Type	4.4.1	M	V
Callback-Number	4.4.2	M	V
Callback-Id	4.4.3	M	V
Idle-Timeout	4.4.4	M	V
Port-Limit	4.4.5	M	V
NAS-Filter-Rule	4.4.6	M	V
Filter-Id	4.4.7	M	V
Configuration-Token	4.4.8	M	V
QoS-Filter-Rule	4.4.9		
Framed-Protocol	4.4.10.1	M	V
Framed-Routing	4.4.10.2	M	V
Framed-MTU	4.4.10.3	M	V
Framed-Compression	4.4.10.4	M	V
Framed-IP-Address	4.4.10.5.1	M	V
Framed-IP-Netmask	4.4.10.5.2	M	V
Framed-Route	4.4.10.5.3	M	V
Framed-Pool	4.4.10.5.4	M	V
Framed-Interface-Id	4.4.10.5.5	M	V
Framed-IPv6-Prefix	4.4.10.5.6	M	V
Framed-IPv6-Route	4.4.10.5.7	M	V
Framed-IPv6-Pool	4.4.10.5.8	M	V
Framed-IPX-Network	4.4.10.6.1	M	V
Framed-Appletalk-Link	4.4.10.7.1	M	V
Framed-Appletalk-Network	4.4.10.7.2	M	V
Framed-Appletalk-Zone	4.4.10.7.3	M	V
ARAP-Features	4.4.10.8.1	M	V
ARAP-Zone-Access	4.4.10.8.2	M	V
Login-IP-Host	4.4.11.1	M	V
Login-IPv6-Host	4.4.11.2	M	V
Login-Service	4.4.11.3	M	V
Login-TCP-Port	4.4.11.4.1	M	V
Login-LAT-Service	4.4.11.5.1	M	V
Login-LAT-Node	4.4.11.5.2	M	V
Login-LAT-Group	4.4.11.5.3	M	V
Login-LAT-Port	4.4.11.5.4	M	V

4.4.1 AVP Service-Type

L'AVP Service-Type (code d'AVP 6) est du type Enumerated et contient le type de service que l'utilisateur a demandé ou le type de service à fournir. Une telle AVP PEUT être présente dans une demande ou réponse d'authentification et/ou d'autorisation. Un NAS n'est pas obligé de mettre en œuvre tous ces types de services. Il DOIT traiter les AVP Service-Type inconnues ou non prises en charge reçues dans une réponse comme un échec et terminer la session avec un code de résultat DIAMETER_INVALID_AVP_VALUE.

Lorsque utilisée dans une demande, l'AVP Service-Type DEVRAIT être considérée comme une indication au serveur que le NAS pense que l'utilisateur préfèrerait le type de service indiqué. Le serveur n'est pas obligé de respecter ce conseil. De plus, si le service spécifié par le serveur est pris en charge, mais non compatible avec le mode d'accès actuel, le NAS DOIT refuser de commencer la session. Le NAS DOIT aussi générer le ou les messages d'erreur appropriés.

La liste complète des valeurs définies que l'AVP Service-Type peut prendre se trouve dans la [RFC2865] et le registre IANA pertinent [RADIUS-ATT], mais les valeurs suivantes doivent être plus qualifiés ici :

Login (1) : l'usager devrait être connecté à un hôte. Le message PEUT inclure des AVP supplémentaires comme défini aux paragraphes 4.4.11.4 ou 4.4.11.5.

Framed (2) : un protocole tramé, comme PPP ou SLIP, devrait être lancé pour l'utilisateur. Le message PEUT inclure des AVP supplémentaires définies aux paragraphes 4.4.10 ou 4.5 pour des services de tunnelage.

Callback Login (3) : l'utilisateur devrait être déconnecté et rappelé, puis connecté à un hôte. Le message PEUT inclure des AVP supplémentaires définies dans cette section.

Callback Framed (4) : l'utilisateur devrait être déconnecté et rappelé, et ensuite un protocole tramé, comme PPP ou SLIP, devrait être lancé pour l'utilisateur. Le message PEUT inclure des AVP supplémentaires définies aux paragraphes 4.4.10 ou 4.5 pour les services de tunnelage.

4.4.2 AVP Callback-Number

L'AVP Callback-Number (code d'AVP 19) est du type UTF8String et contient une chaîne de numérotation à utiliser pour le rappel, dont le format est spécifique du déploiement. L'AVP Callback-Number PEUT être utilisée dans une demande d'authentification et/ou autorisation comme indication au serveur qu'un service de rappel est désiré, mais le serveur n'est pas obligé de respecter le conseil dans la réponse correspondante.

La codification de la gamme d'usage permise pour ce champ sort du domaine d'application de la présente spécification.

4.4.3 AVP Callback-Id

L'AVP Callback-Id (code d'AVP 20) est du type UTF8String et contient le nom d'un endroit à appeler, à interpréter par le NAS. Cette AVP PEUT être présente dans une réponse d'authentification et/ou autorisation.

Cette AVP n'est pas destinée à l'itinérance car elle suppose que l'identifiant de rappel est configuré sur le NAS. L'utilisation de l'AVP Callback-Number (paragraphe 4.4.2) est donc RECOMMANDÉE.

4.4.4 AVP Idle-Timeout

L'AVP Idle-Timeout (code d'AVP 28) est du type Unsigned32 et règle le nombre maximum de secondes consécutives d'inactivité de la connexion permis à l'utilisateur avant la terminaison de la session ou avant la production d'une invite. Sa valeur par défaut est "aucune" ou spécifique du système.

4.4.5 AVP Port-Limit

L'AVP Port-Limit (code d'AVP 62) est du type Unsigned32 et règle le nombre maximum d'accès que le NAS fournit à l'utilisateur. Elle PEUT être utilisée dans une demande d'authentification et/ou autorisation comme indication au serveur qu'un service PPP multi liaisons [RFC1990] est désiré, mais le serveur n'est pas obligé de respecter ce conseil dans la réponse correspondante.

4.4.6 AVP NAS-Filter-Rule

L'AVP NAS-Filter-Rule (code d'AVP 400) est du type IPFilterRule et fournit des règles de filtre qui doivent être configurées sur le NAS pour l'utilisateur. Une ou plusieurs de ces AVP PEUVENT être présentes dans une réponse d'autorisation.

4.4.7 AVP Filter-Id

L'AVP Filter-Id (code d'AVP 11) est du type UTF8String et contient le nom de la liste des filtres pour cet usager. Elle est destinée à être lisible pour l'homme. Zéro, une ou plusieurs AVP Filter-Id PEUVENT être envoyées dans un message de réponse d'autorisation.

Identifier une liste de filtres par le nom permet que les filtres soient utilisés sur différents NAS sans égard aux détails de la mise en œuvre de la liste de filtres. Cependant, cette AVP n'est pas favorable à l'itinérance car la dénomination des filtres diffère d'un fournisseur de service à l'autre.

Dans les environnements où la rétro compatibilité avec RADIUS n'est pas exigée, il est RECOMMANDÉ que l'AVP NAS-Filter-Rule (paragraphe 4.4.6) soit utilisée à la place.

4.4.8 AVP Configuration-Token

L'AVP Configuration-Token (code d'AVP 78) est du type OctetString et est envoyée par un serveur Diameter à un agent mandataire Diameter dans une commande AA-Answer pour indiquer un type de profil d'utilisateur à utiliser. Elle ne devrait pas être envoyée à un client Diameter (NAS).

Le format du champ Données de cette AVP est spécifique du site.

4.4.9 AVP QoS-Filter-Rule

L'AVP QoS-Filter-Rule (code d'AVP 407) est du type QoSFilterRule (paragraphe 4.1.1) et fournit des règles de filtre de QS qui doivent être configurées sur le NAS pour l'utilisateur. Une ou plusieurs de ces AVP PEUVENT être présentes dans une réponse d'autorisation.

L'utilisation de cette AVP N'EST PAS RECOMMANDÉE ; les AVP définies par la [RFC5777] DEVRAIENT être utilisées à la place.

Les options suivantes sont définies pour les filtres QoSFilterRule :

DSCP <color> : si action est réglé à étiquette (paragraphe 4.1.1), cette option DOIT être incluse dans la règle.

Les valeurs de "Color" sont définies dans la [RFC2474]. La correspondance exacte des valeurs de DSCP est requise (pas de gabarits ou de gammes).

metering <rate> <color_under> <color_over>

L'option "metering" fournit une transmission assurée, comme défini dans la [RFC2597] et DOIT être présente si l'action est réglée à "meter" (paragraphe 4.1.1). L'option "rate" est le débit, en bits par seconde, utilisé par l'appareil d'accès pour marquer les paquets. Le trafic sur le débit est marqué avec le codet color_over, et le trafic sous le débit est marqué avec le codet color_under. Les options color_under et color_over contiennent les préférences d'abandon et DOIVENT se conformer aux mots clés de codets recommandés décrits dans la [RFC2597] (par exemple, AF13).

L'option "metering" prend aussi en charge la limite stricte sur le trafic requise par la transmission expédiée, comme défini dans la [RFC3246]. L'option color_over peut contenir le mot clé "drop" pour empêcher la transmission du trafic qui excède le paramètre "rate".

4.4.10 AVP d'autorisation d'accès tramé

Ce paragraphe fait la liste des AVP d'autorisation nécessaires pour la prise en charge de l'accès tramé, comme PPP et SLIP. Les AVP définies dans ce paragraphe PEUVENT être présentes dans un message si l'AVP Service-Type a été réglée à "Framed" ou "Callback Framed".

4.4.10.1 AVP Framed-Protocol

L'AVP Framed-Protocol (code d'AVP 7) est du type Enumerated et contient le tramage à utiliser pour l'accès tramé. Cette AVP PEUT être présente dans les demandes et les réponses. La liste des valeurs acceptées figure dans [RADIUS-ATT].

4.4.10.2 AVP Framed-Routing

L'AVP Framed-Routing (code d'AVP 10) est du type Enumerated et contient la méthode d'acheminement pour l'utilisateur lorsque l'utilisateur est un routeur pour un réseau. Cette AVP DEVRAIT n'être présente que dans les réponses d'autorisation. La liste des valeurs acceptées figure dans [RADIUS-ATT].

4.4.10.3 AVP Framed-MTU

L'AVP Framed-MTU (code d'AVP 12) est du type Unsigned32 et contient l'unité de transmission maximum (MTU, *Maximum Transmission Unit*) à configurer pour l'utilisateur, quand elle n'est pas négociée par d'autres moyens (comme PPP). Cette AVP DEVRAIT n'être présente que dans les réponses d'autorisation. La valeur de MTU DOIT être dans la gamme de 64 à 65535.

4.4.10.4 AVP AVP Framed-Compression

L'AVP Framed-Compression (code d'AVP 13) est du type Enumerated et contient le protocole de compression à utiliser pour la liaison. Elle PEUT être utilisée dans une demande d'autorisation comme indication au serveur qu'un type spécifique de compression est désiré, mais le serveur n'est pas obligé de suivre ce conseil dans la réponse correspondante.

Plus d'une AVP de protocole de compression PEUT être envoyée. Le NAS est responsable de l'application du bon protocole de compression au trafic de liaison approprié.

La liste des valeurs acceptées figure dans [RADIUS-ATT].

4.4.10.5 AVP d'autorisation d'accès IP

Les AVP définies dans ce paragraphe sont utilisées lorsque l'utilisateur demande le service d'accès à IP ou qu'il lui est accordé.

4.4.10.5.1 AVP Framed-IP-Address

L'AVP Framed-IP-Address (code d'AVP 8) [RFC2865] est du type OctetString et contient une adresse IPv4 du type spécifié dans la valeur d'attribut à configurer pour l'utilisateur. Elle PEUT être utilisée dans une demande d'autorisation comme indication au serveur qu'une adresse spécifique est désirée, mais le serveur n'est pas obligé de suivre ce conseil dans la réponse correspondante.

Deux valeurs ont une signification particulière : 0xFFFFFFFF et 0xFFFFFFFE. La valeur 0xFFFFFFFF indique que le NAS devrait permettre à l'utilisateur de choisir une adresse (c'est-à-dire, de la négocier). La valeur 0xFFFFFFFE indique que le NAS devrait choisir une adresse pour l'utilisateur (par exemple, allouée dans un réservoir d'adresses conservé par le NAS).

4.4.10.5.2 AVP Framed-IP-Netmask

L'AVP Framed-IP-Netmask (code d'AVP 9) est du type OctetString et contient les quatre octets du gabarit de réseau IPv4 à configurer pour l'utilisateur lorsque l'utilisateur est un routeur pour un réseau. Elle PEUT être utilisée dans une demande d'autorisation comme indication au serveur qu'un gabarit de réseau spécifique est désiré, mais le serveur n'est pas obligé de suivre ce conseil dans la réponse correspondante. Cette AVP DOIT être présente dans une réponse si la demande incluait cette AVP avec une valeur de 0xFFFFFFFF.

4.4.10.5.3 AVP Framed-Route

L'AVP Framed-Route (code d'AVP 22) est du type UTF8String et contient les 7 bits d'informations d'acheminement en US-ASCII à configurer pour l'utilisateur sur le NAS. Zéro, une ou plusieurs de ces AVP PEUVENT être présentes dans une réponse d'autorisation.

La chaîne DOIT contenir un préfixe de destination en forme quadratique séparée par des points, facultativement suivie par une barre oblique et un spécificateur de longueur décimal déclarant combien de bits de poids fort du préfixe devraient être utilisés. Ceci est suivi d'une espace, d'une adresse de passerelle en forme quadratique séparée par des points, une espace, et une ou plusieurs métriques séparées par des espaces ; par exemple, "192.0.2.0/24 192.0.2.1 1"

Le spécificateur de longueur peut être omis, et dans ce cas il devrait être par défaut de 8 bits pour les préfixes de classe A, de 16 bits pour les préfixes de classe B, et de 24 bits pour les préfixes de classe C ; par exemple, "192.0.2.0 192.0.2.1 1"

Chaque fois que l'adresse de passerelle est spécifiée comme "0.0.0.0", l'adresse IP de l'utilisateur DEVRAIT être utilisée comme adresse de passerelle.

4.4.10.5.4 AVP Framed-Pool

L'AVP Framed-Pool (code d'AVP 88) est du type OctetString et contient le nom d'un réservoir d'adresses allouées qui DEVRAIT être utilisé pour allouer une adresse pour l'utilisateur. Si un NAS ne prend pas en charge les réservoirs de plusieurs adresses, le NAS DEVRAIT ignorer cette AVP. 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.

Bien que spécifié comme type OctetString pour la compatibilité avec RADIUS [RFC2869], le codage du champ Données DEVRAIT aussi se conformer aux règles pour le format de données UTF8String.

4.4.10.5.5 AVP Framed-Interface-Id

L'AVP Framed-Interface-Id (code d'AVP 96) est du type Unsigned64 et contient l'identifiant d'interface IPv6 à configurer pour l'utilisateur. Elle PEUT être utilisée dans des demandes d'autorisation comme indication au serveur qu'un identifiant d'interface spécifique est désiré, mais le serveur n'est pas obligé de suivre ce conseil dans la réponse correspondante.

4.4.10.5.6 AVP Framed-IPv6-Prefix

L'AVP Framed-IPv6-Prefix (code d'AVP 97) est du type OctetString et contient le préfixe IPv6 à configurer pour l'utilisateur. Une ou plusieurs AVP PEUVENT être utilisées dans les demandes d'autorisation comme indication au serveur que des préfixes IPv6 spécifiques sont désirés, mais le serveur n'est pas obligé de suivre ce conseil dans la réponse correspondante.

4.4.10.5.7 AVP Framed-IPv6-Route

L'AVP Framed-IPv6-Route (code d'AVP 99) est du type UTF8String et contient les informations d'acheminement en US-ASCII à configurer pour l'utilisateur sur le NAS. Zéro, une ou plusieurs de ces AVP PEUVENT être présentes dans une réponse d'autorisation.

La chaîne DOIT contenir un préfixe d'adresse IPv6 suivi par une barre oblique et un spécificateur de longueur décimal déclarant combien de bits de poids fort du préfixe devraient être utilisés. Ceci est suivi par une espace, une adresse de passerelle en notation hexadécimale, une espace, et une ou plusieurs métriques séparées par des espaces ; par exemple, "2001:db8::/32 2001:db8:106:a00:20ff:fe99:a998 1"

Chaque fois que l'adresse de passerelle est l'adresse IPv6 inspécifiée, l'adresse IP de l'utilisateur DEVRAIT être utilisée comme adresse de passerelle, comme dans : "2001:db8::/32 :: 1"

4.4.10.5.8 AVP Framed-IPv6-Pool

L'AVP Framed-IPv6-Pool (code d'AVP 100) est du type OctetString et contient le nom d'un réservoir alloué qui DEVRAIT être utilisé pour allouer un préfixe IPv6 pour l'utilisateur. Si l'appareil d'accès ne prend pas en charge les réservoirs de préfixes multiples, il DOIT ignorer cette AVP.

Bien que spécifié comme type OctetString pour la compatibilité avec RADIUS [RFC3162], le codage du champ Data DEVRAIT aussi se conformer aux règles sur le format Data UTF8String.

4.4.10.6 AVP d'accès IPX

Les AVP définies dans ce paragraphe sont utilisés lorsque l'utilisateur demande l'accès, ou qu'il est accordé, au service réseau IPX [IPX].

4.4.10.6.1 AVP Framed-IPX-Network

L'AVP Framed-IPX-Network (code d'AVP 23) est du type Unsigned32 et contient le numéro de réseau IPX à configurer pour l'utilisateur. Elle PEUT être utilisée dans une demande d'autorisation comme indication au serveur qu'une adresse spécifique est désirée, mais le serveur n'est pas obligé de suivre ce conseil dans la réponse correspondante.

Deux adresses ont une signification particulière : 0xFFFFFFFF et 0xFFFFFFFE. La valeur 0xFFFFFFFF indique que le NAS devrait permettre à l'utilisateur de choisir une adresse (c'est-à-dire, la négocier). La valeur 0xFFFFFFFE indique que le NAS devrait choisir une adresse pour l'utilisateur (par exemple, l'allouer à partir d'un réservoir d'un ou plusieurs réseaux IPX conservé par le NAS).

4.4.10.7 AVP d'accès réseau AppleTalk

Les AVP définies dans ce paragraphe sont utilisées lorsque l'utilisateur demande l'accès, ou qu'il est accordé, au service réseau AppleTalk [AppleTalk].

4.4.10.7.1 AVP Framed-Appletalk-Link

L'AVP Framed-Appletalk-Link (code d'AVP 37) est du type Unsigned32 et contient le numéro de réseau AppleTalk qui devrait être utilisé pour la liaison série pour l'utilisateur, qui est un autre routeur AppleTalk. Cette AVP DOIT seulement être présente dans une réponse d'autorisation et n'est jamais utilisée lorsque l'utilisateur n'est pas un autre routeur.

En dépit de la taille du champ, les valeurs vont de 0 à 65 535. La valeur spéciale de 0 indique une liaison série non numérotée. Une valeur de 1 à 65 535 signifie que la liaison série entre le NAS et l'utilisateur devrait recevoir cette valeur comme numéro de réseau AppleTalk.

4.4.10.7.2 AVP Framed-Appletalk-Network

L'AVP Framed-Appletalk-Network (code d'AVP 38) est du type Unsigned32 et contient le numéro de réseau AppleTalk que le NAS devrait sonder pour allouer un nœud AppleTalk pour l'utilisateur. Cette AVP DOIT être présente seulement dans une réponse d'autorisation et n'est utilisée que si l'utilisateur est un autre routeur. Plusieurs instances de cette AVP indiquent que le NAS peut sonder, en utilisant n'importe lequel des numéros de réseau spécifiés.

En dépit de la taille du champ, les valeurs vont de 0 à 65 535. La valeur spéciale de 0 indique que le NAS devrait allouer un réseau à l'utilisateur, en utilisant sa gamme de câbles par défaut. Une valeur entre 1 et 65 535 (inclus) indique au réseau AppleTalk que le NAS devrait sonder pour trouver une adresse pour l'utilisateur.

4.4.10.7.3 AVP Framed-Appletalk-Zone

L'AVP Framed-Appletalk-Zone (code d'AVP 39) est du type OctetString et contient la zone AppleTalk par défaut à utiliser pour cet usager. Cette AVP DOIT seulement être présente dans une réponse d'autorisation. Plusieurs instances de cette AVP ne sont pas permises dans le même message.

La codification de la gamme permise dans ce champ sort du domaine d'application de la présente spécification.

4.4.10.8 AVP d'accès distant AppleTalk

Les AVP définies dans ce paragraphe sont utilisées lorsque l'utilisateur demande l'accès, ou qu'il lui est accordé, au réseau AppleTalk via le protocole d'accès distant AppleTalk (ARAP, *AppleTalk Remote Access Protocol*) [ARAP]. Elles ne sont présentes que si l'AVP Framed-Protocol (paragraphe 4.4.10.1) est réglée à ARAP. Le paragraphe 2.2 de la RFC 2869 décrit l'utilisation de ces attributs.

4.4.10.8.1 AVP ARAP-Features

L'AVP ARAP-Features (code d'AVP 71) est du type OctetString et PEUT être présente dans le message AA-Accept si l'AVP Framed-Protocol est réglée à la valeur de ARAP. Voir dans la RFC 2869 plus d'informations sur le format de cette AVP.

4.4.10.8.2. AVP ARAP-Zone-Access

L'AVP ARAP-Zone-Access (code d'AVP 72) est du type Enumerated et PEUT être présente dans le message AA-Accept si l'AVP Framed-Protocol est réglée à la valeur de ARAP.

La liste des valeurs acceptées figure dans [RADIUS-ATT] et est définie dans la [RFC2869].

4.4.11 AVP d'autorisation d'accès non tramé

Ce paragraphe contient les AVP d'autorisation qui sont nécessaires pour prendre en charge la fonctionnalité de serveur terminal. Les AVP définies dans ce paragraphe PEUVENT être présentes dans un message si l'AVP Service-Type a été réglée à "Login" ou "Callback Login".

4.4.11.1 AVP Login-IP-Host

L'AVP Login-IP-Host (code d'AVP 14) [RFC2865] est du type OctetString et contient l'adresse IPv4 d'un hôte avec lequel connecter l'utilisateur lorsque l'AVP Login-Service est incluse. Elle PEUT être utilisée dans une commande AA-Request comme indication au serveur Diameter qu'un hôte spécifique est désiré, mais le serveur Diameter n'est pas obligé de suivre ce conseil dans la réponse AA.

Deux adresses ont une signification particulière : toute de uns et toute de zéros. La valeur toute de uns indique que le NAS DEVRAIT permettre à l'utilisateur de choisir une adresse. La valeur 0 indique que le NAS DEVRAIT choisir un hôte pour y connecter l'utilisateur.

4.4.11.2 AVP Login-IPv6-Host

L'AVP Login-IPv6-Host (code d'AVP 98) [RFC3162] est du type OctetString et contient l'adresse IPv6 d'un hôte auquel connecter l'utilisateur lorsque l'AVP Login-Service est incluse. Elle PEUT être utilisée dans une commande AA-Request comme indication au serveur Diameter qu'un hôte spécifique est désiré, mais le serveur Diameter n'est pas obligé de suivre ce conseil dans la réponse AA.

Deux adresses ont une signification particulière : 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF et 0. La valeur 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF indique que le NAS DEVRAIT permettre à l'utilisateur de choisir une adresse. La valeur 0 indique que le NAS DEVRAIT choisir un hôte pour y connecter l'utilisateur.

4.4.11.3 AVP Login-Service

L'AVP Login-Service (code d'AVP 15) est du type Enumerated et contient le service qui devrait être utilisé pour connecter l'utilisateur à l'hôte. Cette AVP DEVRAIT n'être présente que dans les réponses d'autorisation. La liste des valeurs acceptées figure dans la RFC 2869.

4.4.11.4 Services TCP

L'AVP décrite dans le paragraphe qui suit PEUT être présente si l'AVP Login-Service est réglée à Telnet, Rlogin, TCP Clear, ou TCP Clear Quiet.

4.4.11.4.1 AVP Login-TCP-Port

L'AVP Login-TCP-Port (code d'AVP 16) est du type Unsigned32 et contient l'accès TCP auquel l'utilisateur va être connecté lorsque l'AVP Login-Service est aussi présente. Cette AVP DEVRAIT n'être présente que dans les réponses d'autorisation. La valeur NE DOIT PAS être supérieure à 65 535.

4.4.11.5 Services LAT

Les AVP décrites dans ce paragraphe PEUVENT être présentes si l'AVP Login-Service est réglée à LAT [LAT].

4.4.11.5.1 AVP Login-LAT-Service

L'AVP Login-LAT-Service (code d'AVP 34) est du type OctetString et contient le système auquel l'utilisateur va être connecté par LAT. Elle PEUT être utilisée dans une demande d'autorisation comme indication au serveur qu'un service spécifique est désiré, mais le serveur n'est pas obligé de suivre ce conseil dans la réponse correspondante. Cette AVP DOIT n'être présente que dans la réponse si l'AVP Login-Service déclare que LAT est désiré.

Les administrateurs utilisent cet attribut de service lorsque ils traitent des systèmes en grappes. Dans ces environnements, plusieurs hôtes en temps partagé différents partagent les mêmes ressources (disques, imprimantes, etc.) et les administrateurs configurent souvent chaque hôte à offrir l'accès (le service) pour chacune des ressources partagées. Dans ce cas, chaque hôte de la grappe annonce ses services par des diffusions LAT.

Les utilisateurs sophistiqués savent souvent quels fournisseurs de service (machines) sont plus rapides et tendent à utiliser un nom de nœud lorsque ils initient une connexion LAT. Certains administrateurs veulent que des utilisateurs particuliers utilisent certaines machines comme forme principale d'équilibrage de charge (bien que LAT lui-même sache faire l'équilibrage de charge).

Le champ String contient l'identité du service LAT à utiliser. L'architecture LAT permet que cette chaîne contienne des caractères $ (dollar), - (tiret), . (point), _ (souligné), numériques, alphabétiques majuscules et minuscules, et l'extension de jeu de caractère ISO Latin-1 [ISO.8859-1]. Toutes les comparaisons de chaîne LAT sont insensibles à la casse.

4.4.11.5.2 AVP Login-LAT-Node

L'AVP Login-LAT-Node (code d'AVP 35) est du type OctetString et contient le nœud auquel l'utilisateur va être automatiquement connecté par LAT. Elle PEUT être utilisée dans une demande d'autorisation comme indication au serveur qu'un nœud LAT spécifique est désiré, mais le serveur n'est pas obligé de suivre ce conseil dans la réponse correspondante. Cette AVP DOIT n'être présente que dans une réponse si l'AVP Login-Service-Type est réglée à LAT.

Le champ String contient l'identité du service LAT à utiliser. L'architecture LAT permet que cette chaîne contienne des caractères $ (dollar), - (tiret), . (point), _ (souligné), numériques, alphabétiques majuscules et minuscules, et l'extension de jeu de caractère ISO Latin-1 [ISO.8859-1]. Toutes les comparaisons de chaîne LAT sont insensibles à la casse.

4.4.11.5.3 AVP Login-LAT-Group

L'AVP Login-LAT-Group (code d'AVP 36) est du type OctetString et contient une chaîne qui identifie les codes de groupe LAT que ce usager est autorisé à utiliser. Elle PEUT être utilisée dans une demande d'autorisation comme indication au serveur qu'un groupe spécifique est désiré, mais le serveur n'est pas obligé de suivre ce conseil dans la réponse correspondante. Cette AVP DOIT n'être présente que dans une réponse si l'AVP Login-Service-Type est réglée à LAT.

LAT prend en charge 256 différents codes de groupe, que LAT utilise comme une forme de droits d'accès. LAT code les groupes comme un schéma binaire de 256 bits.

Les administrateurs peuvent allouer un ou plusieurs des bits de code de groupe au fournisseur de service LAT ; il n'acceptera les connexions LAT que si elles ont ces codes de groupe établis dans le schéma binaire. Les administrateurs allouent un schéma binaire de codes de groupe autorisé à chaque utilisateur. LAT les prend dans le système d'exploitation et les utilise dans ses demandes aux fournisseurs de service.

La codification de la gamme des utilisations permises de ce champ sort du domaine d'application de cette spécification.

4.4.11.5.4 AVP Login-LAT-Port

L'AVP Login-LAT-Port (code d'AVP 63) est du type OctetString et contient l'accès auquel l'utilisateur va être connecté par LAT. Elle PEUT être utilisée dans une demande d'autorisation comme indication au serveur qu'un accès spécifique est

désiré, mais le serveur n'est pas obligé de suivre ce conseil dans la réponse correspondante. Cette AVP DOIT n'être présente que dans une réponse si l'AVP Login-Service-Type est réglée à LAT.

Le champ String contient l'identité du service LAT à utiliser. L'architecture LAT permet que cette chaîne contienne des caractères $ (dollar), - (tiret), . (point), _ (souligné), numériques, alphabétiques majuscules et minuscules, et l'extension de jeu de caractère ISO Latin-1 [ISO.8859-1]. Toutes les comparaisons de chaîne LAT sont insensibles à la casse.

4.5 AVP de tunnelage de NAS

Certains NAS prennent en charge des services de tunnel obligatoires dans lesquels les données de connexion entrantes sont convoyées par une méthode d'encapsulation jusqu'à une passerelle ailleurs dans le réseau. Ceci est normalement transparent pour l'utilisateur du service, et les caractéristiques du tunnel peuvent être décrites par le serveur distant d'authentification, autorisation, et comptabilité, sur la base des informations d'autorisation de l'utilisateur. Plusieurs caractéristiques de tunnel peuvent être retournées, et la mise en œuvre de NAS peut en choisir une. Voir plus d'informations dans les [RFC2868] et [RFC2867].

Le tableau suivant donne les valeurs de fanions possibles pour les AVP de niveau session.

		Règles de fanion d'AVP	
Nom d'attribut	**§**	**Doit**	**Ne doit pas**
Tunneling	4.5.1	M	V
Tunnel-Type	4.5.2	M	V
Tunnel-Medium-Type	4.5.3	M	V
Tunnel-Client-Endpoint	4.5.4	M	V
Tunnel-Server-Endpoint	4.5.5	M	V
Tunnel-Password	4.5.6	M	V
Tunnel-Private-Group-Id	4.5.7	M	V
Tunnel-Assignment-Id	4.5.8	M	V
Tunnel-Preference	4.5.9	M	V
Tunnel-Client-Auth-Id	4.5.10	M	V
Tunnel-Server-Auth-Id	4.5.11	M	V

4.5.1 AVP Tunneling

L'AVP Tunneling *(tunnelage)* (code d'AVP 401) est du type Grouped et contient les AVP suivantes, utilisées pour décrire un service de tunnel obligatoire [RFC2868], [RFC2867]. Son champ Données a la grammaire ABNF suivante :

```
Tunneling   ::= < En-tête d'AVP : 401 >
                { Tunnel-Type } (type de tunnel)
                { Tunnel-Medium-Type } (type de support de tunnel)
                { Tunnel-Client-Endpoint } (point d'extrémité client du tunnel)
                { Tunnel-Server-Endpoint } (point d'extrémité serveur du tunnel)
                [ Tunnel-Preference ] (préférence du tunnel)
                [ Tunnel-Client-Auth-Id ] (identifiant d'autorisation du client du tunnel)
                [ Tunnel-Server-Auth-Id ] (identifiant d'autorisation du serveur du tunnel)
                [ Tunnel-Assignment-Id ] (identifiant d'allocation de tunnel)
                [ Tunnel-Password ] (mot de passe du tunnel)
                [ Tunnel-Private-Group-Id ] (identifiant de groupe privé du tunnel)
```

4.5.2 AVP Tunnel-Type

L'AVP Tunnel-Type (code d'AVP 64) est du type Enumerated et contient le ou les protocoles de tunnelage à utiliser (dans le cas de l'initiateur d'un tunnel) ou en usage (dans le cas de l'extrémité de terminaison d'un tunnel). Elle PEUT être utilisée dans une demande d'autorisation comme indication au serveur qu'un type de tunnel spécifique est désiré, mais le serveur n'est pas obligé de suivre ce conseil dans la réponse correspondante. L'AVP Tunnel-Type DEVRAIT aussi être incluse dans les messages ACR.

Un initiateur de tunnel n'est pas obligé de mettre en œuvre un de ces types de tunnel. Si un initiateur de tunnel reçoit une réponse qui ne contient que des types de tunnel inconnus ou non pris en charge, l'initiateur du tunnel DOIT se comporter comme si une réponse avait été reçue avec un code de résultat indiquant un échec. La liste des valeurs acceptées figure dans [RADIUS-ATT].

4.5.3 AVP Tunnel-Medium-Type

L'AVP Tunnel-Medium-Type (code d'AVP 65) est du type Enumerated et contient le support de transport à utiliser lors de la création d'un tunnel pour les protocoles (comme L2TP [RFC3931]) qui peuvent fonctionner sur plusieurs transports. Elle PEUT être utilisée dans une demande d'autorisation comme indication au serveur qu'un support spécifique est désiré, mais le serveur n'est pas obligé de suivre ce conseil dans la réponse correspondante. La liste des valeurs acceptées figure dans [RADIUS-ATT].

4.5.4 AVP Tunnel-Client-Endpoint

L'AVP Tunnel-Client-Endpoint (code d'AVP 66) est du type UTF8String et contient l'adresse de l'extrémité initiatrice du tunnel. Elle PEUT être utilisée dans une demande d'autorisation comme indication au serveur qu'un point d'extrémité spécifique est désiré, mais le serveur n'est pas obligé de suivre ce conseil dans la réponse correspondante. Cette AVP DEVRAIT être incluse dans les messages ACR correspondants, auquel cas elle indique d'adresse d'où le tunnel a été initié. Cette AVP, avec les AVP Tunnel-Server-Endpoint (paragraphe 4.5.5) et Session-Id ([RFC6733], paragraphe 8.8) peut être utilisée pour fournir un moyen unique au monde pour identifier un tunnel pour les besoins de la comptabilité et de la vérification.

Si la valeur de l'AVP Tunnel-Medium-Type (paragraphe 4.5.3) est IPv4 (1), cette chaîne est alors soit le nom de domaine pleinement qualifié (FQDN) de la machine client du tunnel, soit une adresse IP en "décimal séparé par des points". Les mises en œuvre DOIVENT prendre en charge le format décimal séparé par des points et DEVRAIENT accepter le format FQDN pour les adresses IP.

Si Tunnel-Medium-Type est IPv6 (2), cette chaîne est alors soit le FQDN de la machine client du tunnel, soit une représentation textuelle de l'adresse dans la forme préférée ou de remplacement [RFC3516]. Les mises en œuvre conformes DOIVENT accepter la forme préférée et DEVRAIENT accepter les deux formes de texte de remplacement et le format FQDN pour les adresses IPv6.

Si Tunnel-Medium-Type n'est ni IPv4 ni IPv6, la chaîne est alors une étiquette qui se réfère aux données locales de configuration du client Diameter qui décrivent l'adresse de client de l'interface ou spécifique du support à utiliser.

Noter que cette application traite les noms de domaines internationalisés (IDN) de la même façon que le protocole Diameter de base (voir les détails à l'Appendice D de la RFC 6733).

4.5.5 AVP Tunnel-Server-Endpoint

L'AVP Tunnel-Server-Endpoint (code d'AVP 67) est du type UTF8String et contient l'adresse de l'extrémité serveur du tunnel. Elle PEUT être utilisée dans une demande d'autorisation comme indication au serveur qu'un point d'extrémité spécifique est désiré, mais le serveur n'est pas obligé de suivre ce conseil dans la réponse correspondante.

Cette AVP DEVRAIT être incluse dans les messages ACR correspondants, auquel cas elle indique l'adresse d'où le tunnel a été initié. Cette AVP, avec les AVP Tunnel-Client-Endpoint (paragraphe 4.5.4) et Session-Id ([RFC6733], paragraphe 8.8) peut être utilisée pour fournir un moyen unique au monde pour identifier un tunnel pour les besoins de la comptabilité et de la vérification.

Si Tunnel-Medium-Type est IPv4 (1), cette chaîne est alors soit le nom de domaine pleinement qualifié (FQDN) de la machine serveur du tunnel, soit une adresse IP en "décimal séparé par des points". Les mises en œuvre DOIVENT accepter le format décimal séparé par des points et DEVRAIENT accepter le format FQDN pour les adresses IP.

Si Tunnel-Medium-Type est IPv6 (2), cette chaîne est alors soit le FQDN de la machine serveur du tunnel, soit une représentation textuelle de l'adresse en forme préférée ou de remplacement [RFC3516]. Les mises en œuvre DOIVENT accepter la forme préférée et DEVRAIENT accepter la forme texte de remplacement et le format FQDN pour les adresses IPv6.

Si Tunnel-Medium-Type n'est ni IPv4 ni IPv6, cette chaîne est une étiquette qui se réfère aux données de configuration locales pour le client Diameter qui décrivent l'adresse de serveur de l'interface ou spécifique du support à utiliser.

Noter que cette application traite les IDN de la même façon que le protocole Diameter de base (voir les détails à l'Appendice D de la RFC 6733).

4.5.6 AVP Tunnel-Password

L'AVP Tunnel-Password (code d'AVP 69) est du type OctetString et peut contenir un mot de passe à utiliser pour s'authentifier auprès d'un serveur distant.

L'AVP Tunnel-Password AVP NE DEVRAIT PAS être utilisée dans des environnements de mandataires qui ne sont pas de confiance sans la chiffrer en utilisant une technique de sécurité de bout en bout.

4.5.7 AVP Tunnel-Private-Group-Id

L'AVP Tunnel-Private-Group-Id (code d'AVP 81) est du type OctetString et contient l'identifiant de groupe pour une certaine session tunnelée. L'AVP Tunnel-Private-Group-Id PEUT être incluse dans une demande d'autorisation si l'initiateur du tunnel peut prédéterminer le groupe résultant d'une certaine connexion. Elle DEVRAIT être incluse dans la réponse d'autorisation si cette session tunnelée doit être traitée comme appartenant à un groupe privé particulier. Les groupes privés peuvent être utilisés pour associer une session tunnelée à un groupe d'utilisateurs particulier. Par exemple, elle PEUT être utilisée pour faciliter l'acheminement d'adresses IP non enregistrées à travers une certaine interface. Cette AVP DEVRAIT être incluse dans les messages ACR qui relèvent de la session tunnelée.

4.5.8 AVP Tunnel-Assignment-Id

L'AVP Tunnel-Assignment-Id (code d'AVP 82) est du type OctetString et est utilisée pour indiquer à l'initiateur du tunnel le tunnel particulier à allouer à une session. Certains protocoles de tunnelage, comme PPTP [RFC2637] et L2TP [RFC3931], permettent que des sessions entre les deux mêmes points d'extrémité de tunnel soient multiplexées sur le même tunnel et aussi qu'une certaine session utilise son propre tunnel dédié. Cet attribut fournit un mécanisme pour que Diameter informe l'initiateur de tunnel (par exemple, un LAC) d'allouer la session à un tunnel multiplexé ou à un tunnel séparé. De plus, elle permet que des sessions qui partagent des tunnels multiplexés soient allouées à des tunnels multiplexés différents.

Une mise en œuvre de tunnelage particulière peut allouer des caractéristiques différentes à des tunnels particuliers. Par exemple, des tunnels différents peuvent recevoir des paramètres de qualité de service différents. De tels tunnels peuvent être utilisés pour porter des sessions individuelles ou multiples. L'attribut Tunnel-Assignment-Id permet donc au serveur Diameter d'indiquer qu'une certaine session est à allouer à un tunnel fournissant un niveau de service approprié. Il est prévu que tous les attributs de tunnelage Diameter en rapport avec la qualité de service qui seront définis à l'avenir et qui accompagneront celui-ci seront associés par l'initiateur du tunnel à l'identifiant donné par cet attribut. En attendant, toute sémantique donnée à une chaîne d'identifiant particulière relève de la configuration locale chez l'initiateur de tunnel.

L'AVP Tunnel-Assignment-Id n'a de signification que pour Diameter et l'initiateur de tunnel. L'identifiant qu'il spécifie n'est destiné qu'à l'utilisation locale de Diameter et de l'initiateur du tunnel. L'identifiant alloué par l'initiateur du tunnel n'est pas transmis à l'homologue du tunnel.

Cet attribut PEUT être inclus dans les réponses d'autorisation. L'initiateur du tunnel qui reçoit cet attribut PEUT choisir de l'ignorer et d'allouer la session à un tunnel arbitraire multiplexé ou non entre les points d'extrémité désirés. Cette AVP DEVRAIT aussi être incluse dans les messages de demande de comptabilité relevant de la session tunnelée.

Si un initiateur de tunnel prend en charge l'AVP Tunnel-Assignment-Id, il devrait alors allouer une session à un tunnel de la manière suivante :

- Si cette AVP est présente et si un tunnel existe entre les points d'extrémité spécifiés avec l'identifiant spécifié, la session devrait alors être allouée à ce tunnel.
- Si cette AVP est présente et si aucun tunnel n'existe entre les points d'extrémité spécifiés avec l'identifiant spécifié, un nouveau tunnel devrait alors être établi pour la session et l'identifiant spécifié devrait être associé au nouveau tunnel.
- Si cette AVP n'est pas présente, la session est alors allouée à un tunnel non désigné. Si il n'existe pas encore de tunnel non désigné entre les points d'extrémité spécifiés, il en est établi un et il est utilisé pour cette session et pour les suivantes établies sans l'attribut Tunnel-Assignment-Id. Un initiateur de tunnel NE DOIT PAS allouer une session pour laquelle une AVP Tunnel-Assignment-Id n'a pas été spécifiée au tunnel désigné (c'est-à-dire, un qui a été initié par une session spécifiant cette AVP).

Note que le même identifiant peut être utilisé pour nommer des tunnels différents si ceux-ci sont entre des points d'extrémité différents.

4.5.9 AVP Tunnel-Preference

L'AVP Tunnel-Preference (code d'AVP 83) est du type Unsigned32 et est utilisée pour identifier la préférence relative allouée à chaque tunnel lorsque plus d'un ensemble d'AVP de tunnelage est retourné au sein d'AVP groupées séparés. Elle PEUT être utilisée dans une demande d'autorisation comme indication au serveur qu'une préférence spécifique est désirée, mais le serveur n'est pas obligé de suivre ce conseil dans la réponse correspondante.

Par exemple, supposons que les AVP qui décrivent deux tunnels sont retournées par le serveur, une avec un type de tunnel de PPTP et l'autre avec un type de tunnel de L2TP. Si le tunnel initiateur prend en charge un seul des types de tunnel retournés, il va initier un tunnel de ce type. Si, cependant, il prend en charge les deux protocoles de tunnel, il DEVRAIT utiliser la valeur de l'AVP Tunnel-Preference pour décider quel tunnel devrait être lancé. Le tunnel qui a la plus faible valeur numérique dans le champ Valeur de cette AVP DEVRAIT recevoir la plus forte préférence. Les valeurs allouées à deux instances ou plus de l'AVP Tunnel-Preference au sein d'une certaine réponse d'autorisation PEUVENT être identiques. Dans ce cas, l'initiateur du tunnel DEVRAIT utiliser une métrique configurée en local pour décider quel ensemble d'AVP utiliser.

4.5.10 AVP Tunnel-Client-Auth-Id

L'AVP Tunnel-Client-Auth-Id (code d'AVP 90) est du type UTF8String et spécifie le nom de 7 bits en US-ASCII utilisé par l'initiateur du tunnel durant la phase d'authentification de l'établissement du tunnel. Elle PEUT être utilisée dans une demande d'autorisation comme indication au serveur qu'une préférence spécifique est désirée, mais le serveur n'est pas obligé de suivre ce conseil dans la réponse correspondante. Cette AVP DOIT être présente dans la réponse d'autorisation si un nom d'authentification autre que celui par défaut est désiré. Cette AVP DEVRAIT être incluse dans les messages ACR relevant de la session tunnelée.

4.5.11 AVP Tunnel-Server-Auth-Id

L'AVP Tunnel-Server-Auth-Id (code d'AVP 91) est du type UTF8String et spécifie le nom de 7 bits en US-ASCII utilisé par la terminaison du tunnel durant la phase d'authentification de l'établissement du tunnel. Elle PEUT être utilisée dans une demande d'autorisation comme indication au serveur qu'une préférence spécifique est désirée, mais le serveur n'est pas obligé de suivre ce conseil dans la réponse correspondante. Cette AVP DOIT être présente dans la réponse d'autorisation si un nom d'authentification autre que celui par défaut est désiré. Cette AVP DEVRAIT être incluse dans le messages ACR relevant de la session tunnelée.

4.6 AVP de comptabilité de NAS

Les applications qui mettent en œuvre la présente spécification utilisent la comptabilité Diameter (comme définie dans la [RFC6733]) et les AVP du paragraphe suivant. L'usage d'AVP spécifiques de service est défini dans les tableaux de la Section 5.

Si la comptabilité est active, les messages de demande de comptabilité (ACR) DEVRAIENT être envoyés après l'achèvement de toutes transactions d'authentification ou d'autorisation et à la fin d'une session. La valeur de l'AVP Accounting-Record-Type [RFC6733] indique le type d'événement. Toutes les autres AVP identifient la session et fournissent des informations supplémentaires relatives à l'événement.

L'achèvement avec succès de la première transaction d'authentification ou d'autorisation DEVRAIT causer l'envoi d'un START_RECORD *(début d'enregistrement)*. Si des authentifications ou autorisations supplémentaires surviennent dans des transactions ultérieures, le premier échange devrait générer un START_RECORD, et les suivantes un INTERIM_RECORD *(enregistrement intermédiaire)*. Pour une certaine session, il DOIT seulement y avoir un seul ensemble d'enregistrements START et STOP correspondants, avec un nombre arbitraire de INTERIM_RECORDS entre eux, ou un EVENT_RECORD *(enregistrement d'événement)* indiquant la raison pour laquelle une session n'a pas débuté.

Le tableau suivant donne les valeurs de fanions possibles pour les AVP de niveau session.

		Règles de fanion d'AVP	
Nom d'attribut	**§**	**Doit**	**Ne doit pas**
Accounting-Input-Octets	4.6.1	M	V
Accounting-Output-Octets	4.6.2	M	V
Accounting-Input-Packets	4.6.3	M	V
Accounting-Output-Packets	4.6.4	M	V
Acct-Session-Time	4.6.5	M	V
Acct-Authentic	4.6.6	M	V
Accounting-Auth-Method	4.6.7	M	V
Acct-Delay-Time	4.6.8	M	V
Acct-Link-Count	4.6.9	M	V
Acct-Tunnel-Connection	4.6.10	M	V
Acct-Tunnel-Packets-Lost	4.6.11	M	V

4.6.1 AVP Accounting-Input-Octets

L'AVP Accounting-Input-Octets (code d'AVP 363) est du type Unsigned64 et contient le nombre d'octets reçus de l'utilisateur.

Pour l'usage du NAS, cette AVP indique combien d'octets ont été reçus de l'accès dans le courant de cette session. Elle peut seulement être présente dans les messages ACR qui ont un type d'enregistrement comptable [RFC6733] de INTERIM_RECORD ou STOP_RECORD.

4.6.2 AVP Accounting-Output-Octets

L'AVP Accounting-Output-Octets (code d'AVP 364) est du type Unsigned64 et contient le nombre d'octets envoyés à l'utilisateur.

Pour l'usage de NAS, cette AVP indique combien d'octets ont été envoyés à l'accès dans le courant de cette session. Elle ne peut être présente que dans les messages ACR qui ont un type d'enregistrement comptable de INTERIM_RECORD ou STOP_RECORD.

4.6.3 AVP Accounting-Input-Packets

L'AVP Accounting-Input-Packets (code d'AVP 365) est du type Unsigned64 et contient le nombre de paquets reçus de l'utilisateur.

Pour l'usage de NAS, cette AVP indique combien de paquets ont été reçus de l'accès dans le courant d'une session fournie à un usager tramé. Elle ne peut être présente que dans les messages ACR qui ont un type d'enregistrement comptable de INTERIM_RECORD ou STOP_RECORD.

4.6.4 AVP Accounting-Output-Packets

L'AVP Accounting-Output-Packets (code d'AVP 366) est du type Unsigned64 et contient le nombre de paquets IP envoyés à l'utilisateur.

Pour l'usage de NAS, cette AVP indique combien de paquets ont été envoyés à l'accès dans le courant d'une session fournie à un usager tramé. Elle ne peut être présente que dans les messages ACR qui ont un type d'enregistrement comptable de INTERIM_RECORD ou STOP_RECORD.

4.6.5 AVP Acct-Session-Time

L'AVP Acct-Session-Time (code d'AVP 46) est du type Unsigned32 et indique la longueur de la session en cours en secondes. Elle ne peut être présente que dans les messages ACR qui ont un type d'enregistrement comptable de INTERIM_RECORD ou STOP_RECORD.

4.6.6 AVP Acct-Authentic

L'AVP Acct-Authentic (code d'AVP 45) est du type Enumerated et spécifie comment l'utilisateur a été authentifié. La liste des valeurs acceptées figure dans [RADIUS-ATT].

4.6.7 AVP Accounting-Auth-Method

L'AVP Accounting-Auth-Method (code d'AVP 406) est du type Enumerated. Un NAS PEUT inclure cette AVP dans un message Accounting-Request pour indiquer la méthode utilisée pour authentifier l'utilisateur. (Noter que cette AVP est sémantiquement équivalente, et les valeurs acceptées sont identiques, à l'attribut RADIUS Microsoft spécifique du fabricant MS-Acct-Auth-Type [RFC2548]).

4.6.8 AVP Acct-Delay-Time

L'AVP Acct-Delay-Time (code d'AVP 41) est du type Unsigned32 et indique le nombre de secondes pendant lequel le client Diameter a essayé d'envoyer la demande de comptabilité (ACR, *Accounting-Request*). Le serveur de comptabilité peut soustraire cette valeur de l'heure d'arrivée de l'ACR au serveur pour calculer l'heure approximative de l'événement qui a causé la génération de l'ACR.

Cette AVP n'est pas utilisée pour les retransmissions au niveau transport (TCP ou SCTP). Elle peut être plutôt utilisée lorsque une commande ACR ne peut pas être transmise parce que il n'y a pas d'homologue approprié à qui la transmettre ou qu'elle a été rejetée parce qu'elle n'a pas pu être livrée. Dans ces cas, la commande PEUT être mise en mémoire tampon et transmise ultérieurement, lorsque une connexion avec un homologue approprié sera disponible ou après l'écoulement d'un délai suffisant pour que l'hôte de destination puisse être accessible et opérationnel. Si l'ACR est envoyé à nouveau de cette façon, l'AVP Acct-Delay-Time DEVRAIT être incluse. La valeur de cette AVP indique le nombre de secondes qui se sont écoulées entre l'heure de la première tentative de transmission et la tentative actuelle.

4.6.9 AVP Acct-Link-Count

L'AVP Acct-Link-Count (code d'AVP 51) est du type Unsigned32 et indique le nombre total de liaisons qui ont été actives (actuelles ou closes) dans une certaine session multi liaisons au moment de la génération de l'enregistrement comptable. Cette AVP PEUT être incluse dans les AVP Accounting-Request pour toute session qui peut faire partie d'un service multi liaisons.

L'AVP Acct-Link-Count AVP peut être utilisée pour rendre plus facile à un serveur de comptabilité de savoir quand il a tous les enregistrements pour un certain service multi liaisons. Lorsque le nombre d'AVP Accounting-Request reçues avec Accounting-Record-Type = STOP_RECORD et avec les mêmes AVP Acct-Multi-Session-Id et Session-Id uniques égaux à la plus grande valeur de Acct-Link-Count vue dans ces AVP Accounting-Request, toutes les AVP Accounting-Request STOP_RECORD pour ce service multi liaison ont été reçues.

L'exemple qui suit, qui montre huit AVP Accounting-Request, illustre comment l'AVP Acct-Link-Count est utilisée. Dans le tableau ci-dessous, seules les AVP pertinentes sont montrées, bien que des AVP supplémentaires contenant des informations comptables seraient présentes dans les AVP de demande de comptabilité.

Acct-Multi-Session-Id	Session-Id	Accounting-Record-Type	Acct-Link-Count
"...10"	"...10"	START_RECORD	1
"...10"	"...11"	START_RECORD	2
"...10"	"...11"	STOP_RECORD	2
"...10"	"...12"	START_RECORD	3
"...10"	"...13"	START_RECORD	4
"...10"	"...12"	STOP_RECORD	4
"...10"	"...13"	STOP_RECORD	4
"...10"	"...10"	STOP_RECORD	4

4.6.10 AVP Acct-Tunnel-Connection

L'AVP Acct-Tunnel-Connection (code d'AVP 68) est du type OctetString et contient l'identifiant alloué à la session de tunnel. Cette AVP, avec les AVP Tunnel-Client-Endpoint (paragraphe 4.5.4) et Tunnel-Server-Endpoint (paragraphe 4.5.5) peut être utilisée pour fournir un moyen d'identifier de façon univoque une session de tunnel pour les besoins de vérification.

Le format de l'identifiant dans cette AVP dépend de la valeur de l'AVP Tunnel-Type (paragraphe 4.5.2). Par exemple, pour identifier pleinement une connexion de tunnel L2TP, l'identifiant de tunnel L2TP et l'identifiant d'appel peuvent être codés dans ce champ. Le codage exact de ce champ dépend de la mise en œuvre.

4.6.11 AVP Acct-Tunnel-Packets-Lost

L'AVP Acct-Tunnel-Packets-Lost (code d'AVP 86) est du type Unsigned32 et contient le nombre de paquets perdus sur un certain tunnel.

5. Tableau d'occurrence des AVP

Les tableaux suivants présentent les AVP utilisées par les applications de NAS dans les messages de NAS et spécifient dans quels messages Diameter elles peuvent ou ne peuvent pas être présentes. Les messages et AVP définis dans le protocole Diameter de base [RFC6733] ne sont pas décrits dans le présent document. Noter que les AVP qui ne peuvent être présentes qu'au sein d'une AVP groupée ne sont pas représentées dans ces tableaux.

Les tableaux utilisent les symboles suivants :
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 : exactement une instance de l'AVP DOIT être présente dans le message.

5.1 Tableau des AVP de demande/réponse AA

Le tableau de ce paragraphe se limite aux codes de commande définis dans la présente spécification.

Nom d'attribut	Commande AAR	Commande AAA
Acct-Interim-Interval	0	0-1
ARAP-Challenge-Response	0	0-1
ARAP-Features	0	0-1
ARAP-Password	0-1	0
ARAP-Security	0-1	0-1
ARAP-Security-Data	0+	0+
ARAP-Zone-Access	0	0-1
Auth-Application-Id	1	1
Auth-Grace-Period	0-1	0-1
Auth-Request-Type	1	1
Auth-Session-State	0-1	0-1
Authorization-Lifetime	0-1	0-1
Callback-Id	0	0-1
Callback-Number	0-1	0-1
Called-Station-Id	0-1	0
Calling-Station-Id	0-1	0
CHAP-Auth	0-1	0
CHAP-Challenge	0-1	0
Class	0	0+
Configuration-Token	0	0+
Connect-Info	0+	0
Destination-Host	0-1	0
Destination-Realm	1	0
Error-Message	0	0-1
Error-Reporting-Host	0	0-1
Failed-AVP	0+0+	
Filter-Id	0	0+
Framed-Appletalk-Link	0	0-1
Framed-Appletalk-Network	00+	
Framed-Appletalk-Zone	0	0-1
Framed-Compression	0+	0+
Framed-Interface-Id	0-1	0-1
Framed-IP-Address	0-1	0-1
Framed-IP-Netmask	0-1	0-1
Framed-IPv6-Prefix	0+	0+
Framed-IPv6-Pool	0	0-1
Framed-IPv6-Route	0	0+
Framed-IPX-Network	0	0-1
Framed-MTU	0-1	0-1
Framed-Pool	0	0-1
Framed-Protocol	0-1	0-1
Framed-Route	0	0+
Framed-Routing	0	0-1
Idle-Timeout	0	0-1
Login-IP-Host	0+	0+
Login-IPv6-Host	0+	0+
Login-LAT-Group	0-1	0-1
Login-LAT-Node	0-1	0-1
Login-LAT-Port	0-1	0-1
Login-LAT-Service	0-1	0-1
Login-Service	0	0-1
Login-TCP-Port	0	0-1
Multi-Round-Time-Out	0	0-1

NAS-Filter-Rule	0	0+
NAS-Identifier	0-1	0
NAS-IP-Address	0-1	0|
NAS-IPv6-Address	0-1	0
NAS-Port	0-1	0|
NAS-Port-Id	0-1	0|
NAS-Port-Type	0-1	0
Origin-AAA-Protocol	0-1	0-1
Origin-Host	1	1
Origin-Realm	1	1
Origin-State-Id	0-1	0-1
Originating-Line-Info	0-1	0
Password-Retry	0	0-1
Port-Limit	0-1	0-1
Prompt	0	0-1
Proxy-Info	0+	0+
QoS-Filter-Rule	0	0+
Re-Auth-Request-Type	0	0-1
Redirect-Host	0	0+
Redirect-Host-Usage	0	0-1
Redirect-Max-Cache-Time	0	0-1
Reply-Message	0	0+
Result-Code	0	1
Route-Record	0+	0
Service-Type	0-1	0-1
Session-Id	1	1
Session-Timeout	0	0-1
State	0-1	0-1
Tunneling	0+	0+
User-Name	0-1	0-1
User-Password	0-1	0

5.2 Tableaux des AVP de comptabilité

Les tableaux de ce paragraphe sont utilisés pour montrer quelles AVP définies dans le présent document doivent être présentes et utilisées dans les messages de comptabilité d'application de NAS. Ces AVP sont définies dans le présent document, ainsi que dans les [RFC6733] et [RFC2866].

5.2.1 Tableau des AVP de comptabilité d'accès structuré

Le tableau de ce paragraphe est utilisé lorsque l'AVP Service-Type (paragraphe 4.4.1) spécifie un accès tramé.

Nom d'attribut	**Commande ACR**	**Commande ACA**
Accounting-Auth-Method	0-1	0
Accounting-Input-Octets	1	0
Accounting-Input-Packets	1	0
Accounting-Output-Octets	1	0
Accounting-Output-Packets	1	0
Accounting-Record-Number	0-1	0-1
Accounting-Record-Type	1	1
Accounting-Realtime-Required	0-1 | 0-1	
Accounting-Sub-Session-Id	0-1	0-1
Acct-Application-Id	0-1	0-1
Acct-Session-Id	1	0-1
Acct-Multi-Session-Id	0-1	0-1
Acct-Authentic	1	0
Acct-Delay-Time	0-1	0
Acct-Interim-Interval	0-1	0-1
Acct-Link-Count	0-1	0
Acct-Session-Time	1	0
Acct-Tunnel-Connection	0-1	0
Acct-Tunnel-Packets-Lost	0-1	0

Authorization-Lifetime	0-1	0
Callback-Id	0-1	0
Callback-Number	0-1	0
Called-Station-Id	0-1	0
Calling-Station-Id	0-1	0
Class	0+	0+
Connection-Info	0+	0
Destination-Host	0-1	0
Destination-Realm	1	0
Event-Timestamp	0-1	0-1
Error-Message	0	0-1
Error-Reporting-Host	0	0-1
Failed-AVP	0	0+
Framed-Appletalk-Link	0-1	0
Framed-Appletalk-Network	0-1	0
Framed-Appletalk-Zone	0-1	0
Framed-Compression	0-1	0
Framed-IP-Address	0-1	0
Framed-IP-Netmask	0-1	0
Framed-IPv6-Prefix	0+	0
Framed-IPv6-Pool	0-1	0
Framed-IPX-Network	0-1	0
Framed-MTU	0-1	0
Framed-Pool	0-1	0
Framed-Protocol	0-1	0
Framed-Route	0-1	0
Framed-Routing	0-1	0
NAS-Filter-Rule	0+	0
NAS-Identifier	0-1	0-1
NAS-IP-Address	0-1	0-1
NAS-IPv6-Address	0-1	0-1
NAS-Port	0-1	0-1
NAS-Port-Id	0-1	0-1
NAS-Port-Type	0-1	0-1
Origin-AAA-Protocol	0-1	0-1
Origin-Host	1	1
Origin-Realm	1	1
Origin-State-Id	0-1	0-1
Originating-Line-Info	0-1	0
Proxy-Info	0+	0+
QoS-Filter-Rule	0+	0
Route-Record	0+	0
Result-Code	0	1
Service-Type	0-1	0-1
Session-Id	1	1
Termination-Cause	0-1	0-1
Tunnel-Assignment-Id	0-1	0
Tunnel-Client-Endpoint	0-1	0
Tunnel-Medium-Type	0-1	0
Tunnel-Private-Group-Id	0-1	0
Tunnel-Server-Endpoint	0-1	0
Tunnel-Type	0-1	0
User-Name	0-1	0-1

5.2.2 Tableau des AVP de comptabilité d'accès non tramé

Le tableau de ce paragraphe est utilisé lorsque l'AVP Service-Type (paragraphe 4.4.1) spécifie un accès non tramé.

Nom d'attribut	**Commande ACR**	**Commande ACA**
Accounting-Auth-Method	0-1	0
Accounting-Input-Octets	1	0
Accounting-Output-Octets	1	0

Accounting-Record-Type	1	1
Accounting-Record-Number	0-1	0-1
Accounting-Realtime-Required	0-1	0-1
Accounting-Sub-Session-Id	0-1	0-1
Acct-Application-Id	0-1	0-1
Acct-Session-Id	1	0-1
Acct-Multi-Session-Id	0-1	0-1
Acct-Authentic	1	0
Acct-Delay-Time	0-1	0
Acct-Interim-Interval	0-1	0-1
Acct-Link-Count	0-1	0
Acct-Session-Time	1	0
Authorization-Lifetime	0-1	0
Callback-Id	0-1	0
Callback-Number	0-1	0
Called-Station-Id	0-1	0
Calling-Station-Id	0-1	0
Class	0+	0+
Connection-Info	0+	0
Destination-Host	0-1	0
Destination-Realm	1	0
Event-Timestamp	0-1	0-1
Error-Message	0	0-1
Error-Reporting-Host	0	0-1
Failed-AVP	0	0+
Login-IP-Host	0+	0
Login-IPv6-Hos	0+	0
Login-LAT-Service	0-1	0
Login-LAT-Node	0-1	0
Login-LAT-Group	0-1	0
Login-LAT-Port	0-1	0
Login-Service	0-1	0
Login-TCP-Port	0-1	0
NAS-Identifier	0-1	0-1
NAS-IP-Address	0-1	0-1
NAS-IPv6-Address	0-1	0-1
NAS-Port	0-1	0-1
NAS-Port-Id	0-1	0-1
NAS-Port-Type	0-1	0-1
Origin-AAA-Protocol	0-1	0-1
Origin-Host	1	1
Origin-Realm	1	1
Origin-State-Id	0-1	0-1
Originating-Line-Info	0-1	0
Proxy-Info	0+	0+
QoS-Filter-Rule	0+	0
Route-Record	0+	0
Result-Code	0	1
Session-Id	1	1
Service-Type	0-1	0-1
Termination-Cause	0-1	0-1
User-Name	0-1	0-1

6. Considérations relatives à Unicode

Un certain nombre d'AVP de la présente RFC utilisent le type UTF8String spécifié dans le protocole Diameter de base [RFC6733]. Des différences de mise en œuvre du traitement d'entrée Unicode peuvent résulter en ce que l'entrée du même caractère Unicode génère des chaînes UTF-8 différentes qui ne correspondent pas lorsque elles sont comparées. Il peut en résulter des problèmes d'interopérabilité entre un serveur d'accès réseau et un serveur Diameter lorsque une chaîne UTF-8 entrée en local est comparée avec une qui est reçue via Diameter. Beaucoup des utilisations de UTF8String dans cette RFC sont limitées au sous ensemble à 7 bits compatible US-ASCII de UTF-8, où cette classe de problèmes de comparaison de

chaîne Unicode ne se pose pas.

Une préparation soigneuse des chaînes Unicode peut augmenter la probabilité que la comparaison de chaîne fonctionne d'une façon qui ait un sens pour les utilisateurs normaux dans le monde ; la [RFC3454] est un exemple d'un cadre pour une telle préparation de chaîne Unicode. L'application Diameter spécifiée dans la présente RFC a été déployée en utilisant Unicode conformément à la [RFC4005], qui n'exige aucune préparation de chaîne Unicode. Par suite, des exigences supplémentaires pour la préparation de chaînes Unicode dans cette RFC ne seraient pas rétro compatibles avec l'usage existant.

Le serveur Diameter et les serveurs d'accès réseau qu'il dessert peuvent être supposés être sous un contrôle administratif commun, et toutes les chaînes UTF-8 impliquées font partie de la configuration de ces serveurs. Donc, les interfaces administratives pour les mises en œuvre de cette RFC :

a. DEVRAIENT accepter une entrée directe UTF-8 de toutes les chaînes de configuration pour les AVP qui acceptent les caractères Unicode au delà du sous ensemble à 7 bits compatible US-ASCII de Unicode (en plus de toutes dispositions pour accepter les caractères Unicode pour le traitement dans UTF-8), et
b. DEVRAIENT rendre toutes ces chaînes de configuration disponibles comme chaînes UTF-8.

Cette fonctionnalité permet à un administrateur qui rencontre des problèmes de comparaison de chaînes Unicode de copier une instance de chaîne UTF-8 problématique d'un serveur à l'autre, après quoi les deux copies (maintenant identiques) devraient se comparer comme espéré.

7. Considérations relatives à l'IANA

Plusieurs des espaces de noms utilisés dans le présent document sont gérés par l'autorité d'allocation des numéros de l'Internent (IANA, *Internet Assigned Numbers Authority*) [IANA], incluant les codes d'AVP [AVP-Codes], les valeurs spécifiques d'AVP [AVP-Vals], les identifiants d'application [App-Ids], les codes de commande [Command-Codes], et les valeurs d'attributs RADIUS [RADIUS-ATT].

Pour les valeurs actuellement allouées et les politiques gouvernant l'allocation dans ces espaces de noms, prière de se reporter aux registres référencés ci-dessus.

8 Considérations sur la sécurité

Le présent document décrit les extensions à Diameter pour l'application de NAS. Les considérations sur la sécurité concernant le protocole Diameter lui-même sont exposées dans la [RFC6733]. L'utilisation de cette application de Diameter DOIT prendre en compte les questions de sécurité et les exigences du protocole de base.

8.1 Considérations d'authentification

Le présent document ne contient pas de protocole de sécurité mais expose comment les protocoles d'authentification PPP peuvent être portés au sein du protocole Diameter. Les protocoles d'authentification PPP décrits sont PAP et CHAP.

L'utilisation de PAP DEVRAIT être déconseillée, car il expose les mots de passe des utilisateurs à des entités éventuellement non fiables. Cependant, PAP est aussi fréquemment utilisé avec des mots de passe à utilisation unique, qui ne présentent pas de risque pour la sécurité.

Le présent document décrit aussi comment CHAP peut être porté dans le protocole Diameter, ce qui est exigé pour la rétro compatibilité avec RADIUS. Le protocole CHAP, tel qu'utilisé dans un environnement RADIUS, facilite les attaques en répétition d'authentification.

L'utilisation des protocoles d'authentification EAP [RFC4072] peut offrir une meilleure sécurité, en donnant une méthode qui convient aux circonstances. Selon la valeur de l'AVP Auth-Request-Type, le protocole Diameter permet des demandes d'autorisation seule qui ne contiennent pas d'informations d'authentification provenant du client. Cette capacité va au-delà des capacités de vérification d'appel fournies par RADIUS (paragraphe 5.6 de la [RFC2865]) en ce qu'aucune décision d'accès n'est demandée. Par conséquent, une nouvelle session ne peut pas débuter par suite d'une réponse à une demande d'autorisation seule sans introduire un faiblesse significative de sécurité .

8.2 Considérations sur les AVP

Les AVP Diameter contiennent souvent des données sensibles pour la sécurité ; par exemple, des mots de passe d'utilisateur

et des données de localisation, des adresses réseau et des clés de chiffrement. À l'exception des AVP Configuration-Token (paragraphe 4.4.8) QoS-Filter-Rule (paragraphe 4.4.9) et Tunneling (paragraphe 4.5.1) toutes les AVP définies dans le présent document sont considérées comme sensibles pour la sécurité.

Les messages Diameter qui contiennent toute AVP considérée comme sensible pour la sécurité DOIVENT être envoyés protégés via TLS ou IPsec mutuellement authentifiés. De plus, ces messages NE DOIVENT PAS être envoyés via des nœuds intermédiaires si il n'y a pas de sécurité de bout en bout entre le générateur et le receveur ou si le générateur n'a pas une configuration localement de confiance qui indique que la sécurité de bout en bout n'est pas nécessaire. Par exemple, la sécurité de bout en bout peut n'être pas requise dans le cas où un nœud intermédiaire est connu pour fonctionner au titre du même domaine administratif que les points d'extrémité de sorte que la capacité de réussir à compromettre l'intermédiaire impliquerait une forte probabilité d'être capable de compromettre aussi les points d'extrémité. Noter qu'aucun mécanisme de sécurité de bout en bout n'est spécifié dans le présent document.

9. Références

9.1 Références normatives

[ANITypes] NANPA Number Resource Info, "ANI Assignments", <http://www.nanpa.com/number_resource_info/ani_ii_assignments.html >.

[RFC1994] W. Simpson, "Protocole d'authentification par mise en cause de la prise de contact en PPP (CHAP)", août 1996.

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

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

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

[RFC3516] L. Nerenberg, "Extension Contenu binaire à IMAP4", avril 2003. (*MàJ par* RFC4466) *(P.S.)*

[RFC3539] B. Aboba, J. Wood, "Profil de transport d'authentification, d'autorisation et de comptabilité (AAA)", juin 2003. *(P.S.)*

[RFC5234] D. Crocker, éd., P. Overell, "BNF augmenté pour les spécifications de syntaxe : ABNF", janvier 2008. (STD0068)

[RFC5777] J. Korhonen, H. Tschofenig, M. Arumaithurai, M. Jones, A. Lior, "Attributs de classification du trafic et de qualité de service pour Diameter", février 2010. *(P. S.)*

[RFC6733] V. Fajardo, J. Arkko, J. Loughney, G. Zorn, "Protocole de base Diameter", octobre 2012. (*Remplace les* RFC3588, RFC5719) *(P.S.)*

9.2 Références pour information

[ARAP] Apple Computer, "Apple Remote Access Protocol (ARAP) Version 2.0 External Reference Specification", R0612LL/B, septembre 1994.

[AVP-Codes] IANA, "Codes d'AVP", < http://www.iana.org/assignments/aaa-parameters/ >.

[AVP-Vals] IANA, "Valeues spécifiques d'AVP", < http://www.iana.org/assignments/aaa-parameters/ >.

[App-Ids] IANA, "Identifiants d'applications", < http://www.iana.org/assignments/aaa-parameters/ >.

[AppleTalk] Sidhu, G., Andrews, R., et A. Oppenheimer, "Inside AppleTalk", Second Edition Apple Computer, 1990.

[Command-Codes] IANA, "Codes de commande", < http://www.iana.org/assignments/aaa-parameters/ >.

[IANA] IANA, "Internet Assigned Numbers Authority", < http://www.iana.org/ >.

[IPX] Novell, Inc., "NetWare System Technical Interface Overview", #883-000780-001, juin 1989.

[ISO.8859-1] International Organization for Standardization, "Information technology - 8-bit single byte coded graphic - character sets - Part 1: Latin alphabet No. 1, JTC1/ SC2", ISO Standard 8859-1, 1987.

[LAT] Digital Equipment Corp., "Local Area Transport (LAT) Specification V5.0", AA-NL26A-TE, juin 1989.

[RADIUS-ATT] IANA, "Radius Attribute Values", < http://www.iana.org/assignments/radius-types/ >.

[RFC1334] B. Lloyd et W. Simpson, "Protocoles d'authentification PPP", octobre 1992. *(Remplacé par* RFC1994*)*

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

[RFC1990] K. Sklower et autres, "Protocole multi liaisons en PPP (MP)", août 1996. (*Remplace* RFC1717) *(D.S.)*

[RFC2474] K. Nichols, S. Blake, F. Baker et D. Black, "Définition du champ Services différenciés (DS) dans les en-têtes IPv4 et IPv6", décembre 1998. (*MàJ par* RFC3168, RFC3260) *(P.S.)*

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

[RFC2597] J. Heinanen, F. Baker, W. Weiss, J. Wroclawski, "Groupe PHB Transmission assurée", juin 1999. (*MàJ par* RFC3260) (*PS)*

[RFC2637] K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little et G. Zorn, "Protocole de tunnelage point à point (PPTP)", juillet 1999.

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

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

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

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

[RFC2881] D. Mitton, M. Beadles, "Exigences pour la prochaine génération de serveur d'accès réseau (NASREQNG) – modèle de NAS", juillet 2000. *(Information)*

[RFC2989] B. Aboba et autres, "Critères d'évaluation des protocoles AAA pour l'accès réseau", novembre 2000. *(Info.)*

[RFC3169] M. Beadles, D. Mitton, "Critères d'évaluation des protocoles de serveur d'accès réseau", sept. 2001. *(Info.)*

[RFC3246] B. Davie et autres, "Comportement par bond de transmission accélérée", mars 2002. *(P.S.)*

[RFC3454] P. Hoffman et M. Blanchet, "Préparation de chaînes internationalisées ("stringprep")", décembre 2002. *(P.S.)*

[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)*

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

[RFC3931] J. Lau et autres, "Protocole de tunnelage de couche deux - version 3 (L2TPv3)", mars 2005. *(P.S.)*

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

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

[RFC4301] S. Kent et K. Seo, "Architecture de sécurité pour le protocole Internet", décembre 2005. *(P.S.) (Remplace la* RFC2401)

[RFC5246] T. Dierks, E. Rescorla, "Version 1.2 du protocole de sécurité de la couche Transport (TLS)", août 2008. (*Remplace* RFC3268, RFC4346, RFC4366) (*MàJ* RFC4492) (*MàJ par* RFC5746, RFC5878)*(P.S.)*

Appendice A Remerciements

A.1. Pour ce document

La plus grande partie du texte du présent document a été prise directement de la RFC 4005 ; l'éditeur témoigne de sa gratitude à ses auteurs (en particulier Dave Mitton, qui s'est arrangé pour remettre d'aplomb les tableaux d'occurance des AVP !).

Merci (sans ordre particulier) à Jai-Jin Lim, Liu Hans, Sebastien Decugis, Jouni Korhonen, Mark Jones, Hannes Tschofenig, Dave Crocker, David Black, Barry Leiba, Peter Saint-Andre, Stefan Winter, et Lionel Morand pou leurs utiles relectures et commentaires.

A.2 Pour la RFC 4005

Les auteurs tiennent à remercier Carl Rigney, Allan C. Rubens, William Allen Simpson, et Steve Willens de leur travail sur le protocole RADIUS original, à partir duquel beaucoup des concepts de la présente spécification ont été déduits. Merci aussi à Carl Rigney pour les [RFC2866] et [RFC2869], à Ward Willats pour la [RFC2869], à Glen Zorn, Bernard Aboba, et Dave Mitton pour les [RFC2867] et [RFC3162], et à Dory Leifer, John Shriver, Matt Holdrege, Allan Rubens, Glen Zorn, et Ignacio Goyret pour leur travail sur la [RFC2868]. Le présent document a emprunté du texte et des concepts aux deux [RFC2868] et [RFC2869]. Merci à Carl Williams qui a fourni le texte spécifique pour IPv6.

Les auteurs aimeraient aussi remercier les personnes suivantes de leurs contributions au développement du protocole Diameter : Bernard Aboba, Jari Arkko, William Bulley, Kuntal Chowdhury, Daniel C. Fox, Lol Grant, Nancy Greene, Jeff Hagg, Peter Heitman, Paul Krumviede, Fergal Ladley, Ryan Moats, Victor Muslin, Kenneth Peirce, Sumit Vakil, John R. Vollbrecht, et Jeff Weisberg.

Enfin, Pat Calhoun tient à remercier Sun Microsystems, car la plus grande partie des efforts consacrés au présent document l'ont été lorsque il était leur employé.

Adresse de l'éditeur

Glen Zorn
Network Zen
227/358 Thanon Sanphawut
Bang Na, Bangkok 10260
Thaïlande

téléphone : +66 (0)8-1000-4155
mél : glenzorn@gmail.com