Groupe de travail Réseau
Request for Comments : 4006
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

H. Hakala & L. Mattila, Ericsson
J-P. Koskinen, M. Stura & J. Loughney, Nokia
août 2005

Application de contrôle de crédit Diameter

Résumé
Le présent document spécifie une application Diameter qui peut être utilisée pour mettre en œuvre un contrôle de crédit en temps réel pour divers services d'utilisateur final comme l'accès au réseau, des services du protocole d'initialisation de session (SIP, *Session Initiation Protocol*) des services de messagerie, et des services de téléchargement.

Table des Matières

1. Introduction

Le présent document spécifie une application Diameter qui peut être utilisée pour mettre en œuvre le contrôle de crédit (CC) en temps réel pour divers services d'utilisateur final tels que l'accès réseau, les services du protocole d'initialisation de session (SIP, *Session Initiation Protocol*) des services de messagerie, et des services de téléchargement. Il fournit une solution générale au coût en temps réel et au contrôle de crédit.

Le modèle prépayé s'est révélé un succès, par exemple dans les réseaux GSM, où les opérateurs réseau qui offrent des services prépayés ont constaté une croissance substantielle de leur clientèle et de leurs revenus. Les services prépayés se développent maintenant dans de nombreux autres réseaux sans fil et filaires.

Dans la prochaine génération de réseaux sans fil, une fonction supplémentaire est requise au delà de ce qui est spécifié dans le protocole de base Diameter. Par exemple, les exigences de tarification et de facturation du 3GPP [3GPPCHARG] déclarent qu'une application doit être capable de tarifer en temps réel les informations de service. De plus, il est nécessaire de vérifier que le compte de l'utilisateur final est provisionné pour couvrir le service demandé avant l'initialisation de ce service. Lorsque un compte est épuisé ou expiré, l'utilisateur doit se voir refuser la capacité de consulter des événements facturables supplémentaires.

Un mécanisme doit être fourni pour permettre à l'utilisateur d'être informé des charges qui incombent au service demandé. De plus, il y a des services comme les jeux et la publicité qui peuvent créditer aussi bien que débiter un compte d'utilisateur.

Les autres applications Diameter fournissent une autorisation spécifique du service, et elles ne fournissent pas d'autorisation de crédit pour les usagers prépayés. L'autorisation de crédit devra être générique et applicable à tous les environnements de service exigés pour prendre en charge les services prépayés.

Pour satisfaire à ces exigences, il est nécessaire de faciliter les communications de contrôle de crédit entre les éléments de réseau qui fournissent le service (par exemple, serveur d'accès réseau, mandataire SIP, et serveur d'application) et un serveur de contrôle de crédit.

Le domaine d'application de la présente spécification est l'autorisation de crédit. L'autorisation et l'authentification spécifique du service est en dehors de ce domaine d'application.

1.1 Langage des exigences

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

1.2. Terminologie

AAA : authentification, autorisation, et comptabilité.

Réponse AA : une réponse AA se réfère de façon générique à une réponse à une autorisation et authentification spécifique d'un service. Les commandes de réponse AA sont définies dans des applications d'autorisation spécifiques d'un service, par exemple, les [RFC4004] et [RFC4005].

Demande AA : une demande AA se réfère de façon générique à une demande d'autorisation et authentification spécifique d'un service. Les commandes de demande AA sont définies dans des applications d'autorisation spécifiques d'un service, par exemple, les [RFC4004] et [RFC4005].

Contrôle de crédit : le contrôle de crédit est un mécanisme qui interagit directement en temps réel avec un compte et contrôle ou surveille les charges relatives à l'utilisation du service. Le contrôle de crédit est un processus de vérification de la disponibilité du crédit, de la réservation de crédit, de déduction de crédit du compte de l'utilisateur final lorsque le service est achevé et de remboursement du crédit réservé qui n'est pas utilisé.

Serveur de contrôle de crédit Diameter : un serveur de contrôle de crédit Diameter agit comme un serveur prépayé, effectuant en temps réel la tarification et le contrôle de crédit. Il est situé dans le domaine de rattachement et est accédé par les éléments de service ou serveurs AAA Diameter en temps réel pour les besoins de la détermination des prix et du contrôle de crédit avant que l'événement de service soit livré à l'utilisateur final. Il peut aussi interagir avec des systèmes commerciaux.

Client de contrôle de crédit Diameter : un client de contrôle de crédit Diameter est une entité qui interagit avec un serveur de contrôle de crédit. Il surveille l'usage de la quotité accordée selon les instructions retournées par le serveur de contrôle de crédit.

Interrogation : le client de contrôle de crédit Diameter utilise l'interrogation pour initialiser un processus de contrôle de crédit fondé sur la session. Durant le processus de contrôle de crédit, elle est utilisée pour faire rapport de la quotité utilisée et en demander une nouvelle. Une interrogation se transpose en une transaction de demande/réponse.

Événement unique : fondamentalement, une transaction de demande/réponse d'un type d'événement.

Tarification : acte de détermination du coût d'un événement de service.

Service : type de tâche effectuée par un élément de service pour un utilisateur final.

Élément de service : élément de réseau qui fournit un service aux utilisateurs finaux. L'élément de service peut inclure le client de contrôle de crédit Diameter, ou une autre entité (par exemple, un serveur AAA RADIUS) qui peut agir comme client de contrôle de crédit au nom de l'élément de service. Dans ce dernier cas, l'interface entre l'élément de service et le client de contrôle de crédit Diameter sort du domaine d'application de la présente spécification. Des exemples d'éléments de service incluent le serveur d'accès réseau (NAS, *Network Access Server*), un mandataire SIP, et des serveurs d'application tels qu'un serveur de messagerie, un serveur de contenu, et un serveur de jeux.

Événement de service : événement relatif à un service fourni à l'utilisateur final.

Contrôle de crédit fondé sur la session : processus de contrôle de crédit qui fait usage de plusieurs interrogations : la première, une éventuelle intermédiaire, et la finale. La première interrogation est utilisée pour réserver des fonds sur le compte de l'usager et pour initier le processus. Les interrogations intermédiaires peuvent être nécessaires pour demander une nouvelle quotité pendant que le service est en cours d'exécution. L'interrogation finale est utilisée pour quitter le processus. Il est demandé au serveur de contrôle de crédit de conserver l'état de session pour le contrôle de crédit fondé sur la session.

1.3. Annonce de la prise en charge de l'application

Les nœuds Diameter conformes à la présente spécification DOIVENT annoncer leur prise en charge en incluant la valeur de 4 dans le Auth-Application-Id *(identifiant d'application d'authentification)* des commandes Capabilities-Exchange-Request *(demande d'échange de capacités)* et Capabilities-Exchange-Answer*(réponse d'échange de capacités)* [RFC3588].

2. Modèles d'architecture

Les modèles comptables actuels spécifiés dans la comptabilité Radius [RFC2866] et le protocole Diameter de base [RFC3588] ne sont pas suffisants pour le contrôle de crédit en temps réel, où la validité du crédit doit être déterminée avant l'initialisation du service. Aussi, les applications d'autorisation Diameter existantes, [RFC4004] et [RFC4005], ne fournissent que l'autorisation du service, mais ne fournissent pas d'autorisation de crédit pour les utilisateurs prépayés. Afin de prendre en charge le contrôle de crédit en temps réel, un nouveau type de serveur est nécessaire dans l'infrastructure AAA : le serveur Diameter de contrôle de crédit. Le serveur Diameter de contrôle de crédit est l'entité chargée de l'autorisation de crédit pour les abonnés prépayés.

Un élément de service peut authentifier et autoriser l'utilisateur final auprès du serveur AAA en utilisant les protocoles AAA ; par exemple, RADIUS, ou un protocole Diameter de base avec une application Diameter éventuelle.

Les protocoles de comptabilité comme la comptabilité RADIUS et le protocole comptable Diameter de base peuvent être utilisés pour fournir des données comptables au serveur de comptabilité après l'initialisation du service, et pour fournir un éventuel rapport intérimaire avant l'achèvement du service. Cependant, pour le contrôle de crédit en temps réel, ces modèles d'autorisation et de comptabilité ne sont pas suffisants.

Lorsque le contrôle de crédit en temps réel est exigé, le client de contrôle de crédit contacte le serveur de contrôle de crédit avec des informations sur un possible événement de service. Le processus de contrôle de crédit est effectué pour déterminer les charges potentielles et vérifier si la provision du compte de l'utilisateur final est suffisante pour couvrir le coût du service à rendre.

La Figure 1 illustre l'architecture normale de contrôle de crédit, qui consiste en un élément de service avec un client Diameter de contrôle de crédit, un serveur Diameter de contrôle de crédit, et un serveur AAA. Un système de soutien commercial *(Business Support System)* est généralement déployé ; il comporte au moins la fonction de facturation. Dans ce modèle d'architecture, le serveur de contrôle de crédit et le serveur AAA sont des entités logiques. La configuration réelle peut les combiner en un seul hôte. Le protocole de contrôle de crédit est le protocole Diameter de base avec l'application de contrôle de crédit Diameter.

Lorsque un utilisateur final demande des services tels que SIP ou de la messagerie, la demande est normalement transmise à un élément de service (par exemple, un mandataire SIP) dans le domaine de rattachement de l'utilisateur. Dans certains cas, il est possible que l'élément de service dans le domaine visité puisse offrir des services à l'utilisateur final ; cependant, un accord commercial doit exister entre le domaine visité et le domaine de rattachement. L'accès au réseau est un exemple de service offert dans le domaine visité où le serveur d'accès réseau (NAS, *Network Access Server*) à travers une infrastructure AAA, authentifie et autorise l'usager auprès du réseau de rattachement de l'usager.

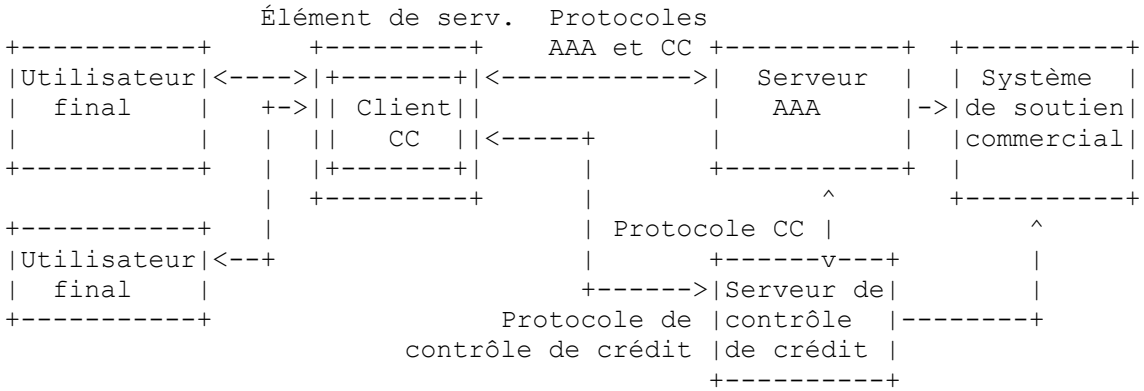


Figure 1 : Architecture typique de contrôle de crédit

Il peut y avoir plusieurs serveurs de contrôle de crédit dans le système pour la redondance et l'équilibrage de charge. Le système peut aussi contenir un ou des serveurs de facturation séparés, et la comptabilité peut être située dans une base de données centralisée. Pour s'assurer que le compte de l'utilisateur final n'est pas débité ou crédité plusieurs fois pour le même événement de service, un seul endroit du système de contrôle de crédit devrait effectuer la détection des duplications. Il peut exister des interfaces internes du système pour relayer les messages entre serveurs et gestionnaire de compte. Cependant, l'architecture détaillée du système de contrôle de crédit et ses interfaces sont spécifiques de la mise en œuvre et sortent du domaine d'application de la présente spécification.

Des relais Diameter transparents au protocole peuvent exister entre le client de contrôle de crédit et le serveur de contrôle

de crédit. Il peut exister aussi des agents de redirection Diameter qui renvoient les clients de contrôle de crédit aux serveurs de contrôle de crédit et leur permettent de communiquer directement. Ces agents prennent en charge de façon transparente l'application Diameter de contrôle de crédit. Les différents rôles d'agents Diameter sont définis au paragraphe 2.8 du protocole Diameter de base [RFC3588].

Si il existe des mandataires Diameter de contrôle de crédit entre le client de contrôle de crédit et le serveur de contrôle de crédit, ils DOIVENT annoncer la prise en charge de l'application Diameter de contrôle de crédit.

3. Messages de contrôle de crédit

Cette section définit les nouvelles valeurs du message Command-Code Diameter qui DOIVENT être prises en charge par toutes les mises en œuvre Diameter qui se conforment à la présente spécification. Les codes de commandes sont les suivants :

Nom de commande	**Abréviation**	**Code**	**Référence**
Credit-Control-Request *(demande de contrôle de crédit)*	CCR	272	3.1
Credit-Control-Answer *(réponse de contrôle de crédit)*	CCA	272	3.2

Le protocole Diameter de base [RFC3588] définit au paragraphe 3.2 la spécification ABNF des codes de commandes. Ces formats sont observés dans les messages de contrôle de crédit.

3.1 Commande Credit-Control-Request (CCR)

Le message Demande de contrôle de crédit (CCR, *Credit-Control-Request*) est indiqué par le champ Code de commande réglé à 272 et le bit 'R' établi dans le champ Fanions de commandes. Il est utilise entre le client Diameter de contrôle de crédit et le serveur de contrôle de crédit pour demander une autorisation de crédit pour un certain service.

Le Auth-Application-Id DOIT être réglé à la valeur 4, indiquant l'application Diameter de contrôle de crédit.

Format de message :

<Credit-Control-Request> ::= < en-tête Diameter: 272, REQ, PXY >
< Session-Id > *(identifiant de session)*
{ Origin-Host } *(hôte d'origine)*
{ Origin-Realm } *(domaine d'origine)*
{ Destination-Realm } *(domaine de destination)*
{ Auth-Application-Id } *(identifiant d'application d'authentification)*
{ Service-Context-Id } *(identifiant de contexte de service)*
{ CC-Request-Type } *(type de demande de contrôle de crédit)*
{ CC-Request-Number } *(numéro de demande de contrôle de crédit)*
[Destination-Host] *(hôte de destination)*
[User-Name] *(nom d'utilisateur)*
[CC-Sub-Session-Id] *(identifiant de sous session de contrôle de crédit)*
[Acct-Multi-Session-Id] *(identifiant de session multiple de comptabilité)*
[Origin-State-Id] *(identifiant d'état d'origine)*
[Event-Timestamp] *(horodatage d'événement)*
*[Subscription-Id] *(identifiant d'abonnement)*
[Service-Identifier] *(identifiant de service)*
[Termination-Cause] *(cause de fin)*
[Requested-Service-Unit] *(unité de service demandé)*
[Requested-Action] *(action demandée)*
*[Used-Service-Unit] *(unités de service utilisées)*
[Multiple-Services-Indicator] *(indicateur de services multiples)*
*[Multiple-Services-Credit-Control] *(contrôle de crédit de services multiples)*
*[Service-Parameter-Info] *(informations de paramètres de service)*
[CC-Correlation-Id] *(identifiant de corrélation de contrôle de crédit)*
[User-Equipment-Info] *(informations d'équipement d'utilisateur)*
*[Proxy-Info] *(informations de mandataire)*
*[Route-Record] *(enregistrement de chemin)*
*[AVP]

3.2 Commande Credit-Control-Answer (CCA)

Le message Réponse de contrôle de crédit (CCA, *Credit-Control-Answer*) est indiqué par le champ de code de commande réglé à 272 et le bit 'R' à zéro dans le champ Fanions de commande. Il est utilisé entre le serveur de contrôle de crédit et le client Diameter de contrôle de crédit pour accuser réception d'une commande Credit-Control-Request.

Format de message :

<Credit-Control-Answer> ::= < en-tête Diameter: 272, PXY >
< Session-Id >
{ Result-Code } *(code de résultat)*
{ Origin-Host }
{ Origin-Realm }
{ Auth-Application-Id }
{ CC-Request-Type }
{ CC-Request-Number }
[User-Name]
[CC-Session-Failover] *(reprise sur échec de session de contrôle de créait)*
[CC-Sub-Session-Id]
[Acct-Multi-Session-Id]
[Origin-State-Id]
[Event-Timestamp]
[Granted-Service-Unit] *(unités de service accordées)*
*[Multiple-Services-Credit-Control]
[Cost-Information] *(informations de coût)*
[Final-Unit-Indication] *(indication des unités finales)*
[Check-Balance-Result] *(résultat de la vérification du solde)*
[Credit-Control-Failure-Handling] *(traitement d'échec de contrôle de crédit)*
[Direct-Debiting-Failure-Handling] *(traitement d'échec de débit direct)*
[Validity-Time] *(durée de validité)*
*[Redirect-Host] *(hôte de redirection)*
[Redirect-Host-Usage] *(utilisation d'hôte de redirection)*
[Redirect-Max-Cache-Time] *(durée maximale de conservation d'hôte de redirection en antémémoire)*
*[Proxy-Info] *(informations de mandataire)*
*[Route-Record] *(enregistrement de chemin)*
*[Failed-AVP] *(AVP en échec)*
*[AVP]

4. Vue d'ensemble de l'application de contrôle de crédit

Le processus d'autorisation de crédit a lieu avant et durant la livraison du service à l'utilisateur final et exige généralement l'authentification et l'autorisation de l'usager avant qu'aucune demande soit envoyée au serveur de contrôle de crédit. L'application de contrôle de crédit définie dans la présente spécification prend en charge deux modèles différents d'autorisation de crédit : l'autorisation de crédit avec réservation de fonds et l'autorisation de crédit avec débit direct. Dans les deux modèles, le client de contrôle de crédit demande une autorisation de crédit au serveur de contrôle de crédit avant de permettre qu'un service soit livré à l'utilisateur final.

Dans le premier modèle, le serveur de contrôle de crédit tarifie la demande, réserve un montant convenable sur le compte de l'usager, et retourne la quantité correspondante de ressources de crédit. Noter que les ressources de crédit peuvent ne pas impliquer un crédit monétaire réel ; les ressources de crédit peuvent être accordées au client de contrôle de crédit sous la forme d'unités (par exemple, un volume de données ou de temps) à mesurer.

À réception d'une réponse d'autorisation de crédit réussie avec un certain montant de ressources de crédit, le client de contrôle de crédit permet la livraison du service à l'utilisateur final et commence à surveiller l'utilisation des ressources accordées. Lorsque les ressources de crédit accordées à l'utilisateur ont été consommées ou que le service a été livré avec succès ou s'est terminé, le client de contrôle de crédit fait rapport au serveur du montant utilisé. Le serveur de contrôle de crédit déduit le montant utilisé du compte de l'utilisateur final ; il peut effectuer la tarification et faire une nouvelle réservation de crédit si la livraison du service se poursuit. Ce processus est accompli avec le contrôle de crédit fondé sur la session qui inclut la première interrogation, d'éventuelles interrogations intermédiaires, et l'interrogation finale. Pour le contrôle de crédit fondé sur la session, le client de contrôle de crédit et le serveur de contrôle de crédit sont tous deux obligés de conserver l'état de session du contrôle de crédit. Le contrôle de crédit fondé sur la session est décrit plus en détails, avec plus de variantes, à la Section 5.

Par contre, l'autorisation de crédit avec débit direct est un processus d'une seule transaction dans lequel le serveur de contrôle de crédit déduit directement une somme convenable du compte de l'utilisateur aussitôt qu'est reçue la demande d'autorisation de crédit. À réception d'une réponse d'autorisation de crédit positive, le client de contrôle de crédit permet la livraison du service à l'utilisateur final. Ce processus est réalisé avec l'événement unique. L'état de session n'est pas conservé.

Dans un environnement multi services, un utilisateur final peut produire une demande de service supplémentaire (par exemple, de service de données) durant un service en cours (par exemple, appel vocal) sur le même compte. Autrement, durant une session multimédia active, un type de support supplémentaire est ajouté à la session, causant une nouvelle demande simultanée sur le même compte. Par conséquent, ceci doit être pris en compte lorsque des ressources de crédit sont affectées aux services.

L'application de contrôle de crédit prend aussi en charge des opérations comme l'enquête sur le prix du service, la vérification de l'existence de provisions sur le compte de l'usager, et le reversement du solde créditeur sur le compte de l'utilisateur. Ces opérations sont réalisées avec l'événement unique. L'état de session n'est pas conservé.

Un traitement souple des défaillances spécifiques des applications de contrôle de crédit est défini, dans lequel le fournisseur de service de rattachement peut modéliser le comportement du client de contrôle de crédit selon sa propre politique de gestion des risques de crédit.

L'AVP Credit-Control-Failure-Handling (*traitement de défaillance de contrôle de crédit*) et l'AVP Direct-Debiting-Failure-Handling *(traitement d'échec de débit direct)* sont définies pour déterminer ce qui est fait si l'envoi de messages de contrôle de crédit au serveur de contrôle de crédit a été temporairement empêché. L'usage des AVP Credit-Control-Failure-Handling et Direct-Debiting-Failure-Handling permet une certaine souplesse, car le traitement des défaillances peut être différent pour la session de contrôle de crédit et celle de débit direct d'événement unique.

4.1 Entrées et interopérabilité de tarification spécifique du service

L'application Diameter de contrôle de crédit définit le cadre du contrôle de crédit ; elle fournit des mécanismes génériques de contrôle de crédit qui prennent en charge plusieurs applications de service. L'application de contrôle de crédit ne définit donc pas les AVP qui pourraient être utilisées comme entrées dans le processus de tarification. Faire la liste des services possibles qui pourraient utiliser cette application Diameter sort du domaine d'application de ce mécanisme générique.

Il est raisonnable de s'attendre à ce qu'un accord de niveau de service existe entre les fournisseurs de client de contrôle de crédit et le serveur de contrôle de crédit couvrant la facturation, les services offerts, les accords d'itinérance, les entrées de facturation acceptées (c'est-à-dire, les AVP), et ainsi de suite.

Donc, on suppose qu'un serveur de contrôle de crédit Diameter ne fournira le service qu'aux clients de contrôle de crédit Diameter qui sont acceptés à l'avance quant au contenu des messages de contrôle de crédit. Naturellement, il est possible que tout client de contrôle de crédit Diameter puisse échanger des messages de contrôle de crédit avec tout serveur de contrôle de crédit Diameter, mais avec une plus forte probabilité que les services/AVP non pris en charge puissent être présents dans le message de contrôle de crédit, causant le rejet par le serveur de la demande avec un code de résultat approprié.

4.1.1 Spécification des AVP d'entrées de tarification

Il y a deux façons de fournir des entrées de facturation au serveur de contrôle de crédit : soit en utilisant les AVP, soit en les incluant dans l'AVP Service-Parameter-Info *(informations de paramètres de service)*. Les principes généraux d'envoi des paramètres de facturation sont les suivants :

1a. Le service DEVRAIT réutiliser les AVP existantes si il peut utiliser les AVP définies dans les applications Diameter existantes (par exemple, NASREQ pour les services d'accès réseau). La réutilisation des AVP existantes est fortement recommandée dans la [RFC3588]. Pour les AVP de type Enumerated, le service peut exiger qu'une nouvelle valeur soit définie. L'allocation de nouvelles valeurs d'AVP est faite comme spécifié au paragraphe 1.2 de la [RFC3588].

1b. De nouvelles AVP peuvent être définies si les AVP existantes ne donnent pas des informations de tarification suffisantes. Dans ce cas, les procédures définies dans la [RFC3588] pour créer de nouvelles AVP DOIVENT être suivies.

1c. Pour les services spécifiques d'une seule mise en œuvre de fabricant, un code d'AVP Vendor-Specific pour utilisation privée peut être utilisé. Lorsque une AVP Vendor-Specific est mise en œuvre par plus d'un fabricant, l'allocation des AVP globales est plutôt encouragée ; voir la [RFC3588].

2. L'AVP Service-Parameter-Info PEUT être utilisée comme conteneur pour passer les informations de tarification traditionnelles dans leur forme codée originale (par exemple, BER ASN.1). Cette méthode peut être utilisée pour éviter des conversions inutiles d'une format de données existant à un format d'AVP. Dans ce cas, l'entrée de tarification est incorporée dans l'AVP Service-Parameter-Info comme défini au paragraphe 8.43.

De nouvelles applications de service DEVRAIENT favoriser l'utilisation d'AVP explicitement définies, comme décrit aux points 1a et 1b, pour simplifier l'interopérabilité.

4.1.2 Documentation spécifique du service

Les AVP d'entrée de tarification spécifiques du service, le contenu de l'AVP Service-Parameter-Info ou Service-Context-Id (définie au paragraphe 8.42) sortent du domaine d'application du présent document. Pour faciliter l'interopérabilité, il est RECOMMANDÉ que les entrées de tarification et les valeurs de Service-Context-Id soient coordonnées via une RFC pour information ou une autre référence permanente et directement disponible. La spécification d'un autre organisme de normalisation coopératif (par exemple, 3GPP, OMA, et 3GPP2) DEVRAIT être utilisée. Cependant, des services privés peuvent être déployés qui sont soumis à des accords entre les fournisseurs de serveur et clients de contrôle de crédit. Dans ce cas, des AVP spécifiques de fabricants peuvent être utilisées.

La présente spécification, avec les documents spécifiques de service ci-dessus, gouverne le message de contrôle de crédit. Des documents spécifiques des services définissent quelles AVP existantes ou nouvelles sont utilisées comme entrées du processus de tarification (c'est-à-dire, celles qui ne définissent pas de nouvelles applications de contrôle de crédit) et donc doivent être incluses dans la commande Credit-Control-Request par un client de contrôle de crédit Diameter qui prend en charge un certain service comme *[AVP]. Si Service-Parameter-Info devait être utilisée, le document spécifique du service DEVRAIT spécifier le contenu exact de cette AVP groupée.

L'AVP Service-Context-Id DOIT être incluse au niveau commande d'une demande de contrôle de crédit pour identifier le document spécifique du service qui s'applique à la demande. Le service ou groupe de tarifs spécifique auquel se rapporte la demande est identifié de façon univoque par la combinaison de Service-Context-Id et Service-Identifier ou Rating-Group.

4.1.3 Traitement des entrées le tarification non prises en charge/incorrectes

Il est exigé des mises en œuvre de contrôle de crédit Diameter qu'elles prennent en charge les AVP de tarification obligatoires définies dans la documentation spécifique des services qu'elles soutiennent, conformément au règles sur le bit 'M' de la [RFC3588].

Si une entrée de tarification nécessaire au processus de tarification est incorrecte dans la demande de contrôle de crédit, ou si le serveur de contrôle de crédit ne prend pas en charge le contexte de service demandé (identifié par l'AVP Service-Context-Id au niveau commande) la réponse de contrôle de crédit DOIT contenir le code d'erreur DIAMETER_RATING_FAILED. Un message CCA avec cette erreur DOIT contenir une ou plusieurs AVP Failed-AVP contenant les AVP manquantes et/ou non prises en charge qui ont causé la défaillance. Un client de contrôle de crédit Diameter qui reçoit le code d'erreur DIAMETER_RATING_FAILED en réponse à une demande NE DOIT PAS envoyer de telles demandes à l'avenir.

4.1.4 Attributs RADIUS de tarification spécifiques du fabricant

Lorsque des documents spécifiques d'un service incluent des attributs RADIUS spécifiques de fabricant qui pourraient être utilisés comme entrées dans le processus de tarification, les règles décrites dans la [RFC4005] pour formater l'AVP Diameter DOIVENT être suivies.

Par exemple, si le code d'AVP utilisé est le code de type d'attribut de fabricant, le fanion Vendor-Specific DOIT être réglé à 1 et le Vendor-ID DOIT être réglé à la valeur d'identification de fabricant de l'IANA. Le champ AVP Diameter contient seulement la valeur d'attribut de l'attribut RADIUS.

5. Contrôle de crédit fondé sur la session

5.1 Principes généraux

Pour un contrôle de crédit fondé sur la session, plusieurs interrogations sont nécessaires : la première, les interrogations intermédiaires (facultatives) et l'interrogation finale. Ceci est illustré aux Figures 2 et 3.

Si le client de contrôle de crédit effectue une réservation de crédit avant d'accorder le service à l'utilisateur final, il DOIT utiliser plusieurs interrogations au serveur de contrôle de crédit (c'est-à-dire, le contrôle de crédit fondé sur la session). Dans ce cas, le serveur de contrôle de crédit DOIT conserver l'état de la session de contrôle de crédit.

Chaque session de contrôle de crédit DOIT avoir un identifiant de session unique au monde, comme défini dans la [RFC3588], qui NE DOIT PAS être changé durant la durée de vie d'une session de contrôle de crédit.

Certaines applications requièrent plusieurs sous sessions de contrôle de crédit. Ces applications vont envoyer des messages avec une AVP Session-Id constante, mais avec une AVP CC-Sub-Session-Id différente. Si plusieurs sous sessions de crédit sont utilisées, toutes les sous sessions DOIVENT être closes séparément avant que la session principale soit close afin que les unités par sous session puissent être rapportées. L'absence de cette AVP implique qu'aucune sous session n'est utilisée.

Noter que l'élément de service peut envoyer un message de réautorisation spécifique du service au serveur AAA à cause de l'expiration de la durée de vie de l'autorisation durant une session de contrôle de crédit en cours. Cependant, la réautorisation spécifique de service n'influence pas l'autorisation de crédit qui est en cours entre le client de contrôle de crédit et le serveur de contrôle de crédit, car l'autorisation de crédit est contrôlée par le taux de consommation de la quotité allouée.

Si la réautorisation spécifique du service échoue, l'utilisateur sera déconnecté, et le client de contrôle de crédit DOIT envoyer une interrogation finale au serveur de contrôle de crédit.

Le serveur de contrôle de crédit Diameter peut chercher à contrôler la pérennité de la validité de la quotité accordée et/ou la production d'interrogations intermédiaires. Donc, il PEUT inclure l'AVP Validity-Time dans le message de réponse au client de contrôle de crédit. À l'expiration de la durée de validité, le client de contrôle de crédit DOIT générer une demande de mise à jour de contrôle de crédit et rapporter la quotité utilisée au serveur de contrôle de crédit. Il appartient au serveur de contrôle de crédit de déterminer la valeur de Validity-Time à utiliser pour la consommation des unités de service accordées. Si Validity-Time est utilisée, sa valeur DEVRAIT être donnée en entrée pour régler le temporisateur de supervision de session Tcc (le temporisateur de supervision de session PEUT être réglé à deux fois la valeur de Validity-Time, comme défini à la Section 13). Comme les demandes de mise à jour de contrôle de crédit sont aussi produites à l'expiration des unités de service accordées et/ou pour des événements de service à mi session, l'omission de Validity-Time ne signifie pas que ne sont pas effectuées des interrogations intermédiaires pour les besoins du contrôle de crédit.

5.1.1. Prise en charge des changements des horaires de tarif de base

Le serveur et le client de contrôle de crédit Diameter PEUVENT facultativement prendre en charge un mécanisme de changement de tarif. Le serveur de contrôle de crédit Diameter peut inclure une AVP Tariff-Time-Change dans le message de réponse. Noter que les unités accordées devraient être allouées sur la base du scénario de plus mauvais cas pour le changement de tarif à venir, afin que les unités utilisées rapportées globales n'excèdent jamais la réservation de crédit.

Lorsque le client de contrôle de crédit Diameter rapporte les unités utilisées et qu'un changement de tarif s'est produit durant la période de rapport, le client de contrôle de crédit Diameter DOIT individualiser séparément les unités utilisées avant et après le changement de tarif. Si le client est incapable de distinguer si des unités enjambant le changement de tarif ont été utilisées avant ou après le changement de tarif, le client de contrôle de crédit DOIT individualiser ces unités dans une troisième catégorie.

Si un client ne prend pas en charge le mécanisme de changement de tarif, et si il reçoit un message CCA portant l'AVP Tariff-Time-Change, il DOIT terminer la session de contrôle de crédit, en donnant dans l'AVP Termination-Cause une raison de DIAMETER_BAD_ANSWER *(mauvaise réponse Diameter)*.

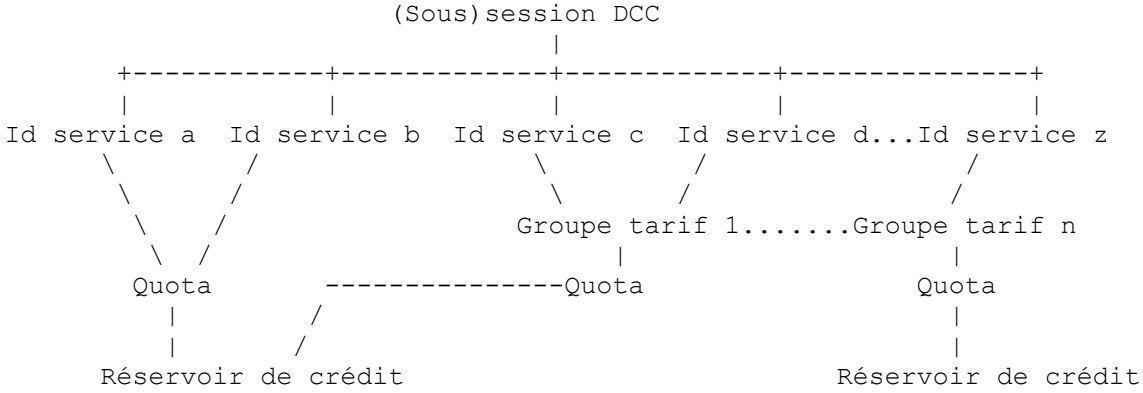
Pour les services fondés sur le temps, le quota est consommé en continu au taux régulier de 60 secondes par minute. Au moment où les ressources de crédit sont allouées, le serveur sait déjà combien d'unités seront consommées avant que l'heure du tarif change et combien d'unités seront consommées ensuite. De même, le serveur peut déterminer les unités consommées au taux d'avant et les unités consommées au taux d'après pour le cas où l'utilisateur final clôturerait la session avant la consommation de la quotité allouée. Il n'y a pas besoin de trafic supplémentaire entre le client et le serveur dans le cas de changements du tarif horaire pour le service fondé sur une durée continue. Donc, le mécanisme de changement de tarif n'est pas utilisé pour de tels services. Pour les services fondés sur le temps où le quota N'EST PAS consommé en continu à un taux régulier, le mécanisme de changement de tarif décrit pour les unités de volume et d'événement PEUT être utilisé.

5.1.2 Contrôle de crédit pour plusieurs services dans une (sous-)session

Lorsque plusieurs services sont utilisés dans la même session d'utilisateur et que chaque service ou groupe de services a un coût différent, il est nécessaire d'effectuer un contrôle de crédit indépendant pour chaque service. L'utilisation de sous sessions de contrôle de crédit pour réaliser un contrôle de crédit indépendant va avoir pour résultat une charge accrue de signalisation et d'usage de ressources à la fois chez le client et chez le serveur de contrôle de crédit. Par exemple, durant une session d'accès réseau, l'utilisateur final peut utiliser plusieurs services HTTP soumis à des coûts d'accès différents. Les attributs spécifiques de l'accès réseau comme la qualité de service (QS) sont communs à tous les services portés dans le support d'accès, mais le coût du support peut varier selon son contenu.

Pour optimiser la prise en charge de ces scénarios, l'application de contrôle de crédit permet un contrôle de crédit indépendant de plusieurs services dans une seule (sous) session de contrôle de crédit. Cela se fait en incluant l'AVP facultative Multiple-Services-Credit-Control dans les messages Credit-Control-Request/Answer. Il est possible de demander et allouer des ressources comme un réservoir de crédit partagé entre de multiples services. Les services peuvent être groupés en groupes de niveau de prix afin de réaliser encore plus d'agrégation d'allocation de crédit. Il est aussi possible de demander et allouer des quotas sur la base du service. Lorsque des quotas sont alloués à un réservoir au moyen de l'AVP Multiple-Services-Credit-Control, les quotas restent des objets indépendants qui peuvent être réautorisés indépendamment à tout moment. Les quotas peuvent aussi recevoir des codes de résultat, des durées de validité et des Final-Unit-Indications indépendants.

Un groupe de tarification *(Rating-Group)* regroupe un ensemble de services, identifiés par un identifiant de service *(Service-Identifier)*, et soumis au même type de coût et de tarif (par exemple, 0,1 €/minute). On suppose que l'élément de service a reçu des groupes de tarification, des identifiants de service, et leurs paramètres associés qui définissent ce qui doit être mesuré par des moyens qui sortent du domaine d'application de la présente spécification. (Des exemples de paramètres associés aux identifiants de service sont des quintuplets IP et des URL HTTP.) Les identifiants de service permettent l'autorisation du crédit sur la base du service ainsi que le rapport élément par élément de l'utilisation du service. Il appartient au serveur de contrôle de crédit d'autoriser ou non le crédit pour un ou plusieurs services ou pour l'ensemble du groupe de tarification. Cependant, le client DEVRAIT toujours faire rapport des unités utilisées au plus fin niveau de granularité pris en charge. Lorsque un quota est alloué à un groupe de tarification, tous les services qui appartiennent à ce groupe tirent sur le quota alloué. Voici une représentation graphique des relations entre les identifiants de service, les groupes de tarification, les réservoirs de crédit, et les (sous) sessions de contrôle de crédit.



Si on utilise un contrôle de crédit indépendant de plusieurs services, la durée de validité et l'indication d'unité finale DEVRAIENT être présentes soit dans la ou les AVP Multiple-Services-Credit-Control, soit au niveau commande comme des AVP seules. Cependant, l'AVP Result-Code PEUT être présente à la fois au niveau commande et dans l'AVP Multiple-Services-Credit-Control. Si le code de résultat sur le niveau commande indique une valeur autre que SUCCÈS, le code de résultat au niveau commande prend la préséance sur tout ce qui est inclus dans l'AVP Multiple-Services-Credit-Control.

Le client de contrôle de crédit DOIT indiquer la prise en charge du contrôle de crédit indépendant de plusieurs services dans une (sous) session en incluant l'AVP Multiple-Services-Indicator dans la première interrogation. Un serveur de contrôle de crédit qui ne prend pas en charge cette caractéristique DOIT traiter l'AVP Multiple-Services-Indicator et tous AVP Multiple-Services-Credit-Control reçus comme des AVP invalides.

Si le client a indiqué la prise en charge du contrôle de crédit indépendant de plusieurs services, un serveur de contrôle de crédit qui souhaite utiliser la caractéristique DOIT retourner les unités accordées dans l'AVP Multiple-Services-Credit-Control associée à l'identifiant de service et/ou groupe de tarification correspondants.

Pour éviter une situation où plusieurs réservations de crédit parallèles (et aussi normalement petites) doivent être faites sur le même compte (c'est-à-dire, fragmentation de crédit) et aussi pour éviter de charger inutilement le serveur de contrôle de crédit, il est possible de fournir des unités de service comme un réservoir qui s'applique à plusieurs services ou groupes de

tarification. Cela se fait en fournissant les unités de service sous la forme d'un quota pour un service ou groupe de tarification particulier dans l'AVP Multiple-Services-Credit-Control, et aussi en incluant une référence à un réservoir de crédit pour ce type d'unités.

La référence inclut un multiplicateur dérivé du paramètre de tarification, qui traduit les unités de service d'un type spécifique en les unités de service abstraites du réservoir. Par exemple, si le paramètre de tarification pour le service 1 est 1 €/Moctet et si le paramètre de tarification pour le service 2 est 0,5 €/Moctet, les multiplicateurs pourraient être respectivement 10 et 5 pour les services 1 et 2.

Si S est le total des unités de service dans le réservoir, M1, M2, ..., Mn sont les multiplicateurs fournis pour les services 1, 2, ..., n, et C1, C2, ..., Cn sont les ressources utilisées dans la session, alors le crédit du réservoir est épuisé et une réautorisation DOIT être demandée quand : $C1*M1 + C2*M2 + ... + Cn*Mn \geq S$

Le crédit total du réservoir, S, est calculé à partir des quotas, qui sont actuellement alloués comme suit au réservoir :

$$S = Q1*M1 + Q2*M2 + ... + Qn*Mn$$

Si des services ou groupes de tarification sont ajoutés ou supprimés au réservoir, le crédit total est alors ajusté de façon appropriée. Noter que lorsque le crédit total est ajusté à cause de la suppression de services ou groupes de tarification du réservoir, la valeur qui doit être retirée est celle consommée (c'est-à-dire, Cx*Mx).

Les réautorisations pour un service ou groupe de tarification individuel peuvent être demandées à tout moment ; par exemple, si un quota "hors réservoir" est utilisé ou si la durée de validité expire.

Lorsque plusieurs AVP G-S-U-Pool-Reference (paragraphe 8.30) avec le même G-S-U-Pool-Identifier sont fournies dans une AVP Multiple-Services-Credit-Control (paragraphe 8.16) avec l'AVP Granted-Service-Unit, elles DOIVENT alors avoir des valeurs différentes de CC-Unit-Type, et elles tirent toutes séparément sur le réservoir de crédit. Par exemple, si un multiplicateur pour l'instant (M1t) et un multiplicateur pour le volume (M1v) sont donnés, les ressources utilisées du réservoir sont alors la somme C1t*M1t + C1v*M1v, où C1t est l'unité de temps et C1v est l'unité de volume.

Lorsque les unités de service sont fournies dans une AVP Multiple-Services-Credit-Control sans une AVP G-S-U-Pool-Reference correspondante, elles sont alors traitées indépendamment de tout réservoir de crédit et de tout autre service ou groupe de tarification dans la session.

Le concept de réservoir de crédit est un outil optimal pour éviter un effet de sur réservation par le mécanisme de base de changement d'heure de tarif à un seul quota (le mécanisme décrit au paragraphe 5.1.1). Donc, les clients et serveurs de contrôle de crédit Diameter qui mettent en œuvre le contrôle de crédit indépendant de multiples services DEVRAIENT utiliser le concept de réservoir de crédit lorsque ils prennent en charge le changement d'heure de tarif. Le serveur de contrôle de crédit Diameter DEVRAIT inclure les deux AVP Tariff-Time-Change et Tariff-Change-Usage dans deux allocations de quotas dans le message de réponse (c'est-à-dire, deux instances de l'AVP Multiple-Services-Credit-Control). Une des unités accordées est allouée pour être utilisée avant le changement de tarif potentiel, tandis que la seconde est à utiliser après. Les deux quotas d'unités accordés DOIVENT contenir le même identifiant de service et/ou groupe de tarification. Ce mécanisme de double quotas assure que les unités utilisées rapportées globales ne vont jamais excéder la réservation de crédit. Le client de contrôle de crédit Diameter rapporte les deux unité utilisées avant et après le changement de tarif dans une seule instance d'AVP Multiple-Services-Credit-Control.

Le traitement de l'échec des sessions de contrôle de crédit est défini au paragraphe 5.7 et reflété dans l'automate à états de contrôle de crédit de base à la Section 7. Les clients et serveurs de contrôle de crédit qui mettent en œuvre le contrôle de crédit indépendant de multiples services dans une fonctionnalité de (sous) session DOIVENT s'assurer que le traitement des défaillances et le comportement général sont en pleine cohérence avec les paragraphes mentionnés ci dessus, tout en maintenant la capacité de traiter en parallèle la réautorisation de crédit en cours dans une (sous) session. Donc, il est RECOMMANDÉ que les clients de contrôle de crédit Diameter tiennent une file d'attente de messages PendingU et relancent le temporisateur Tx (Section 13) chaque fois qu'un message CCR de valeur UPDATE_REQUEST est envoyé quand ils sont dans un état PendingU. Lorsque des réponses à tous les messages en instance ont été reçues, l'automate à états passe à l'état OPEN, et Tx est arrêté. Naturellement, l'action effectuée lorsque est détecté un problème sur la session selon le paragraphe 5.7 affecte tous les services en cours (par exemple, une reprise sur défaillance sur un serveur de secours si c'est possible affecte tous les messages CCR de la valeur UPDATE_REQUEST dans la file d'attente PendingU).

Comme le client peut envoyer des messages CCR de valeur UPDATE_REQUEST dans l'état PendingU (c'est-à-dire, sans attendre une réponse à la réautorisation de crédit en cours) l'espace entre ces demandes peut être très bref, et le serveur peut n'avoir pas encore reçu la ou les réponses précédentes. Donc, dans cette situation, le serveur peut recevoir des demandes déclassées et NE DEVRAIT PAS considérer cela comme une condition d'erreur. Une réponse appropriée doit être retournée pour chacune de ces demandes.

5.2 Première interrogation

Lorsque le contrôle de crédit fondé sur la session est exigé (par exemple, le serveur d'authentification a indiqué un utilisateur prépayé) la première interrogation DOIT être envoyée avant que le client de contrôle de crédit Diameter permette un événement de service à l'utilisateur final. Le CC-Request-Type est réglé à la valeur INITIAL_REQUEST dans le message de demande.

Si le client de contrôle de crédit Diameter connaît le coût de l'événement de service (par exemple, un serveur de contenu qui délivre des tonalités d'appel connaît leur coût) la quantité monétaire à facturer est incluse dans l'AVP Requested-Service-Unit. Si le client de contrôle de crédit Diameter ne connaît pas le coût de l'événement de service, l'AVP Requested-Service-Unit PEUT contenir le nombre d'événements de service incorporés. Lorsque l'AVP Multiple-Services-Credit-Control est utilisée, elle DOIT contenir l'AVP Requested-Service-Unit pour indiquer que le quota pour le service/groupe de tarification associé est demandé. Dans le cas de services multiples, l'AVP Service-Identifier ou l'AVP Rating-Group au sein de l'AVP Multiple-Services-Credit-Control indique toujours le service concerné. Des informations supplémentaires d'événement de service à facturer PEUVENT être envoyées comme AVP spécifiques du service ou PEUVENT être envoyées au sein de l'AVP Service-Parameter-Info au niveau commande. L'AVP Service-Context-Id indique le document spécifique du service applicable à la demande.

L'AVP Event-Timestamp DEVRAIT être incluse dans la demande et contenir l'heure à laquelle l'événement de service est demandé dans l'élément de service. L'AVP Subscription-Id DEVRAIT être incluse pour identifier l'utilisateur final au serveur de contrôle de crédit. Le client de contrôle de crédit PEUT inclure l'AVP User-Equipment-Info afin que le serveur de contrôle de crédit ait des indications sur le type et les capacités de l'appareil d'accès de l'utilisateur final. Comment le serveur de contrôle de crédit utilise ces informations sort du domaine d'application du présent document.
Le serveur de contrôle de crédit DEVRAIT tarifer l'événement de service et faire une réservation de crédit à partir du compte de l'utilisateur final qui couvre le coût de l'événement de service. Si le type de l'AVP Requested-Service-Unit est monétaire, aucune tarification n'est nécessaire, mais le montant monétaire correspondant est réservé sur le compte de l'utilisateur final.
Le serveur de contrôle de crédit retourne l'AVP Granted-Service-Unit dans le message de réponse au client de contrôle de crédit Diameter. L'AVP Granted-Service-Unit contient la quantité d'unités de service que le client de contrôle de crédit Diameter peut fournir à l'utilisateur final jusqu'à ce qu'une nouvelle Credit-Control-Request DOIVE être envoyée au serveur de contrôle de crédit. Si plusieurs types d'unités sont envoyés dans le message de réponse, le client de contrôle de crédit DOIT traiter chaque type d'unité séparément. Le type de l'AVP Granted-Service-Unit peut être du temps, du volume, spécifique du service, ou de l'argent, selon le type d'événement de service. Le ou les types d'unités NE DEVRAIENT PAS être changés au sein d'une session de contrôle de crédit en cours.

Il DOIT y avoir un maximum d'une instance du même type d'unité dans un message de réponse. Cependant, si plusieurs quotas sont portés au client de contrôle de crédit dans des AVP Multiple-Services-Credit-Control, il est possible de porter deux instances du même type d'unité associées à un identifiant de service/groupe de tarification. C'est normalement le cas lorsque un changement d'heure de tarif est attendu et que le serveur de contrôle de crédit veut faire une distinction entre le quota accordé avant et après le changement de tarif.

Si le serveur de contrôle de crédit détermine qu'aucun autre contrôle n'est nécessaire pour le service, il PEUT inclure le code de résultat qui indique que le contrôle de crédit n'est pas applicable (par exemple, si le service est gratuit). Ce code de résultat au niveau commande implique que la session de contrôle de crédit va se terminer.

Le message Credit-Control-Answer PEUT aussi inclure l'AVP Final-Unit-Indication pour indiquer que le message de réponse contient les unités finales pour le service. Après que l'utilisateur final a consommé ces unités, le client de contrôle de crédit Diameter DOIT se comporter comme décrit au paragraphe 5.6.

Le présent document définit deux approches différentes pour effectuer la première interrogation à utiliser dans les différentes architectures de réseau. La première approche utilise les messages de contrôle de crédit après que l'autorisation et l'authentification de l'utilisateur ont eu lieu. La seconde approche utilise des messages d'autorisation spécifiques du service pour effectuer la première interrogation durant la phase d'autorisation/authentification de l'utilisateur, et les messages de contrôle de crédit pour les interrogations intermédiaires et finales. Si une mise en œuvre de client de contrôle de crédit prend en charge les deux méthodes, déterminer quelle méthode utiliser DEVRAIT être configurable.

Dans un environnement de service tel que le serveur d'accès réseau (NAS, *Network Access Server*) on souhaite effectuer la première interrogation au titre du processus d'autorisation/authentification pour les besoins de l'efficacité du protocole. D'autres autorisations de crédit après la première interrogation sont effectuées avec des commandes de contrôle de crédit définies dans la présente spécification. Les mises en œuvre de client de contrôle de crédit fonctionnant dans les environnements mentionnés DEVRAIENT prendre en charge cette méthode. Si le serveur de contrôle de crédit et le serveur

AAA sont des entités physiques séparées, l'élément de service envoie les messages de demande au serveur AAA, qui produit alors une demande appropriée ou délègue la demande reçue vers l'avant au serveur de contrôle de crédit.

Dans d'autres environnements de service, comme le réseau 3GPP et certains scénarios SIP, il y a un découplage substantiel entre l'enregistrement/accès au réseau et la demande réelle de service (c'est-à-dire, l'authentification/autorisation est exécutée une fois fait l'enregistrement/accès au réseau et n'est pas exécutée pour chaque événement de service demandé par l'abonné). Dans ces environnements, il est plus approprié d'effectuer la première interrogation après que l'utilisateur a été authentifié et autorisé. La première interrogation, l'intermédiaire, et la finale sont exécutées avec les commandes de contrôle de crédit définies dans la présente spécification.

D'autres normes de l'IETF ou des standard développés par d'autres organismes de normalisation pourront définir la méthode la plus convenable dans leurs architectures.

5.2.1 Première interrogation après autorisation et authentification

Le client de contrôle de crédit Diameter dans l'élément de service peut obtenir des informations du serveur d'autorisation sur l'exigence du contrôle de crédit, sur la base de sa connaissance de l'utilisateur final. Si le contrôle de crédit est exigé, le serveur de contrôle de crédit a besoin d'être contacté avant d'initialiser la livraison du service à l'utilisateur final. Le protocole comptable et le protocole de contrôle de crédit peuvent être utilisés en parallèle. Le serveur d'autorisation peut aussi déterminer si le flux comptable en parallèle est demandé.

Le diagramme qui suit illustre le cas où les deux protocoles sont utilisés en parallèle et l'élément de service envoie des messages de contrôle de crédit directement au serveur de contrôle de crédit. D'autres exemples de séquences de contrôle de crédit figurent en Annexe A.

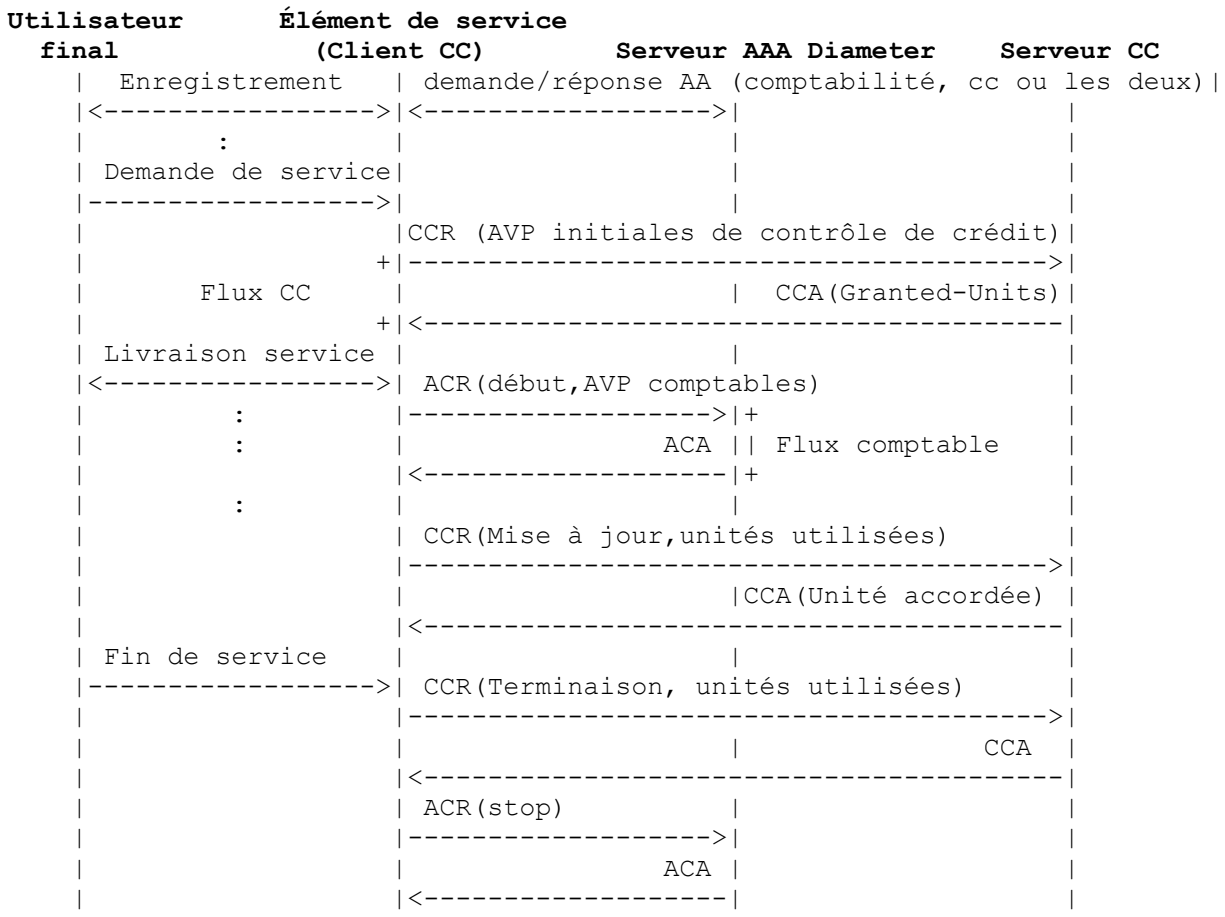


Figure 2 : Exemple de protocole avec première interrogation après l'autorisation/authentification de l'utilisateur

5.2.2 Messages d'autorisation pour la première interrogation

Le client de contrôle de crédit Diameter dans l'élément de service DOIT coopérer activement avec le client d'autorisation/authentification à la construction de la demande AA en ajoutant les AVP appropriées de contrôle de crédit. Le

client de contrôle de crédit DOIT ajouter l'AVP Credit-Control pour indiquer les capacités de contrôle de crédit et PEUT ajouter d'autres AVP de contrôle de crédit pertinentes spécifiques à la commande appropriée d'autorisation/authentification pour effectuer la première interrogation au serveur AAA Diameter de rattachement. Le Auth-Application-Id est réglé à la valeur appropriée, comme défini dans le document pertinent d'application d'autorisation/authentification spécifique du service (par exemple, [RFC4004], [RFC4005]). Le serveur AAA Diameter de rattachement authentifie/autorise l'abonné et détermine si le contrôle de crédit est requis.

Si le contrôle de crédit n'est pas exigé pour l'abonné, le serveur AAA Diameter de rattachement va répondre comme d'habitude, avec un message AA de réponse approprie. Si le contrôle de crédit est exigé pour l'abonné et si l'AVP Credit-Control avec la valeur réglée à CREDIT_AUTHORIZATION est présente dans la demande d'autorisation, le serveur AAA de rattachement DOIT contacter le serveur de contrôle de crédit pour effectuer la première interrogation. Si le contrôle de crédit est exigé pour l'abonné et si l'AVP Credit-Control n'est pas présente dans la demande d'autorisation, le serveur AAA de rattachement DOIT envoyer un message de réponse de rejet d'autorisation.

Le serveur AAA Diameter qui prend en charge le contrôle de crédit doit envoyer au serveur de contrôle de crédit la commande Credit-Control-Request (CCR) définie dans le présent document. Le serveur AAA Diameter remplit la CCR sur la base des AVP spécifiques du service utilisées comme entrées dans le processus de tarification, et éventuellement des AVP de contrôle de crédit reçues dans la demande AA. Le serveur de contrôle de crédit va réserver un montant sur le compte de l'utilisateur, va tarifer la demande et va envoyer un message Credit-Control-Answer au serveur AAA Diameter de rattachement. Le message de réponse inclut la ou les AVP Granted-Service-Unit et PEUT inclure d'autres AVP spécifiques de contrôle de crédit, comme approprié. De plus, le serveur de contrôle de crédit PEUT établir la durée de validité et PEUT inclure l'AVP Credit-Control-Failure-Handling et l'AVP Direct-Debiting-Failure-Handling pour déterminer quoi faire si l'envoi des messages de contrôle de crédit au serveur de contrôle de crédit était temporairement empêché.

À réception du message Credit-Control-Answer du serveur de contrôle de crédit, le serveur AAA Diameter de rattachement va remplir la réponse AA avec les AVP de contrôle de crédit reçues et les attributs de service appropriés conformément à l'application spécifique d'autorisation/authentification (par exemple, [RFC4004], [RFC4005]). Il va ensuite transmettre le paquet au client de contrôle de crédit. Si le serveur AAA Diameter de rattachement reçoit un message de rejet de contrôle de crédit, il va simplement générer un message approprié de rejet d'autorisation au client de contrôle de crédit, incluant le code d'erreur spécifique de contrôle de crédit.

Dans ce modèle, le client de contrôle de crédit envoie les messages de contrôle de crédit ultérieurs au serveur de contrôle de crédit via le serveur AAA Diameter de rattachement. À réception d'un message de réponse de succès d'autorisation avec la ou les AVP Granted-Service-Unit, le client de contrôle de crédit va accorder le service à l'utilisateur final et va générer une demande de contrôle de crédit intermédiaire, comme exigé par l'utilisation des commandes de contrôle de crédit. Le numéro de demande de contrôle de crédit CC-Request-Number de la première demande de mise à jour UPDATE_REQUEST DOIT être réglé à 1 (voir au paragraphe 8.2 comment produire une valeur unique pour l'AVP CC-Request-Number).

Si une réautorisation spécifique du service est effectuée (c'est-à-dire, si la durée de vie de l'autorisation est expirée) le client de contrôle de crédit DOIT ajouter à la demande de réautorisation spécifique du service l'AVP Credit-Control avec une valeur réglée à RE_AUTHORIZATION pour indiquer que le serveur de contrôle de crédit NE DOIT PAS être contacté. Lorsque le contrôle de crédit fondé sur la session est utilisé pour l'abonné, un flux constant de messages de contrôle de crédit s'écoule à travers le serveur AAA Diameter de rattachement. Le serveur AAA Diameter de rattachement peut utiliser ce flux de messages de contrôle de crédit pour déduire que l'activité de l'utilisateur est en cours ; donc, il est recommandé de régler la durée de vie d'autorisation à une valeur raisonnablement élevée lorsque le contrôle de crédit est utilisé pour l'abonné.

Dans ce scénario, le serveur AAA Diameter de rattachement DOIT annoncer la prise en charge de l'application de contrôle de crédit à ses homologues durant le processus d'échange de capacités.

Le diagramme qui suit illustre l'utilisation des messages d'autorisation/authentification pour effectuer la première interrogation. Le flux comptable parallèle n'est pas montré sur la figure.

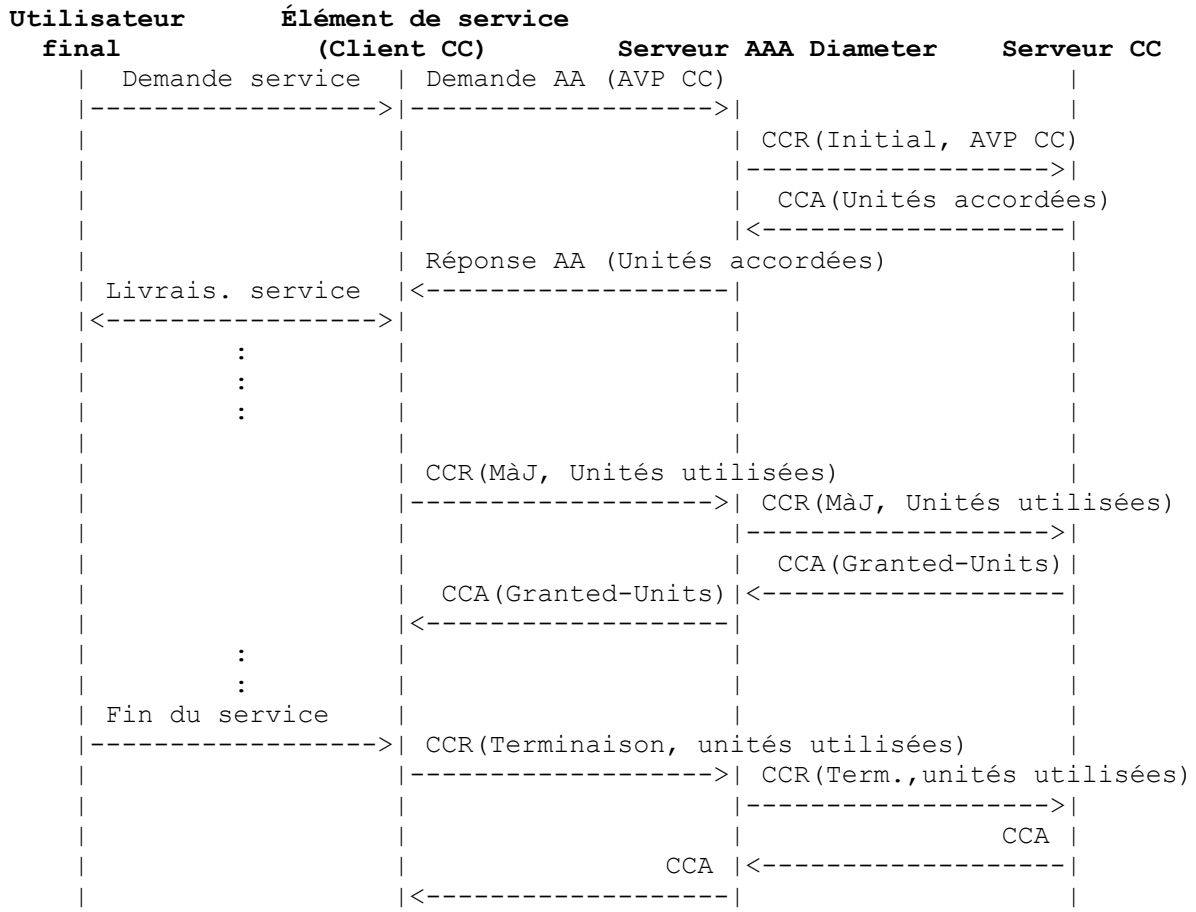


Figure 3 : Exemple de protocole avec des messages d'autorisation à la première interrogation

5.3 Interrogation intermédiaire

Lorsque toutes les unités de service accordées pour un type d'unités sont dépensées par l'utilisateur final ou que la durée de validité est expirée, le client de contrôle de crédit Diameter DOIT envoyer une nouvelle demande de contrôle de crédit au serveur de contrôle de crédit. Si le contrôle de crédit est appliqué pour plusieurs services dans une session de contrôle de crédit (c'est-à-dire, des unités associées à des identifiants de service ou groupe de tarification sont accordées) une nouvelle demande de contrôle de crédit DOIT être envoyée au serveur de contrôle de crédit lorsque la réservation de crédit a été entièrement consommée, ou à l'expiration de la durée de validité. Il appartient toujours au client de contrôle de crédit Diameter d'envoyer une nouvelle demande bien avant l'expiration de la demande précédente afin d'éviter une interruption de l'élément de service. Même si les unités de service accordées réservées par le serveur de contrôle de crédit n'ont pas été dépensées à l'expiration de la durée de validité, le client de contrôle de crédit Diameter DOIT envoyer une nouvelle demande de contrôle de crédit au serveur de contrôle de crédit.

Il peut aussi y avoir des événements de service de mi session, qui peuvent affecter la tarification de l'événement de service en cours. Dans ce cas, une mise à jour spontanée (une nouvelle demande de contrôle de crédit) DEVRAIT être envoyée incluant les informations relatives à l'événement de service même si toutes les unités de service accordées n'ont pas été dépensées ou si la durée de validité n'est pas expirée.

Lorsque les unités utilisées sont rapportées au serveur de contrôle de crédit, le client de contrôle de crédit n'aura plus aucune unité en sa possession avant que les nouvelles unités accordées soient reçues du serveur de contrôle de crédit. Lorsque les nouvelles unités accordées sont reçues, ces unités s'appliquent à partir du point où s'est arrêtée la mesure des unités utilisées rapportées. Lorsque un contrôle de crédit de plusieurs services indépendants est pris en charge, ce processus peut être exécuté pour un ou plusieurs services, un seul groupe de tarification, ou un réservoir au sein de la (sous) session.

L'AVP CC-Request-Type est réglée à la valeur UPDATE_REQUEST dans le message de demande intermédiaire. L'AVP Subscription-Id DEVRAIT être incluse dans le message intermédiaire pour identifier l'utilisateur final chez le serveur de contrôle de crédit. L'AVP Service-Context-Id indique le document spécifique de service applicable à la demande.

L'AVP Requested-Service-Unit PEUT contenir le nouveau montant d'unités de service demandé. Lorsque l'AVP Multiple-Services-Credit-Control est utilisée, elle DOIT contenir l'AVP Requested-Service-Unit si un nouveau quota est demandé

pour le service/groupe de tarification associé. L'AVP Used-Service-Unit contient le montant des unités de service utilisées mesuré depuis le moment où le service est devenu actif ou, si des interrogations intermédiaires sont utilisées durant la session, depuis le moment où s'est terminée la mesure précédente. Les mêmes types d'unités utilisés dans le message précédent DEVRAIENT être utilisés. Si plusieurs types d'unités ont été inclus dans le message de réponse précédent, les unités de service utilisées pour chaque type d'unités DOIVENT être rapportées.

L'AVP Event-Timestamp DEVRAIT être incluse dans la demande et contenir l'heure de l'événement qui a déclanché l'envoi de la nouvelle demande de contrôle de crédit.

Le serveur de contrôle de crédit DOIT déduire le montant utilisé du compte de l'utilisateur final. Il PEUT tarifer la nouvelle demande et faire une nouvelle réservation de crédit à partir du compte de l'utilisateur pour couvrir le coût de l'événement de service demandé.

Un message Réponse de contrôle de crédit avec l'AVP CC-Request-Type réglée à la valeur UPDATE_REQUEST PEUT inclure l'AVP Cost-Information contenant l'estimation cumulée du coût de la session, sans prendre en compte les réservations de crédit.

Le message Demande de contrôle de crédit PEUT aussi inclure l'AVP Final-Unit-Indication pour indiquer que le message de réponse contient les unités finales pour le service. Après la consommation de ces unités par l'utilisateur final, le client Diameter de contrôle de crédit DOIT se comporter comme décrit au paragraphe 5.6.

Il peut y avoir plusieurs interrogations intermédiaires au sein d'une session.

5.4 Interrogation finale

Lorsque l'utilisateur final termine la session de service, ou lorsque a lieu une terminaison de service en douceur décrite au paragraphe 5.6, le client de contrôle de crédit Diameter DOIT envoyer un message de demande de contrôle de crédit finale au serveur de contrôle de crédit. L'AVP CC-Request-Type est réglée à la valeur TERMINATION_REQUEST. L'AVP Service-Context-Id indique le document spécifique de service applicable à la demande.

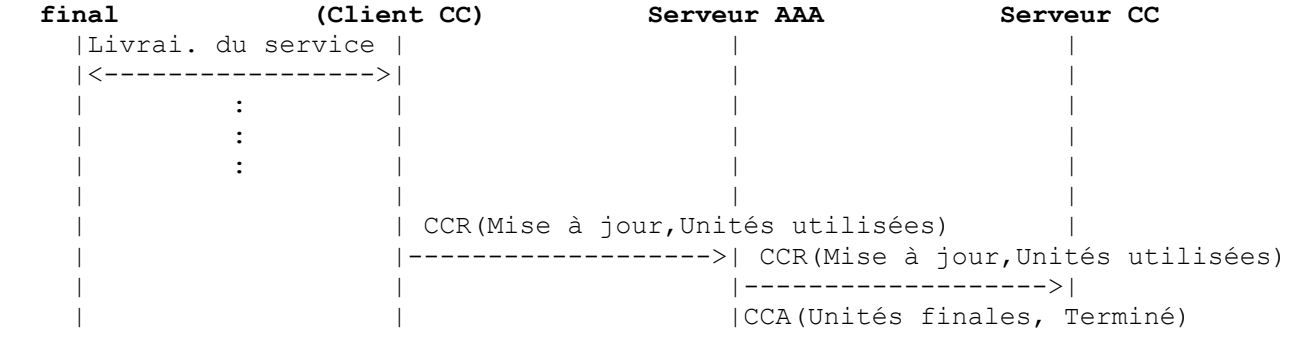
L'AVP Event-Timestamp DEVRAIT être incluse dans la demande et contenir l'heure de fin de la session.

L'AVP Used-Service-Unit contient le montant des unités de service utilisées mesuré à partir du moment où le service est devenu actif ou, si des interrogations intermédiaires ont été utilisées durant la session, depuis le moment où la mesure précédente s'est achevée. Si des unités de plusieurs types étaient incluses dans le message de réponse précédent, les unités de service utilisées pour chaque type d'unité DOIVENT être rapportées.

Après l'interrogation finale, le serveur de contrôle de crédit DOIT reverser le montant du crédit réservé non utilisé sur le compte de l'utilisateur final et déduire le montant utilisé du compte de l'utilisateur final.

Un message Credit-Control-Answer avec le type de demande de contrôle de crédit réglé à la valeur TERMINATION_REQUEST PEUT inclure l'AVP Cost-Information contenant le coût total estimé pour la session en question.

Si l'utilisateur se déconnecte durant une session de contrôle de crédit en cours, ou si quelque autre raison cause la déconnexion de l'utilisateur (par exemple, une indication d'unités finales cause la déconnexion de l'utilisateur conformément à une politique locale) l'élément de service, conformément à la politique spécifique de l'application, peut envoyer une demande de terminaison de session (STR, *Session-Termination-Request*) au serveur AAA Diameter de rattachement comme de règle [RFC3588]. La Figure 4 illustre le cas où l'indication d'unités finales cause la déconnexion de l'utilisateur une fois consommées les unités finales accordées et la génération de la STR.



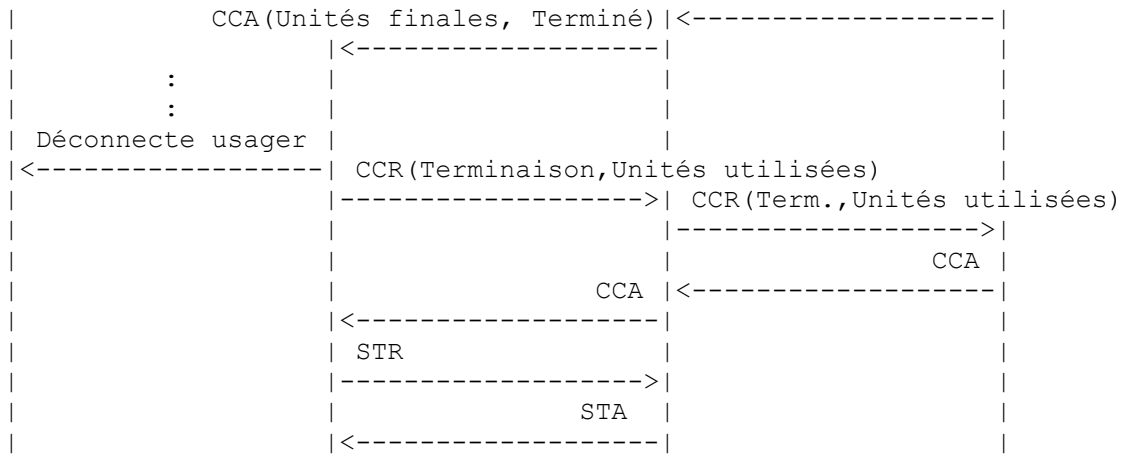


Figure 4 : Déconnexion de l'utilisateur due au défaut de provision du compte

5.5 Réautorisation de crédit à l'initiative du serveur

L'application Diameter de contrôle de crédit prend en charge la réautorisation initiée par le serveur. Le serveur de contrôle de crédit PEUT facultativement initier la réautorisation de crédit en produisant une demande de réauthentification (RAR, *Re-Auth-Request*) comme défini dans le protocole de base Diameter [RFC3588]. L'identifiant d'application d'authentification dans le message RAR est réglé à 4 pour indiquer le contrôle de crédit Diameter, et le type de demande de réauthentification est réglé à AUTHORIZE_ONLY.

Le paragraphe 5.1.2 définit le dispositif pour permettre le contrôle de crédit pour plusieurs services au sein d'une seule (sous) session où le serveur peut autoriser l'utilisation du crédit à un niveau de granularité différent. De plus, le serveur peut fournir des ressources de crédit à plusieurs services ou groupes de tarification comme un réservoir (voir au paragraphe 5.1.2 les détails et les définitions). Donc, le serveur, sur la base de sa logique de service et de sa connaissance de la session en cours, peut décider de demander une réautorisation de crédit pour toute une (sous) session, un seul réservoir de crédit, un seul service, ou un seul groupe de tarification. Pour demander une réautorisation de crédit pour un réservoir de crédit, le serveur inclut dans le message RAR l'AVP G-S-U-Pool-Identifier qui indique le réservoir affecté. Pour demander une réautorisation de crédit pour un service ou groupe de tarification, le serveur inclut dans le message RAR l'AVP Service-Identifier ou l'AVP Rating-Group, selon le cas. Pour demander une réautorisation de crédit pour tous les services en cours dans la (sous) session, le serveur n'inclut aucune des AVP susmentionnées dans le message RAR.

Si une réautorisation de crédit n'est pas déjà en cours (c'est-à-dire, si la session de contrôle de crédit est dans l'état Ouvert) un client de contrôle de crédit qui reçoit un message RAR avec l'identifiant de session égal à une session de contrôle de crédit actuellement active DOIT accuser réception de la demande en envoyant le message Re-Auth-Answer (RAA) et DOIT initier la réautorisation de crédit auprès du serveur en envoyant un message de demande de contrôle de crédit avec l'AVP CC-Request-Type réglée à la valeur UPDATE_REQUEST. Le code de résultat 2002 (DIAMETER_LIMITED_SUCCESS) DEVRAIT être utilisé dans le message RAA pour indiquer qu'un message supplémentaire (c'est-à-dire, un message CCR avec la valeur UPDATE_REQUEST) est nécessaire pour achever la procédure. Si un quota était alloué au service, le client de contrôle de crédit DOIT faire rapport du quota utilisé dans la demande de contrôle de crédit. Noter que l'utilisateur final n'a pas besoin d'être sollicité pour la réautorisation de crédit, car la réautorisation de crédit est transparente pour l'utilisateur (c'est-à-dire, elle a lieu exclusivement entre le client de contrôle de crédit et le serveur de contrôle de crédit).

Lorsque plusieurs services sont pris en charge dans une session d'utilisateur, la procédure du paragraphe précédent sera exécutée à la granularité demandée par le serveur dans le message RAR.

Si une réautorisation de crédit est en cours au moment de la réception du message RAR (c'est-à-dire, une collision RAR-CCR) le client de contrôle de crédit accuse réception de la demande mais n'initie pas une nouvelle réautorisation de crédit. Le code de résultat 2001 (DIAMETER_SUCCESS) DEVRAIT être utilisé dans le message RAA pour indiquer que une procédure de réautorisation de crédit est déjà en cours (c'est-à-dire, le client était dans l'état PendingU lorsque le RAR a été reçu). Le serveur de contrôle de crédit DEVRAIT traiter la demande de contrôle de crédit comme si elle avait été reçue en réponse à la réautorisation de crédit initiée par le serveur, et devrait considérer que le processus de réautorisation de crédit initié par le serveur est réussi à réception du message Re-Auth-Answer.

Lorsque plusieurs services sont pris en charge dans une session d'utilisateur, le serveur peut demander une réautorisation de crédit pour un réservoir de crédit (ou pour la (sous) session) alors que une réautorisation de crédit est déjà en cours pour

certains des services ou groupes de tarification. Dans ce cas, le client accuse réception de la demande du serveur avec un message RAA et DOIT envoyer un nouveau message de demande de contrôle de crédit pour effectuer la réautorisation pour les services/groupes de tarification restants. Le code de résultat 2002 (DIAMETER_LIMITED_SUCCESS) DEVRAIT être utilisé dans le message RAA pour indiquer qu'un message supplémentaire (c'est-à-dire, un message CCR de valeur UPDATE_REQUEST) est exigé pour achever la procédure. Le serveur traite les demandes reçues et retourne une réponse appropriée aux deux demandes.

Les procédures définies ci-dessus sont activées pour chacune des sous sessions de contrôle de crédit Diameter actives. Le serveur PEUT demander la réautorisation pour une sous session active en incluant l'AVP CC-Sub-Session-Id dans le message RAR en plus de l'AVP Session-Id.

5.6 Terminaison de service en douceur

Lorsque il n'y a plus d'argent sur le compte de l'utilisateur, il peut n'être plus autorisé à compiler des événement tarifés supplémentaires. Cependant, le fournisseur de service de rattachement peut offrir certains services ; par exemple, l'accès à un portail de service où il est possible de réapprovisionner le compte, dont il est permis à l'utilisateur de bénéficier pour une durée limitée. Cette durée dépend généralement de la politique du fournisseur de service.

On définit ici le dispositif facultatif de terminaison de service en douceur qui PEUT être pris en charge par le serveur de contrôle de crédit. Les mises en œuvre de client de contrôle de crédit DOIVENT prendre en charge l'indication d'unités finales avec au moins la fermeture de la session de service en cours une fois que l'abonné a consommé toutes les unités finales accordées.

Lorsque est pris en charge un contrôle de crédit indépendant de plusieurs services dans une seule (sous) session de contrôle de crédit, il est possible d'utiliser la terminaison de service en douceur indépendamment pour chaque service/groupe de tarification. Naturellement, le processus de terminaison de service en douceur défini dans les paragraphes qui suivent s'appliquera au service/groupe de tarification spécifique selon les exigences du serveur.

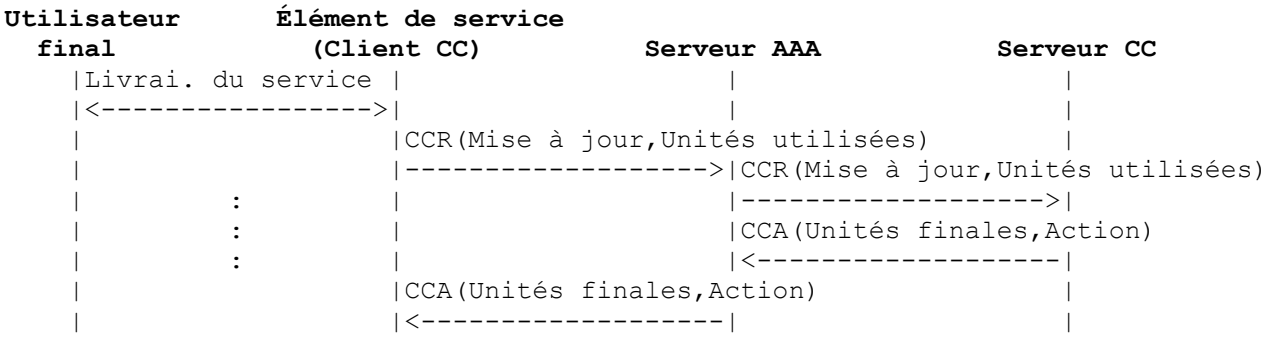
Dans certains environnements de service (par exemple, NAS) la terminaison de service en douceur peut être utilisée pour rediriger l'abonné sur un portail de service pour réapprovisionner en ligne ou pour d'autres services offerts par le fournisseur de service de rattachement. Dans ce cas, le processus de terminaison en douceur installe un ensemble de filtres de paquets pour restreindre la capacité d'accès de l'utilisateur aux seules destinations spécifiées. Tous les paquets IP qui ne correspondent pas aux filtres seront éliminés ou, éventuellement, redirigés sur le portail de service. L'utilisateur peut aussi recevoir une notification appropriée quant aux raisons de la limitation d'accès. Ces actions peuvent être communiquées explicitement du serveur au client ou peuvent être configurées par service au client. Les instructions de redirection ou de restriction explicitement signalées ont toujours la préséance sur celles qui sont configurées.

Il est aussi possible d'utiliser la terminaison de service en douceur pour connecter l'usager prépayé à un serveur d'appoint qui effectue une annonce et invite l'utilisateur à réapprovisionner le compte. Dans ce cas, le serveur de contrôle de crédit envoie seulement l'adresse du serveur d'appoint où l'usager prépayé devra être connecté après que les unités finales accordées auront été consommées. Un exemple en est donné en Appendice A (Flux VII).

Le serveur de contrôle de crédit PEUT initier la terminaison de service en douceur en incluant l'AVP Final-Unit-Indication dans la réponse de contrôle de crédit pour indiquer que le message contient les unités finales pour le service.

Lorsque le client de contrôle de crédit reçoit l'AVP Final-Unit-Indication dans la réponse du serveur, son comportement dépend de la valeur indiquée dans l'AVP Final-Unit-Action. Le serveur peut demander les actions suivantes : TERMINATE *(terminer)*, REDIRECT *(rediriger)*, ou RESTRICT_ACCESS *(accès interdit)*.

La figure suivante illustre la procédure de terminaison de service en douceur décrite dans les paragraphes qui suivent.



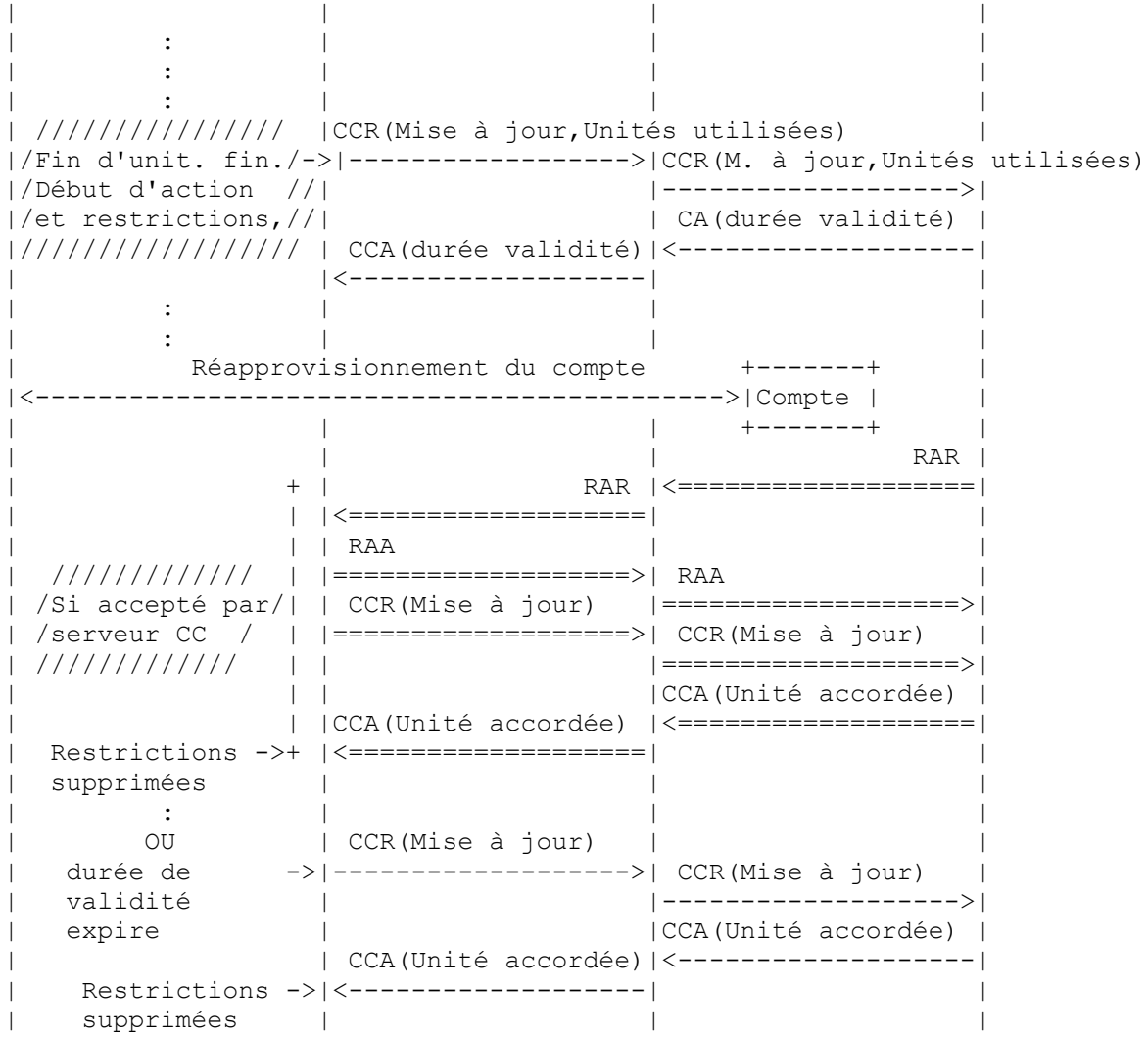


Figure 5 : Procédure facultative de terminaison de service en douceur

5.6.1 Action Terminate

L'AVP Final-Unit-Indication avec l'action Final-Unit-Action TERMINATE n'inclut aucune autre information. Lorsque l'abonné a consommé les unités finales accordées, l'élément de service DOIT terminer le service. C'est le traitement par défaut applicable chaque fois que le client de contrôle de crédit reçoit une valeur d'action d'unités finales non prise en charge et il DOIT être pris en charge par toutes les mises en œuvre de client de contrôle de crédit Diameter qui se conforment à la présente spécification. Un message de demande de contrôle de crédit finale au serveur de contrôle de crédit DOIT être envoyé si l'AVP Final-Unit-Indication indiquant l'action TERMINATE est présente au niveau commande. L'AVP CC-Request-Type dans la demande est réglée à la valeur TERMINATION_REQUEST.

5.6.2 Action de redirection

L'AVP Final-Unit-Indication avec Final-Unit-Action REDIRECT indique à l'élément de service qui prend en charge cette action que, lorsque les unités finales accordées seront consommées, l'utilisateur DOIT être redirigé sur l'adresse spécifiée dans l'AVP Redirect-Server comme suit.

Le serveur de contrôle de crédit envoie l'AVP Redirect-Server dans le message Credit-Control-Answer. Dans ce cas, l'élément de service DOIT rediriger ou connecter l'utilisateur sur la destination spécifiée dans l'AVP Redirect-Server, si possible. Lorsque l'utilisateur final est redirigé (en utilisant des protocoles autres que Diameter) sur le serveur spécifié ou connecté au serveur d'appoint, une autorisation supplémentaire (et éventuellement une authentification) peut être nécessaire avant que l'abonné puisse réapprovisionner le compte ; cependant, ceci sort du domaine d'application de la présente spécification.

En plus de l'AVP Redirect-Server, le serveur de contrôle de crédit PEUT inclure une ou plusieurs AVP Restriction-Filter-Rule (*règle de filtre de restriction*) ou une ou plusieurs AVP Filter-Id dans le message de réponse de contrôle de crédit pour

permettre à l'utilisateur d'accéder à d'autres services (par exemple, des services gratuits). Dans ce cas, l'appareil d'accès DOIT éliminer tous les paquets qui ne correspondent pas aux filtres IP spécifiés dans le message Credit-Control-Answer et, si possible, rediriger l'utilisateur sur la destination spécifiée dans l'AVP Redirect-Server.

Une entité autre que le serveur de contrôle de crédit peut provisionner l'appareil d'accès avec des filtres de paquet IP appropriés pour être utilisés en conjonction avec l'application Diameter de contrôle de crédit. Ce cas est examiné au paragraphe 5.6.3.

Lorsque les unités finales accordées ont été consommées, le client de contrôle de crédit DOIT effectuer une interrogation intermédiaire. L'objet de cette interrogation est d'indiquer au serveur de contrôle de crédit que l'action spécifiée a commencé et de faire rapport des unités utilisées. Le serveur de contrôle de crédit DOIT déduire la quantité utilisée du compte de l'utilisateur final mais NE DOIT PAS faire une nouvelle réservation de crédit. Le client de contrôle de crédit peut, cependant, envoyer des interrogations intermédiaires avant que toutes les unités finales accordées aient été consommées pour lesquelles une tarification et une réservation de provisions pourraient être nécessaires ; par exemple, si la durée de validité arrive à expiration ou si un événement de services de mi-session affecte la tarification du service en cours. Donc, le client de contrôle de crédit NE DOIT PAS inclure d'AVP en rapport avec la tarification dans la demande envoyée une fois que les unités finales accordées ont été consommées comme indication au serveur que l'action d'unités finales demandées a commencé, la tarification et la réservation de provisions ne sont pas exigées (lorsque l'AVP Multiple-Services-Credit-Control est utilisée, les AVP Service-Identifier ou Rating-Group sont incluses pour indiquer les services concernés). Naturellement, le message Credit-Control-Answer ne contient aucune unité de service accordée et DOIT inclure l'AVP Durée de validité pour indiquer au client de contrôle de crédit pendant combien de temps l'abonné est autorisé à utiliser les ressources du réseau avant qu'une nouvelle interrogation intermédiaire soit envoyée au serveur.

À l'expiration de la durée de validité, le client de contrôle de crédit envoie une demande de contrôle de crédit (UPDATE_REQUEST) comme d'habitude. Ce message n'inclut pas d'AVP Used-Service-Unit, car il n'y a pas de quota alloué à rapporter. Le serveur de contrôle de crédit traite la demande et DOIT effectuer la réservation de crédit. Si pendant ce temps l'abonné n'a pas réapprovisionné son compte, qu'il soit déconnecté ou qu'il ait eu accès à des services non contrôlés par un serveur de contrôle de crédit pendant une durée illimitée dépend de la politique du fournisseur de service de rattachement (noter que la dernière option implique que l'élément de service ne devrait pas supprimer les filtres de restriction à la fin du contrôle de crédit). Le serveur va retourner le code de résultat approprié (voir au paragraphe 9.1) dans le message de réponse de contrôle de crédit afin de mettre en œuvre l'action définie par la politique. Autrement, un nouveau quota sera retourné, l'élément de service DOIT supprimer toutes les restrictions éventuelles activées par le processus de terminaison de service en douceur et continuer la session de contrôle de crédit et la session de service comme d'habitude.

Le client de contrôle de crédit peut ne pas attendre jusqu'à l'expiration de la durée de validité et peut envoyer une mise à jour spontanée (une nouvelle demande de contrôle de crédit) si l'élément de service peut déterminer, par exemple, que la communication entre l'utilisateur final et le serveur d'appoint a eu lieu. Un exemple en est donné à l'Appendice A (Figure A.8).

Noter que le serveur de contrôle de crédit peut avoir déjà initié le processus décrit ci-dessus pour la première interrogation. Cependant, le compte de l'utilisateur peut être vide quand la première interrogation est effectuée. Dans ce cas, on peut offrir à l'abonné une chance d'approvisionner le compte et continuer le service. Le client de contrôle de crédit reçoit une réponse de contrôle de crédit ou une réponse d'autorisation spécifique du service avec les AVP Final-Unit-Indication et Durée de validité mais pas d'AVP Granted-Service-Unit. Il commence immédiatement la terminaison de service en douceur sans envoyer de message au serveur. Un exemple de ce cas est illustré à l'Appendice A.

5.6.3 Action d'interdiction d'accès

Une AVP Final-Unit-Indication avec Final-Unit-Action RESTRICT_ACCESS indique à l'appareil qui prend cette action en charge que l'accès de l'utilisateur DOIT être restreint conformément aux filtres de paquets IP donnés dans la ou les AVP Restriction-Filter-Rule ou conformément aux filtres de paquets IP identifiés par la ou les AVP Filter-Id. Le serveur de contrôle de crédit DEVRAIT inclure soit l'AVP Restriction-Filter-Rule, soit l'AVP Filter-Id dans le message Credit-Control-Answer.

Une entité autre que le serveur de contrôle de crédit peut provisionner l'appareil d'accès avec les filtres de paquets IP appropriés pour être utilisés en conjonction avec l'application Diameter de contrôle de crédit. Une telle entité peut, par exemple, configurer l'appareil d'accès avec des flux IP à passer lorsque l'application Diameter de contrôle de crédit indique RESTRICT_ACCESS ou REDIRECT. L'appareil d'accès passe les paquets IP conformément aux règles de filtres qui peuvent avoir été reçues dans le message Credit-Control-Answer en plus de celles qui peuvent avoir été configurées par l'autre entité. Cependant, quand le compte de l'utilisateur ne peut pas couvrir le coût du service demandé, l'action entreprise est de la responsabilité du serveur de contrôle de crédit qui contrôle l'abonné prépayé.

Si une autre entité travaillant en conjonction avec l'application Diameter de contrôle de crédit a déjà approvisionné l'appareil d'accès avec toutes les règles de filtre exigées pour l'utilisateur final, le serveur de contrôle de crédit n'a vraisemblablement pas besoin d'envoyer de filtres supplémentaires. Donc, il est RECOMMANDÉ que les mises en œuvre de serveur de contrôle de crédit qui prennent en charge la terminaison de service en douceur soient configurables à envoyer les AVP Restriction-Filter-Rule, Filter-Id, ou aucune d'entre elles.

Lorsque les unités finales accordées ont été consommées, le client de contrôle de crédit DOIT effectuer une interrogation intermédiaire. Le client de contrôle de crédit et le serveur de contrôle de crédit traitent cette interrogation intermédiaire et exécutent les procédures qui suivent, comme spécifié au paragraphe précédent sur l'action REDIRECT.

Le serveur de contrôle de crédit peut initier la terminaison de service en douceur avec l'action RESTRICT_ACCESS déjà pour la première interrogation, comme spécifié au paragraphe précédent sur l'action REDIRECT.

5.6.4 Utilisation de la réautorisation de crédit à l'initiative du serveur

Une fois que l'abonné a réapprovisionné le compte, il s'attend vraisemblablement à ce que toutes les restrictions installées par la procédure de terminaison en douceur soient immédiatement supprimées et qu'un accès illimité au service soit rétabli. Dans le meilleur des cas, la mise en œuvre de serveur de contrôle de crédit PEUT prendre en charge la réautorisation de crédit à l'initiative du serveur (voir au paragraphe 5.5). Dans ce cas, lorsque le compte a pu être complété, le serveur de contrôle de crédit envoie le message Re-Auth-Request (RAR) pour solliciter une réautorisation de crédit. Le client de contrôle de crédit initie la réautorisation de crédit en envoyant le message de demande de contrôle de crédit avec l'AVP CC-Request-Type réglée à la valeur UPDATE_REQUEST. L'AVP Used-Service-Unit n'est pas incluse dans la demande, car il n'y a pas d'allocation de quota à rapporter. L'AVP Requested-Service-Unit PEUT être incluse dans la demande. Après que le client de contrôle de crédit a réussi a recevoir la réponse de contrôle de crédit avec les nouvelles unités de service accordées, toutes les restrictions éventuellement activées pour les besoins de la terminaison de service en douceur DOIVENT être supprimées dans l'élément de service. La session de contrôle de crédit et la session de service continuent comme d'habitude.

5.7 Procédures sur échec

L'AVP Credit-Control-Failure-Handling (CCFH), décrite dans ce paragraphe, détermine le comportement du client de contrôle de crédit dans des situations d'échec. CCFH peut être reçue du serveur AAA Diameter de rattachement, du serveur de contrôle de crédit, ou peut être configurée en local. La valeur de CCFH reçue du serveur AAA de rattachement outrepasse la valeur configurée en local. La valeur CCFH reçue du serveur de contrôle de crédit dans le message de réponse de contrôle de crédit outrepasse toujours toute autre valeur existante.

Le serveur d'autorisation PEUT inclure l'AVP Accounting-Realtime-Required *(comptabilité en temps réel exigée)* pour déterminer quoi faire si l'envoi d'enregistrements comptables au serveur de comptabilité a été temporairement empêché, comme défini dans la [RFC3588]. Il est RECOMMANDÉ que le client complète les procédures d'échec de contrôle de crédit par un flux comptable de secours vers un serveur de comptabilité. En utilisant différentes combinaisons d'AVP Accounting-Realtime-Required et Credit-Control-Failure-Handling, différents niveaux de sûreté peuvent être construits. Par exemple, en choisissant une AVP Credit-Control-Failure-Handling égale à CONTINUE pour le flux de contrôle de crédit et une AVP Accounting-Realtime-Required égale à DELIVER_AND_GRANT pour le flux comptable, le service peut être accordé à l'utilisateur final même si la connexion au serveur de contrôle de crédit est arrêtée, tant que le serveur de comptabilité est capable de collecter les informations de comptabilité et que l'échange d'informations a lieu entre le serveur de comptabilité et le serveur de contrôle de crédit.

Comme l'application de contrôle de crédit se fonde sur une communication bidirectionnelle en temps réel entre le client de contrôle de crédit et le serveur de contrôle de crédit, l'usage de destinations de remplacement et la mise en mémoire tampon des messages peuvent n'être pas suffisants en cas d'échec de la communication. Parce que le serveur de contrôle de crédit doit maintenir les états de sessions, passer le flux de messages de contrôle de crédit sur un serveur de secours exige une solution complexe de transfert de contexte. Le déplacement du flux de messages de contrôle de crédit sur un serveur de contrôle de crédit de secours durant une session de contrôle de crédit en cours dépend de la valeur de l'AVP CC-Session-Failover. Cependant, la reprise sur défaillance peut se produire en tout point du chemin entre le client de contrôle de crédit et le serveur de contrôle de crédit si une défaillance de transport est détectée avec un homologue, comme décrit dans la [RFC3588]. Par conséquent, le serveur de contrôle de crédit peut recevoir des messages dupliqués. Ces messages dupliqués ou décalés peuvent être détectés au serveur de contrôle de crédit sur la base des AVP Session-Id et CC-Request-Number de l'automate à états de session du serveur de contrôle de crédit (Section 7),.

Si une défaillance survient durant une session de contrôle de crédit en cours, le client de contrôle de crédit peut déplacer le flux de messages de contrôle de crédit sur un serveur de remplacement si le serveur de contrôle de crédit a indiqué "FAILOVER_SUPPORTED" dans l'AVP CC-Session-Failover. Un nom de serveur de contrôle de crédit secondaire, soit

reçu du serveur AAA Diameter de rattachement, soit configuré en local, peut être utilisé comme adresse du serveur de secours. Si l'AVP CC-Session-Failover est réglée à FAILOVER_NOT_SUPPORTED, le flux de messages de contrôle de crédit NE DOIT PAS être déplacé sur un serveur de secours.

Pour une nouvelle session de contrôle de crédits, la reprise sur défaillance par un serveur de contrôle de crédit de remplacement DEVRAIT être effectuée si possible. Par exemple, si une mise en œuvre du client de contrôle de crédit peut déterminer l'indisponibilité du serveur de contrôle de crédit principal, elle peut établir une nouvelle session de contrôle de crédit avec un serveur de contrôle de crédit secondaire éventuellement disponible.

Le profil de transport AAA [RFC3539] définit l'algorithme de chien de garde de couche application qui permet la reprise sur défaillance d'un homologue qui a eu une défaillance et est contrôlé par un temporisateur de chien de garde (Tw) défini dans la [RFC3539]. La valeur initiale recommandée par défaut pour Tw (Twinit) est 30 secondes. Twinit peut être réglé jusqu'à aussi peu que 6 secondes ; cependant, selon la [RFC3539], régler Twinit à une valeur trop basse va vraisemblablement résulter en une probabilité accrue de dupliqués, ainsi qu'en de plus nombreuses tentatives de reprise sur défaillance et de reprises automatiques parasites. Le protocole Diameter de base est commun à plusieurs différents types d'applications AAA Diameter qui peuvent fonctionner sur le même élément de service. Donc, régler le temporisateur Twinit à une valeur inférieure afin de satisfaire les exigences des applications en temps réel, comme l'application Diameter de contrôle de crédit, va certainement causer les problèmes sus mentionnés. Pour les services prépayés, cependant, l'utilisateur final attend une réponse du réseau dans un délai raisonnable. Donc, le client de contrôle de crédit Diameter va réagir plus vite que ne le ferait le protocole de base sous-jacent. Donc la présente spécification définit le temporisateur Tx qui est utilisé par le client de contrôle de crédit (comme défini dans la Section 13) pour superviser la communication avec le serveur de contrôle de crédit. Quand le temporisateur Tx s'est écoulé, le client de contrôle de crédit effectue une action à l'égard de l'utilisateur conformément à l'AVP Credit-Control-Failure-Handling.

Lorsque Tx expire, le client de contrôle de crédit Diameter termine toujours le service si l'AVP Credit-Control-Failure-Handling (CCFH) est réglée à la valeur TERMINATE. La session de contrôle de crédit ne peut être déplacée vers un serveur de remplacement que si est reçue avant l'expiration de Tx une erreur de protocole DIAMETER_TOO_BUSY ou DIAMETER_UNABLE_TO_DELIVER. Donc, la valeur TERMINATE n'est pas appropriée si on désire un comportement de reprise sur défaillance.

Si l'AVP Credit-Control-Failure-Handling est réglée à la valeur CONTINUE ou RETRY_AND_TERMINATE, le service sera accordé à l'utilisateur final à l'expiration du temporisateur Tx . Un message de réponse avec des unités accordées peut arriver plus tard si la reprise sur défaillance de transport du protocole de base s'est produite sur le chemin vers le serveur de contrôle de crédit. (La valeur par défaut de Twinit est trois fois plus que la valeur recommandée de Tx.) Le client de contrôle de crédit DEVRAIT accorder le service à l'utilisateur final, commencer à surveiller l'utilisation des ressources, et attendre une éventuelle réponse tardive jusqu'à la fin de temporisation de la demande (par exemple, 120 secondes). Si la demande échoue et si l'AVP CC-Session-Failover est réglée à FAILOVER_NOT_SUPPORTED, le client de contrôle de crédit termine ou continue le service selon la valeur réglée dans CCFH et DOIT libérer toutes les ressources réservées pour la session de contrôle de crédit. Si l'erreur de protocole DIAMETER_UNABLE_TO_DELIVER ou DIAMETER_TOO_BUSY est reçue ou si la demande arrive en fin de temporisation et si l'AVP CC-Session-Failover est réglée à FAILOVER_SUPPORTED, le client de contrôle de crédit PEUT envoyer la demande à un serveur de secours, si possible. Si le client de contrôle de crédit reçoit une réponse de réussite du serveur de secours, il continue la session de contrôle de crédit avec ce serveur. Si la demande retransmise échoue aussi, le client de contrôle de crédit termine ou continue le service selon la valeur établie dans la CCFH et DOIT libérer toutes les ressources réservées pour la session de contrôle de crédit.

Si une défaillance de communication survient durant la procédure de terminaison de service en douceur, l'élément de service DEVRAIT toujours terminer la session de service en cours.

Si le serveur de contrôle de crédit détecte une défaillance durant une session de contrôle de crédit en cours, il va terminer la session de contrôle de crédit et retourner les unités réservées au compte de l'utilisateur final.

Le temporisateur de supervision de session Tcc (comme défini dans la Section 13) est utilisé dans le serveur de contrôle de crédit pour superviser la session de contrôle de crédit.

Afin de prendre en charge la reprise sur défaillance entre serveurs de contrôle de crédit, le transfert d'informations sur la session de contrôle de crédit et l'état du compte DEVRAIT avoir lieu entre les serveurs de contrôle de crédit principal et secondaire. Les mises en œuvre qui prennent en charge la reprise sur défaillance de session de contrôle de crédit DOIVENT aussi s'assurer d'une détection appropriée des messages dupliqués ou déclassés. La communication entre les serveurs est considérée comme un problème de mise en œuvre et sort du domaine d'application de la présente spécification.

6. Événement unique

L'événement unique est utilisé lorsqu'il n'est pas besoin de conserver d'état dans le serveur de contrôle de crédit Diameter, par exemple, pour se renseigner sur le prix du service. L'utilisation d'un événement unique implique que l'utilisateur a été authentifié et autorisé à l'avance.

L'événement unique peut être utilisé lorsque le client de contrôle de crédit veut savoir le coût de l'événement de service ou vérifier le solde de son compte sans aucune réservation de crédit. Il peut aussi être utilisé pour reverser des unités de service sur le compte de l'utilisateur ou pour un débit direct sans aucune réservation de crédit. L'événement unique est représenté à la Figure 6.

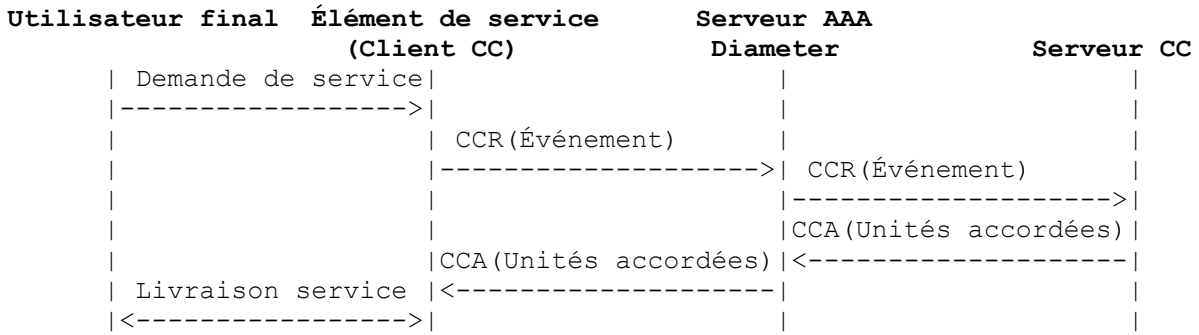


Figure 6 : Événement unique

Dans des environnements comme l'architecture 3GPP, l'événement unique peut être envoyé directement de l'élément de service au serveur de contrôle de crédit.

6.1 Interrogation du prix des services

Le client de contrôle de crédit peut vouloir connaître le prix de l'événement de service. Il peut exister des services offerts par les fournisseurs de service d'application dont les prix ne sont pas connus par le client de contrôle de crédit. L'utilisateur final peut aussi vouloir avoir une estimation du prix d'un événement de service avant de le demander.

Un client de contrôle de crédit Diameter qui demande des informations de coût DOIT régler l'AVP CC-Request-Type égale à EVENT_REQUEST, inclure l'AVP Requested-Action réglée à PRICE_ENQUIRY, et régler les informations d'événement de service demandé dans l'AVP Service-Identifier dans le message de demande de contrôle de crédit. Des informations supplémentaires d'événement de service peuvent être envoyées comme des AVP spécifiques du service ou dans l'AVP Service-Parameter-Info. L'AVP Service-Context-Id indique le document spécifique de service applicable à la demande.

Le serveur de contrôle de crédit calcule le coût de l'événement de service demandé, mais il n'effectue aucune vérification de solde ou réservation de crédit sur le compte.

Le coût estimé de l'événement de service demandé est retourné au client de contrôle de crédit dans l'AVP Cost-Information dans le message Réponse de contrôle de crédit.

6.2 Vérification de provisions

Le client de contrôle de crédit Diameter peut avoir seulement à vérifier que la provision du compte de l'utilisateur final couvre le coût d'un certain service sans réserver d'unités sur le compte au moment de l'interrogation. Cette méthode ne garantit pas qu'il restera du crédit quand le client de contrôle de crédit Diameter demandera le débit du compte dans une demande séparée.

Un client de contrôle de crédit Diameter qui demande le solde du compte DOIT régler l'AVP CC-Request-Type égale à EVENT_REQUEST, inclure une AVP Requested-Action réglée à CHECK_BALANCE, et inclure l'AVP Subscription-Id afin d'identifier l'utilisateur final dans le serveur de contrôle de crédit. L'AVP Service-Context-Id indique le document spécifique de service applicable à la demande.

Le serveur de contrôle de crédit calcule le solde du compte, mais ne fait aucune réservation de crédit sur le compte.

Le résultat du calcul du solde (ENOUGH_CREDIT/NO_CREDIT) est retourné au client de contrôle de crédit dans l'AVP

Check-Balance-Result dans le message Réponse de contrôle de crédit.

6.3 Débit direct

Il y a certains événements de service pour lesquels l'exécution du service est toujours réussie dans l'environnement du service. Le délai entre l'invocation du service et la livraison réelle du service à l'utilisateur final peut être suffisamment long pour que l'utilisation du contrôle de crédit fondé sur la session conduise à des sessions de contrôle de crédit déraisonnablement longues. Dans ces cas, le client de contrôle de crédit Diameter peut utiliser le scénario d'événement unique pour un débit direct. Le client de contrôle de crédit Diameter DEVRAIT être sûr que l'exécution de l'événement de service demandé va réussir lorsque ce scénario est utilisé.

Dans le message de demande de contrôle de crédit, le CC-Request-Type est réglé à la valeur EVENT_REQUEST et l'AVP Requested-Action est réglée à DIRECT_DEBITING. L'AVP Subscription-Id DEVRAIT être incluse pour identifier l'utilisateur final auprès du serveur de contrôle de crédit. L'AVP Event-Timestamp DEVRAIT être incluse dans la demande et contenir l'heure à laquelle l'événement de service est demandé dans l'élément de service. L'AVP Service-Context-Id indique le document spécifique de service applicable à la demande.

Le client de contrôle de crédit Diameter PEUT inclure la somme à facturer dans l'AVP Requested-Service-Unit, si il connaît le coût de l'événement de service. Si le client de contrôle de crédit Diameter ne connaît pas le coût de l'événement de service, l'AVP Requested-Service-Unit PEUT contenir le nombre d'événements de service demandés. L'AVP Service-Identifier indique toujours le service concerné. Des informations supplémentaires d'événement de service à tarifer PEUVENT être envoyées comme AVP spécifiques du service ou dans l'AVP Service-Parameter-Info.

Le serveur de contrôle de crédit DEVRAIT tarifer l'événement de service et déduire la somme correspondante du compte de l'utilisateur final. Si le type de l'AVP Requested-Service-Unit est monétaire, aucune tarification n'est nécessaire, mais la somme correspondante est déduite du compte de l'utilisateur final.

Le serveur de contrôle de crédit retourne l'AVP Granted-Service-Unit dans le message Réponse de contrôle de crédit au client de contrôle de crédit Diameter. L'AVP Granted-Service-Unit contient la quantité d'unités de service que le client de contrôle de crédit Diameter peut fournir à l'utilisateur final. Le type de Granted-Service-Unit peut être du temps, un volume, spécifique du service, ou de l'argent, selon le type d'événement de service.

Si le serveur de contrôle de crédit détermine qu'aucun contrôle de crédit n'est nécessaire pour le service, il peut inclure le code de résultat qui indique que le contrôle de crédit n'est pas applicable (par exemple, service gratuit).

À des fins d'information, le message Réponse de contrôle de crédit PEUT aussi inclure l'AVP Cost-Information qui contient le coût total estimé du service demandé.

6.4 Reversements

Certains services peuvent reverser des unités de service au compte de l'utilisateur ; par exemple, des services de jeu.

Le client de contrôle de crédit DOIT régler CC-Request-Type à la valeur EVENT_REQUEST et l'AVP Requested-Action à REFUND_ACCOUNT dans le message de demande de contrôle de crédit. L'AVP Subscription-Id DEVRAIT être incluse pour identifier l'utilisateur final auprès du serveur de contrôle de crédit. L'AVP Service-Context-Id indique le document spécifique de service applicable à la demande.

Le client de contrôle de crédit Diameter PEUT inclure la somme à reverser dans l'AVP Requested-Service-Unit. L'AVP Service-Identifier indique toujours le service concerné. Si le client de contrôle de crédit Diameter ne connaît pas la somme à reverser, en plus de l'AVP Service-Identifier, il PEUT envoyer des AVP spécifiques du service ou l'AVP Service-Parameter-Info contenant des informations supplémentaires d'événement de service à tarifer.

À des fins d'information, le message Réponse de contrôle de crédit PEUT aussi inclure l'AVP Cost-Information qui contient la somme estimée d'unités reversées.

6.5 Procédure sur échec

La reprise sur défaillance sur un serveur de contrôle de crédit de remplacement est permise pour un événement unique, car le serveur ne conserve pas les états de session. Par exemple, si le client de contrôle de crédit reçoit une erreur de protocole DIAMETER_UNABLE_TO_DELIVER ou DIAMETER_TOO_BUSY, il peut envoyer de nouveau la demande sur un serveur de remplacement, si possible. Il PEUT y avoir des relais transparents au protocole Diameter et des agents de

redirection ou des mandataires de contrôle de crédit Diameter entre le client de contrôle de crédit et le serveur de contrôle de crédit. La reprise sur défaillance peut intervenir en tout point du chemin entre le client de contrôle de crédit et le serveur de contrôle de crédit si une défaillance du transport est détectée avec un homologue, comme décrit dans la [RFC3588]. Comme il peut y avoir des demandes dupliquées pour diverses raisons, le serveur de contrôle de crédit est responsable de la détection des dupliqués en temps réel. Les questions de mise en œuvre de la détection des dupliqués sont discutées à l'Appendice C de la [RFC3588].

Lorsque le client de contrôle de crédit détecte une défaillance de communication avec le serveur de contrôle de crédit, son comportement dépend de l'action demandée. Le temporisateur Tx (comme défini à la Section 13) est utilisé chez le client de contrôle de crédit pour superviser la communication avec le serveur de contrôle de crédit.

Si l'action demandée est PRICE_ENQUIRY ou CHECK_BALANCE et si une défaillance de communication est détectée, le client de contrôle de crédit DEVRAIT transmettre les messages de demande à un autre serveur de contrôle de crédit, si possible. Le nom du serveur de contrôle de crédit secondaire, si il est reçu du serveur AAA Diameter de rattachement, peut être utilisé comme adresse du serveur de secours.

Si l'action demandée est DIRECT_DEBITING, l'AVP Direct-Debiting-Failure-Handling (DDFH) contrôle le comportement du client de contrôle de crédit. La DDFH peut être reçue du serveur AAA Diameter de rattachement ou peut être configurée en local. Le serveur de contrôle de crédit peut aussi envoyer la DDFH dans tout message CCA pour être utilisée pour les événements de débit direct compilés jusque là. La valeur DDFH reçue du serveur AAA Diameter de rattachement prend le pas sur la valeur configurée en local, et la valeur DDFH reçue du serveur de contrôle de crédit dans un message Réponse de contrôle de crédit prend toujours le pas sur toute valeur existante.

Si la DDFH est réglée à TERMINATE_OR_BUFFER, le client de contrôle de crédit NE DEVRAIT PAS accorder le service si il peut déterminer, éventuellement après a une tentative de retransmission sur un serveur de contrôle de crédit de remplacement, à partir du code de résultat ou du code d'erreur dans le message de réponse que des unités n'ont pas été débitées. Autrement, le client de contrôle de crédit DEVRAIT accorder le service à l'utilisateur final et mémoriser la demande dans une mémorisation non volatile de niveau application de contrôle de crédit. (Noter que renvoyer la demande ultérieurement ne garantit pas que le service sera débité, car le compte de l'utilisateur peut être vide lorsque le serveur réussira à traiter la demande.) Le client de contrôle de crédit DOIT marquer ces messages de demande comme possibles dupliqués en établissant le fanion T dans l'en-tête de commande comme décrit à la Section 3 de la [RFC3588].

Si l'AVP Direct-Debiting-Failure-Handling est réglée à CONTINUE, le service DEVRAIT être accordé, même si les messages de contrôle de crédit ne peuvent pas être délivrés et si les messages ne sont pas mis en mémoire tampon.

Si le temporisateur Tx arrive à expiration, le client de contrôle de crédit DOIT continuer le service et attendre une éventuelle réponse tardive. Si la demande arrive en fin de temporisation, le client de contrôle de crédit retransmet la demande (marquée du fanion T) à un serveur de contrôle de crédit de secours, si possible. Si la demande retransmise arrive aussi en fin de temporisation, ou si une erreur temporaire est reçue en réponse, le client de contrôle de crédit met en mémoire tampon la demande si la valeur de l'AVP Direct-Debiting-Failure-Handling est réglée à TERMINATE_OR_BUFFER. Si une réponse d'échec est reçue pour la demande retransmise, le client de contrôle de crédit libère toutes les ressources réservées pour le message d'événement et supprime la demande sans considération de la valeur de la DDFH.

La demande de contrôle de crédit avec l'action demandée REFUND_ACCOUNT devrait toujours être mémorisée dans la mémorisation non volatile de niveau application de contrôle de crédit en cas de défaillance temporaire. Le client de contrôle de crédit DOIT marquer le message de demande retransmis comme possible dupliqué en établissant le fanion T dans l'en-tête de commande comme décrit à la Section 3 de la [RFC3588].

Pour les demandes mémorisées, la mise en œuvre peut choisir de limiter le nombre de tentatives de retransmission et de définir un intervalle de retransmission.

Noter qu'un seul endroit du système de contrôle de crédit DEVRAIT être responsable de la détection des dupliqués. Si il y a seulement un serveur de contrôle de crédit dans le domaine concerné, le serveur de contrôle de crédit peut effectuer la détection des dupliqués. Si il y a plus d'un serveur de contrôle de crédit dans un certain domaine, une seule entité du système de contrôle de crédit devrait en être responsable, pour assurer que le compte de l'utilisateur final n'est pas débité ou crédité plusieurs fois pour le même événement de service.

7. Automate à états d'application de contrôle de crédit

Cette section définit l'automate à états d'application de contrôle de crédit.

Les quatre premiers automates à états doivent être observés par les clients de contrôle de crédit. Le premier décrit le contrôle de crédit fondé sur la session lorsque la première interrogation est exécutée au titre du processus d'autorisation/authentification. Le second décrit le contrôle de crédit fondé sur la session lorsque la première interrogation est exécutée après le processus d'autorisation/authentification. Les exigences sur la prise en charge des automates à états sont discutées au paragraphe 5.2.

Le troisième automate à états décrit le contrôle de crédit fondé sur la session pour les interrogations intermédiaires et finales. Le quatrième décrit le contrôle de crédit fondé sur l'événement. Ces derniers automates à état sont à observer par toutes les mises en œuvre qui se conforment à la présente spécification.

Le cinquième automate à états décrit la session de contrôle de crédit du point de vue du serveur de contrôle de crédit.

Tout événement non mentionné dans les automates à états DOIT être considéré comme condition d'erreur, et une réponse correspondante, si applicable, DOIT être retournée au générateur du message.

Dans le tableau d'états, l'événement "échec d'envoi" *(Failure to send)* signifie que le client de contrôle de crédit Diameter est incapable de communiquer avec la destination désirée ou, si la procédure de reprise sur défaillance est prise en charge, avec une destination de remplacement éventuellement définie (par exemple, la demande arrive en fin de temporisation et le message de réponse n'est pas reçu). Cela pourrait être dû à ce que l'homologue est défaillant, ou dû à une défaillance de liaison physique sur le chemin ou depuis le serveur de contrôle de crédit.

L'événement "erreur temporaire" *(Temporary error)* signifie que le client de contrôle de crédit Diameter a reçu une notification d'erreur de protocole (DIAMETER_TOO_BUSY, DIAMETER_UNABLE_TO_DELIVER, ou DIAMETER_LOOP_DETECTED) dans l'AVP Result-Code de la commande Credit-Control-Answer. La notification d'erreur du protocole ci-dessus peut en fin de compte être reçue en réponse à la demande retransmise à une destination de remplacement définie, si la reprise sur défaillance est prise en charge.

L'événement "échec de réponse" *(Failed answer)* signifie que le client de contrôle de crédit Diameter a reçu une notification de défaillance non transitoire (défaillance permanente) dans la commande Credit-Control-Answer. La notification de défaillance permanente ci-dessus peut en fin de compte être reçue en réponse à la demande retransmise à une destination de remplacement définie, si la reprise sur défaillance est prise en charge.

L'action "demande de mémorisation" *(store request)* signifie qu'une demande est mémorisée dans la mémorisation non volatile de niveau application de contrôle de crédit.

L'événement "échec du traitement" *(Not successfully processed)* signifie que le serveur de contrôle de crédit n'a pas pu réussir à traiter le message ; par exemple, à cause d'un utilisateur final inconnu, d'un compte vide, ou d'erreurs définies dans la [RFC3588].

L'événement "service d'utilisateur terminé" *(User service terminated)* peut être déclanché par diverses raisons, par exemple, la terminaison normale de l'utilisateur, une défaillance réseau, et une demande d'interruption de session (ASR, *Abort-Session-Request*). L'AVP Termination-Cause contient des informations sur la raison de terminaison, comme spécifié dans la [RFC3588].

Le temporisateur Tx, qui est utilisé pour contrôler le temps d'attente chez le client de contrôle de crédit dans l'état Pending *(en cours)*, est arrêté à la sortie de l'état Pending. L'arrêt du temporisateur Tx est omis dans l'automate à états lorsque le nouvel état est Idle *(repos)*, car passer à l'état Idle implique la suppression de la session et de toutes les variables qui lui sont associées.

Les états PendingI, PendingU, PendingT, PendingE, et PendingB sont des états d'attente d'une réponse à une demande de contrôle de crédit relative respectivement aux demandes Initial, Update *(mise à jour)*, Termination *(terminaison)*, Event *(événement)*, ou Buffered *(mise en mémoire tampon)*.

Les acronymes CCFH et DDFH signifient respectivement Credit-Control-Failure-Handling *(traitement d'échec de contrôle de crédit)* et Direct-Debiting-Failure-Handling *(traitement d'échec de débit direct)*.

Dans le tableau d'automate à états suivant, la reprise sur défaillance sur un serveur secondaire sur "erreur temporaire" ou "échec d'envoi" n'est pas explicitement décrite. Passer un flux de messages de contrôle de crédit en cours sur un serveur de

remplacement, est cependant possible si l'AVP CC-Session-Failover est réglée à FAILOVER_SUPPORTED, comme décrit au paragraphe 5.7.

Le nouvel envoi d'un événement de contrôle de crédit à un serveur de remplacement est pris en charge comme décrit au paragraphe 6.5.

CLIENT, fondé sur la session pour la première interrogation avec demande AA

État	**Événement**	**Action**	**Nouvel état**
Repos	Le client ou l'appareil demande l'accès/service	Envoi de demande AA avec des AVP CC ajoutées, lance Tx	PendingI
PendingI	Demande AA réussie, réponse reçue	Accorde le service à l'utilisateur final, arrête Tx	Ouvert
PendingI	Expiration de Tx	Déconnecte usager/appareil	Repos
PendingI	Échec AA,réponse reçue	Déconnecte usager/appareil	Repos
PendingI	Réponse AA reçue avec code de résultat égal à CREDIT_CONTROL_NOT_APPLICABLE	Accorde le service à l'utilisateur final	Repos
PendingI	Service d'usager terminé	Événement de terminaison de file d'attente	PendingI
PendingI	Changement de condition de tarification	La file d'attente a changé l'événement de condition de tarification	PendingI

CLIENT, fondé sur la session pour la première interrogation avec CCR

État	**Événement**	**Action**	**Nouvel état**
Repos	Le client ou appareil demande l'accès/service	Envoie interrogation CC initiale, lancer Tx	PendingI
PendingI	Réponse CC initiale de succès reçue	Arrêt de Tx	Ouvert
PendingI	Échec d'envoi, ou erreur temporaire et CCFH égal à CONTINUE	Accorde le service à l'utilisateur final	Repos
PendingI	Échec d'envoi, ou erreur temporaire et CCFH égal à TERMINATE ou à RETRY_AND_TERMINATE	Termine le service de l'utilisateur final	Repos
PendingI	Tx expiré et CCFH égal à TERMINATE	Termine le service de l'utilisateur final	Repos
PendingI	Tx expiré et CCFH égal à CONTINUE ou à RETRY_AND_TERMINATE	Accorde le service à l'utilisateur final	PendingI
PendingI	Réponse CC initiale reçue avec le code de résultat END_USER_SERVICE_DENIED ou USER_UNKNOWN	Termine le service de l'utilisateur final	Repos
PendingI	Réponse CC initiale reçue avec le code de résultat égal à CREDIT_CONTROL_NOT_APPLICABLE	Accorde le service à l'utilisateur final	Repos
PendingI	Réponse CC initiale d'échec reçue et CCFH égal à CONTINUE	Accorde le service à l'utilisateur final	Repos
PendingI	Réponse CC initiale d'échec reçue et CCFH égal à TERMINATE ou à RETRY_AND_TERMINATE	Termine le service de l'utilisateur final	Repos
PendingI	Service d'utilisateur terminé	Événement de terminaison de file d'attente	PendingI
PendingI	Changement des conditions de tarification	La file d'attente a changé l'événement de condition de tarification	PendingI

CLIENT, fondé sur la session pour les interrogations intermédiaires et finales

État	**Événement**	**Action**	**Nouvel état**
Ouvert	L'unité accordée s'écoule et aucune indication d'unité finale n'est reçue	Envoie demande Mise à jour CC, lancer Tx	PendingU
Ouvert	L'unité accordée s'écoule et action d'unité finale égale à TERMINATE reçue	Termine le service de l'utilisateur final, envoie demande de terminaison CC	PendingT
Ouvert	Changement de condition tarifaire dans la file d'attente	Envoie demande mise à jour CC, lancer Tx	PendingU
Ouvert	Service terminé dans la file d'attente	Envoie demande de terminaison CC	PendingT
Ouvert	Changement de condition tarifaire ou durée de validité écoulée	Envoie demande de mise à jour CC, lancer Tx	PendingU
Ouvert	Service d'utilisateur terminé	Envoie demande de terminaison CC	PendingT
Ouvert	RAR reçue	Envoie RAA suivi par demande mise	PendingU

		à jour CC, lance Tx	
PendingU	Mise à jour CC réussie, réponse reçue	Arrête Tx	Ouvert
PendingU	Échec d'envoi, ou erreur temporaire et CCFH égal à CONTINUE	Accorde le service à l'utilisateur final	Repos
PendingU	Échec d'envoi, ou erreur temporaire et CCFH égal à TERMINATE ou à RETRY_AND_TERMINATE	Termine le service à l'utilisateur final	Repos
PendingU	Tx expiré et CCFH égal à TERMINATE	Termine le service à l'utilisateur final	Repos
PendingU	Tx expiré et CCFH égal à CONTINUE ou à RETRY_AND_TERMINATE	Accorde le service à l'utilisateur final	PendingU
PendingU	Réponse mise à jour CC reçue avec code de résultat END_USER_SERVICE_DENIED	Termine le service à l'utilisateur final	Repos
PendingU	Réponse mise à jour CC reçue avec code de résultat égal à CREDIT_CONTROL_NOT_APPLICABLE	Accorde le service à l'utilisateur final	Repos
PendingU	Échec de mise à jour CC, réponse reçue et CCFH égal à CONTINUE	Accorde le service à l'utilisateur final	Repos
PendingU	Échec de mise à jour CC, réponse reçue et CCFH égal à TERMINATE ou à RETRY_AND_TERMINATE	Termine le service à l'utilisateur final	Repos
PendingU	Service d'utilisateur terminé	Événement de terminaison de file d'attente	PendingU
PendingU	Changement de condition tarifaire	La file d'attente a changé l'événement de condition de tarification	PendingU
PendingU	RAR reçue	Envoie RAA	PendingU
PendingT	CC réussi, réponse de terminaison reçue		Repos
PendingT	Échec d'envoi, erreur temporaire, ou échec de réponse		Repos
PendingT	Changement de condition tarifaire		PendingT

CLIENT, fondé sur l'événement

État	**Événement**	**Action**	**Nouvel état**
Repos	Client ou appareil demande service unique	Envoie demande événement CC, lance Tx	PendingE
Repos	Demande en mémorisation	Envoie la demande mémorisée	PendingB
PendingE	Réponse événement CC réussi reçue	Accorde le service à l'utilisateur final	Repos
PendingE	Échec d'envoi, erreur temporaire, réponse d'échec d'événement CC reçue, ou Tx expiré ; action demandée CHECK_BALANCE ou PRICE_ENQUIRY	Indique une erreur de service	Repos
PendingE	Réponse d'événement CC reçue avec le code de résultat END_USER_SERVICE_DENIED ou USER_UNKNOWN et Tx courant	Termine le service à l'utilisateur final	Repos
PendingE	Réponse d'événement CC reçue avec le code de résultat CREDIT_CONTROL_NOT_APPLICABLE ; action demandée DIRECT_DEBITING	Accorde le service à l'utilisateur final	Repos
PendingE	Échec d'envoi, erreur temporaire , ou réponse d'échec d'événement CC reçue ; action demandée DIRECT_DEBITING ; DDFH égal à CONTINUE	Accorde le service à l'utilisateur final	Repos
PendingE	Réponse d'échec d'événement CC reçue ou erreur temporaire ; action demandée DIRECT_DEBITING ; DDFH égal à TERMINATE_OR_BUFFER et Tx courant	Termine le service à l'utilisateur final	Repos
PendingE	Tx expiré ; action demandée DIRECT_DEBITING	Accorde le service à l'utilisateur final	PendingE
PendingE	Échec d'envoi ; action demandée DIRECT_DEBITING ; DDFH égal à TERMINATE_OR_BUFFER	Mémorise la demande avec le fanion T	Repos
PendingE	Erreur temporaire ; action demandée DIRECT_DEBITING ; DDFH égal à TERMINATE_OR_BUFFER ; Tx expiré	Mémorise la demande	Repos
PendingE	Échec de réponse ou réponse reçue avec code de résultat END_USER_SERVICE DENIED ou USER_UNKNOWN ; action demandée DIRECT_DEBITING ; Tx expiré		Repos
PendingE	Réponse d'échec d'événement CC reçue ; action demandée REFUND_ACCOUNT	Indique erreur de service et supprime la demande	Repos

PendingE	Échec d'envoi ou Tx expiré ; action demandée REFUND_ACCOUNT	Mémorise la demande avec fanion T	Repos
PendingE	Erreur temporaire, et action demandée REFUND_ACCOUNT	Mémorise la demande	Repos
PendingB	Réponse CC réussi reçue	Supprime la demande	Repos
PendingB	Réponse d'échec CC reçue	Supprime la demande	Repos
PendingB	Échec d'envoi ou erreur temporaire		Repos

SERVEUR, fondé sur la session et l'événement

État	**Événement**	**Action**	**Nouvel état**
Repos	Demande CC initiale reçue et traitée avec succès	Envoie réponse CC initiale , réserve les unités, lance Tcc	Ouvert
Repos	Demande CC initiale reçue mais pas traitée avec succès	Envoie une réponse avec le code de résultat de != SUCCESS	Repos
Repos	Demande d'événement CC reçue et traitée avec succès	Envoie réponse d'événement CC	Repos
Repos	Demande d'événement CC reçue mais pas traitée avec succès	Envoie une réponse d'événement CC avec le code de résultat de != SUCCESS	Repos
Ouvert	Demande de mise à jour CC reçue et traitée avec succès	Envoie une réponse de mise à jour CC, débite les unités utilisées, réserve de nouvelles unités, relance Tcc	Ouvert
Ouvert	Demande de mise à jour CC reçue mais pas traitée avec succès	Envoie une réponse de mise à jour CC avec le code de résultat de != SUCCESS, débite les unités utilisées	Repos
Ouvert	Demande de terminaison CC reçue et traitée avec succès	Envoie une réponse de terminaison CC, arrête Tcc, débite les unités utilisées	Repos
Ouvert	Demande de terminaison CC reçue mais pas traitée avec succès	Envoie une réponse de terminaison CC avec le code de résultat de != SUCCESS, débite les unités utilisées	Repos
Ouvert	Temporisateur de supervision de session Tcc expiré	Libère les unités réservées	Repos

8. AVP de contrôle de crédit

Cette section définit les AVP de contrôle de crédit qui sont spécifiques de l'application Diameter de contrôle de crédit et qui PEUVENT être incluses dans les messages de contrôle de crédit Diameter.

Les AVP définies dans cette section PEUVENT aussi être incluses dans les commandes d'autorisation définies dans les applications spécifiques d'autorisation, comme les [RFC4004] et [RFC4005], si la première interrogation est effectuée au titre du processus d'autorisation/authentification, comme décrit au paragraphe 5.2.

Les règles des AVP Diameter sont définies dans le protocole de base Diameter [RFC3588], Section 4. Ces règles d'AVP sont respectées dans les AVP définies dans cette section.

Le tableau qui suit décrit les AVP Diameter définies dans l'application de contrôle de crédit, la valeur de leur code AVP, leur type, les valeurs possibles de fanions, et si l'AVP PEUT être chiffrée. Le protocole de base Diameter [RFC3588] spécifie les règles de fanion d'AVP pour les AVP en son paragraphe 4.5 : "Pour le générateur d'un message Diameter, "Chiffr." (Chiffrement) signifie que si un message contenant cette AVP va être envoyé via un agent Diameter (mandataire, de redirection ou de relais) le message NE DOIT alors PAS être envoyé si il n'y a pas la sécurité de bout en bout entre le générateur et le receveur et si la protection de l'intégrité / confidentialité n'est pas offerte pour cette AVP OU à moins que le générateur ait une configuration locale de confiance qui indique que la sécurité de bout en bout n'est pas nécessaire. De même, pour le générateur d'un message Diameter, un "P" dans la colonne "Peut" signifie que si un message contenant cette AVP va être envoyé via un agent Diameter (mandataire, de redirection ou de relais) le message NE DOIT alors PAS être envoyé tant qu'il n'y a pas la sécurité de bout en bout entre le générateur et le receveur ou à moins que le générateur ait une configuration locale de confiance qui indique que la sécurité de bout en bout n'est pas nécessaire." *(Le "M" dans la colonne "Doit "M" signifie probablement "Obligatoire" (Mandatory). La signification du"V" dans la colonne "Ne doit pas" n 'est pas expliquée.)*

Nom d'attribut	Code AVP	§	Type de données	Règles de fanion d'AVP Doit	Peut	Ne doit pas	Chiffr.
CC-Correlation-Id	411	8.1	OctetString		P, M	V	oui
CC-Input-Octets	412	8.24	Unsigned64	M	P	V	oui
CC-Money	413	8.22	Grouped	M	P	V	oui
CC-Output-Octets	414	8.25	Unsigned64	M	P	V	oui
CC-Request-Number	415	8.2	Unsigned32	M	P	V	oui
CC-Request-Type	416	8.3	Enumerated	M	P	V	oui
CC-Service-Specific-Units	417	8.26	Unsigned64	M	P	V	oui
CC-Session-Failover	418	8.4	Enumerated	M	P	V	oui
CC-Sub-Session-Id	419	8.5	Unsigned64	M	P	V	oui
CC-Time	420	8.21	Unsigned32	M	P	V	oui
CC-Total-Octets	421	8.23	Unsigned64	M	P	V	oui
CC-Unit-Type	454	8.32	Enumerated	M	P	V	oui
Check-Balance-Result	422	8.6	Enumerated	M	P	V	oui
Cost-Information	423	8.7	Grouped	M	P	V	oui
Cost-Unit	424	8.12	UTF8String	M	P	V	oui
Credit-Control	426	8.13	Enumerated	M	P	V	oui
Credit-Control-Failure-Handling	427	8.14	Enumerated	M	P	V	oui
Currency-Code	425	8.11	Unsigned32	M	P	V	oui
Direct-Debiting-Failure-Handling	428	8.15	Enumerated	M	P	V	oui
Exponent	429	8.9	Integer32	M	P	V	oui
Final-Unit-Action	449	8.35	Enumerated	M	P	V	oui
Final-Unit-Indication	430	8.34	Grouped	M	P	V	oui
Granted-Service-Unit	431	8.17	Grouped	M	P	V	oui
G-S-U-Pool-Identifier	453	8.31	Unsigned32	M	P	V	oui
G-S-U-Pool-Reference	457	8.30	Grouped	M	P	V	oui
Multiple-Services-Credit-Control	456	8.16	Grouped	M	P	V	oui
Multiple-Services-Indicator	455	8.40	Enumerated	M	P	V	oui
Rating-Group	432	8.29	Unsigned32	M	P	V	oui
Redirect-Address-Type	433	8.38	Enumerated	M	P	V	oui
Redirect-Server	434	8.37	Grouped	M	P	V	oui
Redirect-Server-Address	435	8.39	UTF8String	M	P	V	oui
Requested-Action	436	8.41	Enumerated	M	P	V	oui
Requested-Service-Unit	437	8.18	Grouped	M	P	V	oui
Restriction-Filter-Rule	438	8.36	IPFiltrRule	M	P	V	oui
Service-Context-Id	461	8.42	UTF8String	M	P	V	oui
Service-Identifier	439	8.28	Unsigned32	M	P	V	oui
Service-Parameter-Info	440	8.43	Grouped		P,M	V	oui
Service-Parameter-Type	441	8.44	Unsigned32		P,M	V	oui
Service-Parameter-Value	442	8.45	OctetString		P,M	V	oui
Subscription-Id	443	8.46	Grouped	M	P	V	oui
Subscription-Id-Data	444	8.48	UTF8String	M	P	V	oui
Subscription-Id-Type	450	8.47	Enumerated	M	P	V	oui
Tariff-Change-Usage	452	8.27	Enumerated	M	P	V	oui
Tariff-Time-Change	451	8.20	Time	M	P	V	oui
Unit-Value	445	8.8	Grouped	M	P	V	oui
Used-Service-Unit	446	8.19	Grouped	M	P	V	oui
User-Equipment-Info	458	8.49	Grouped		P,M	V	oui
User-Equipment-Info-Type	459	8.50	Enumerated		P,M	V	oui
User-Equipment-Info-Value	460	8.51	OctetString		P,M	V	oui
Value-Digits	447	8.10	Integer64	M	P	V	oui
Validity-Time	448	8.33	Unsigned32	M	P	V	oui

8.1 AVP CC-Correlation-Id

L'AVP CC-Correlation-Id (code d'AVP 411) est du type OctetString *(chaîne d'octets)* et contient des informations pour corréler les demandes de contrôle de crédit générées pour les différents composants du service ; par exemple, de niveau transport et service. Celui qui alloue le Service-Context-Id (c'est-à-dire, l'identifiant unique d'un document spécifique de service) est aussi responsable de définir le contenu et le codage de l'AVP CC-Correlation-Id.

8.2 AVP CC-Request-Number

L'AVP CC-Request-Number (code d'AVP 415) est du type Unsigned32 *(32 bits non signés)* et identifie cette demande au sein d'une session. Comme les AVP Session-Id sont uniques au monde, la combinaison des AVP Session-Id et CC-Request-Number est aussi unique au monde et peut être utilisée pour confronter les messages de contrôle de crédit avec les confirmations. Une façon simple de produire des nombres uniques est de régler la valeur à 0 pour une demande de contrôle de crédit de type INITIAL_REQUEST et EVENT_REQUEST et de régler la valeur à 1 pour la première UPDATE_REQUEST, à 2 pour la seconde, et ainsi de suite jusqu'à ce que la valeur pour TERMINATION_REQUEST soit un de plus que pour la dernière UPDATE_REQUEST.

8.3 AVP CC-Request-Type

L'AVP CC-Request-Type (code d'AVP 416) est du type Enumerated *(énumération)* et contient la raison de l'envoi du message de demande de contrôle de crédit. Elle DOIT être présente dans tous les messages de demande de contrôle de crédit. Les valeurs suivantes sont définies pour l'AVP CC-Request-Type :

INITIAL_REQUEST : 1
Une demande initiale est utilisée pour initier une session de contrôle de crédit, et contient les informations de contrôle de crédit qui sont pertinentes pour l'initiation.

UPDATE_REQUEST : 2
Une demande de mise à jour contient les informations de contrôle de crédit pour une session de contrôle de crédit existante. Les demandes de mise à jour de contrôle de crédit DEVRAIENT être envoyées chaque fois qu'une réautorisation de contrôle de crédit est nécessaire à l'expiration du quota alloué ou de la durée de validité. De plus, des événements spécifiques de service supplémentaires PEUVENT déclancher une demande de mise à jour spontanée.

TERMINATION_REQUEST : 3
Une demande Termination est envoyée pour terminer une session de contrôle de crédit et contient des informations de contrôle de crédit pertinentes pour la session existante.

EVENT_REQUEST : 4
Une demande Event est utilisée lorsque il n'est pas nécessaire de conserver d'état de session de contrôle de crédit dans le serveur de contrôle de crédit. Cette demande contient toutes les informations pertinentes pour le service, et est la seule demande du service. La raison de la demande d'événement est détaillée dans l'AVP Requested-Action. L'AVP Requested-Action DOIT être incluse dans le message de demande de contrôle de crédit lorsque CC-Request-Type est réglé à EVENT_REQUEST.

8.4 AVP CC-Session-Failover

L'AVP CC-Session-Failover (code d'AVP 418) est du type Enumerated et contient les informations sur la prise en charge du déplacement du flux de messages de contrôle de crédit sur un serveur de secours durant une session de contrôle de crédit en cours. Dans les défaillances de communication, le flux de messages de contrôle de crédit peut être déplacé vers une destination de remplacement si le serveur de contrôle de crédit prend en charge la reprise sur défaillance sur un serveur de remplacement. Le nom du serveur de contrôle de crédit secondaire, si il est reçu du serveur AAA Diameter de rattachement, peut être utilisé comme adresse du serveur de secours. Une mise en œuvre n'est pas obligée de prendre en charge le déplacement du flux de messages de contrôle de crédit sur un serveur de remplacement, car cela exige aussi de déplacer les informations relatives à la session de contrôle de crédit sur le serveur de secours.

Les valeurs suivantes sont définies pour l'AVP CC-Session-Failover :

FAILOVER_NOT_SUPPORTED : 0
Lorsque l'AVP CC-Session-Failover est réglée à FAILOVER_NOT_SUPPORTED, le flux de messages de contrôle de crédit NE DOIT PAS être déplacé vers une destination de remplacement dans le cas d'une défaillance de communication. C'est le comportement par défaut si l'AVP n'est pas incluse dans la réponse du serveur d'autorisation ou de contrôle de crédit.

FAILOVER_SUPPORTED : 1
Lorsque l'AVP CC-Session-Failover est réglée à FAILOVER_SUPPORTED, le flux de messages de contrôle de crédit DEVRAIT être passé sur une destination de remplacement dans le cas d'une défaillance de communication. Passer le flux de messages de contrôle de crédit à un serveur de secours PEUT exiger que les informations relatives à la session de contrôle de crédit soient aussi transmises au serveur de remplacement.

8.5 AVP CC-Sub-Session-Id

L'AVP CC-Sub-Session-Id (code d'AVP 419) est du type Unsigned64 *(64 bits non signés)* et contient l'identifiant de sous session de contrôle de crédit. La combinaison du Session-Id et de cette AVP DOIT être unique par sous session, et la valeur de cette AVP DOIT être à croissance monotone de un pour toutes les nouvelles sous sessions. L'absence de cette AVP implique qu'aucune sous session n'est utilisée.

8.6 AVP Check-Balance-Result

L'AVP Check-Balance-Result (code d'AVP 422) est du type Enumerated et contient le résultat de la vérification du solde. Cette AVP n'est applicable que lorsque l'AVP Requested-Action indique CHECK_BALANCE dans la commande de demande de contrôle de crédit.

Les valeurs suivantes sont définies pour l'AVP Check-Balance-Result :

ENOUGH_CREDIT : 0. Il y a assez de crédit sur le compte pour couvrir le service demandé.

NO_CREDIT : 1. Il n'y a pas assez de crédit sur le compte pour couvrir le service demandé.

8.7 AVP Cost-Information

L'AVP Cost-Information (code d'AVP 423) est du type Grouped, et elle est utilisée pour retourner les informations de coût d'un service, que le client de contrôle de crédit peut transférer de façon transparente à l'utilisateur final. L'AVP incluse Unit-Value contient l'estimation du coût (toujours le type Money) du service, dans le cas d'une demande de prix, ou l'estimation cumulée des coûts, dans le cas de session de contrôle de crédit.

Le Currency-Code spécifie dans quelle monnaie le coût est donné. Le Cost-Unit spécifie l'unité lorsque le coût du service est un coût par unité (par exemple, le coût du service est 1 € par minute).

Lorsque l'AVP Requested-Action avec la valeur PRICE_ENQUIRY est incluse dans la commande de demande de contrôle de crédit, l'AVP Cost-Information envoyée dans la commande Credit-Control-Answer suivante contient l'estimation du coût du service demandé, sans que soit faite aucune réservation.

L'AVP Cost-Information incluse dans la commande Credit-Control-Answer avec le CC-Request-Type réglé à UPDATE_REQUEST contient l'estimation des coûts cumulés pour la session, sans prendre en compte aucune réservation de crédit.

L'AVP Cost-Information incluse dans la commande Credit-Control-Answer avec le CC-Request-Type réglé à EVENT_REQUEST ou TERMINATION_REQUEST contient le coût total estimé pour le service demandé.

Elle est définie comme suit (selon la grouped-avp-def de la [RFC3588]) :

```
Cost-Information ::= < en-tête d'AVP : 423 >
                     { Unit-Value }
                     { Currency-Code }
                     [ Cost-Unit ]
```

8.8 AVP Unit-Value

L'AVP Unit-Value est du type Grouped (code d'AVP 445) et spécifie les unités comme valeur décimale. La valeur d'unité est une valeur avec un exposant ; c'est-à-dire, Unit-Value = AVP Value-Digits * 10^Exposant. Cette représentation évite des arrondis indésirables. Par exemple, la valeur de 2,3 est représentée comme Value-Digits = 23 et Exposant = -1. L'absence de la partie exposant DOIT être interprétée comme exposant égal à zéro.

Elle est définie comme suit (selon la grouped-avp-def de la [RFC3588]) :

```
Unit-Value ::= < en-tête d'AVP : 445 >
                    { Value-Digits }
                    [ Exponent ]
```

8.9 AVP Exponent

L'AVP Exponent est du type Integer32 (code d'AVP 429) et contient la valeur d'exposant à appliquer pour l'AVP Value-Digit au sein de l'AVP Unit-Value.

8.10 AVP Value-Digits

L'AVP Value-Digits est du type Integer64 (code d'AVP 447) et contient les chiffres significatifs du nombre. Si des valeurs décimales sont nécessaires pour représenter les unités, l'échelle DOIT être indiquée avec l'AVP Exponent en rapport. Par exemple, pour la quantité monétaire 0,05 €, la valeur de l'AVP Value-Digits DOIT être réglée à 5, et l'échelle DOIT être indiquée avec l'AVP Exponent réglé à -2.

8.11 AVP Currency-Code

L'AVP Currency-Code (code d'AVP 425) est du type Unsigned32 et contient un code de monnaie qui spécifie dans quelle monnaie ont été données les valeurs des AVP qui contiennent les unités monétaires. Elle est spécifiée en utilisant les valeurs numériques définies dans la norme ISO 4217 [ISO4217].

8.12 AVP Cost-Unit

L'AVP Cost-Unit (code d'AVP 424) est du type UTF8String, et est utilisée pour afficher une chaîne lisible par l'homme à l'utilisateur final. Elle spécifie l'unité applicable à Cost-Information lorsque le coût du service est un coût par unité (par exemple, le coût du service est de 1 € par minute). Cost-Unit peut être des minutes, des heures, des jours, des kilo octets, des méga octets, etc.

8.13 AVP Credit-Control

L'AVP Credit-Control (code d'AVP 426) est du type Enumerated et DOIT être incluse dans les demandes AA lorsque l'élément de service a des capacités de contrôle de crédit.

CREDIT_AUTHORIZATION : 0
Si le serveur AAA Diameter de rattachement détermine que l'utilisateur a un abonnement prépayé, cette valeur indique que le serveur de contrôle de crédit DOIT être contacté pour effectuer la première interrogation. La valeur de l'AVP Credit-Control DOIT toujours être réglée à 0 dans une demande AA envoyée pour effectuer la première interrogation et pour initier une nouvelle session de contrôle de crédit.

RE_AUTHORIZATION : 1
Cette valeur indique au serveur AAA Diameter qu'une session de contrôle de crédit est en cours pour l'abonné et que le serveur de contrôle de crédit NE DOIT PAS être contacté. L'AVP Credit-Control réglée à la valeur de 1 n'est à n'utiliser que lorsque la première interrogation a été effectuée avec succès et que la session de contrôle de crédit est en cours (c'est-à-dire, une réautorisation déclanchée par Authorization-Lifetime). Cette valeur NE DOIT PAS être utilisée dans une demande AA envoyée pour effectuer la première interrogation.

8.14 AVP Credit-Control-Failure-Handling

L'AVP Credit-Control-Failure-Handling (code d'AVP 427) est du type Enumerated. Le client de contrôle de crédit utilise les informations de cette AVP pour décider que faire si l'envoi de messages de contrôle de crédit au serveur de contrôle de crédit a été, par exemple, temporairement empêché par un problème réseau. Selon la logique du service, le serveur de contrôle de crédit peut ordonner au client de terminer le service immédiatement quand il y a des raisons de croire que le service ne peut pas être facturé, ou pour essayer une reprise sur défaillance sur un serveur de remplacement, si possible. Ensuite, le serveur peut soit terminer, soit accorder le service, si la connexion de remplacement devait aussi échouer.

TERMINATE : 0
Lorsque l'AVP Credit-Control-Failure-Handling est réglée à TERMINATE, le service DOIT seulement être accordé tant qu'il y a une connexion au serveur de contrôle de crédit. Si le client de contrôle de crédit ne reçoit aucun message Réponse de contrôle de crédit dans le délai du temporisateur Tx (comme défini à la Section 13) la demande de contrôle de crédit est considérée comme ayant échoué, et la session de service de l'utilisateur final est terminée. C'est le comportement par défaut si l'AVP n'est pas incluse dans la réponse du serveur d'autorisation ou de contrôle de crédit.

CONTINUE: 1
Lorsque l'AVP Credit-Control-Failure-Handling est réglée à CONTINUE, le client de contrôle de crédit DEVRAIT envoyer à nouveau la demande à un serveur de remplacement dans le cas de défaillances de transport ou temporaires, pourvu qu'une procédure de reprise sur défaillance soit prise en charge au serveur de contrôle de crédit et au client de contrôle de crédit, et qu'un serveur de remplacement soit disponible. Autrement, le service DEVRAIT être accordé, même si les messages de contrôle de crédit ne peuvent pas être livrés.

RETRY_AND_TERMINATE : 2
Lorsque l'AVP Credit-Control-Failure-Handling est réglé à RETRY_AND_TERMINATE, le client de contrôle de crédit DEVRAIT envoyer à nouveau la demande à un serveur de remplacement dans le cas de défaillances de transport ou temporaires, pourvu qu'une procédure de reprise sur défaillance soit prise en charge chez le serveur de contrôle de crédit et le client de contrôle de crédit, et qu'un serveur de remplacement soit disponible. Autrement, le service DEVRAIT ne pas être accordé lorsque les messages de contrôle de crédit ne peuvent pas être délivrés.

8.15 AVP Direct-Debiting-Failure-Handling

L'AVP Direct-Debiting-Failure-Handling (code d'AVP 428) est du type Enumerated. Le client de contrôle de crédit utilise les informations de cette AVP pour décider quoi faire si l'envoi des messages de contrôle de crédit (AVP Requested-Action réglée à DIRECT_DEBITING) au serveur de contrôle de crédit a été, par exemple, temporairement empêché à cause d'un problème réseau.

TERMINATE_OR_BUFFER : 0
Lorsque l'AVP Direct-Debiting-Failure-Handling est réglée à TERMINATE_OR_BUFFER, le service DOIT être accordé pour autant qu'il y ait une connexion au serveur de contrôle de crédit. Si le client de contrôle de crédit ne reçoit aucun message Réponse de contrôle de crédit dans le délai du temporisateur Tx (comme défini à la Section 13) la demande de contrôle de crédit est considérée comme ayant échoué. Le client DEVRAIT terminer le service si il peut déterminer à partir de la réponse d'échec que les unités n'ont pas été débitées. Autrement, le client de contrôle de crédit DEVRAIT accorder le service, mémoriser la demande dans une mémorisation non volatile de niveau application, et essayer d'envoyer à nouveau la demande. Ces demandes DOIVENT être marquées comme de possibles dupliquées en réglant le fanion T dans l'en-tête de commande, comme décrit à la section 3 de la [RFC3588].

C'est le comportement par défaut si l'AVP n'est pas incluse dans la réponse du serveur d'autorisation.

CONTINUE : 1
Lorsque l'AVP Direct-Debiting-Failure-Handling est réglée à CONTINUE, le service DEVRAIT être accordé, même si les messages de contrôle de crédit ne peuvent pas être livrés, et la demande devrait être supprimée.

8.16 AVP Multiple-Services-Credit-Control

L'AVP Multiple-Services-Credit-Control (code d'AVP 456) est de type Grouped et contient les AVP qui se rapportent au contrôle de crédit indépendant de plusieurs caractéristiques de services. Noter que chaque instance de cette AVP porte des unités relatives à un ou plusieurs services ou relatives à un seul groupe de tarification.

Les AVP Service-Identifier et Rating-Group sont utilisées pour associer les unités accordées à un certain service ou groupe de tarification. Si les deux AVP Service-Identifier et Rating-Group sont incluses, la cible des unités de service est toujours le ou les services indiqués par la valeur de la ou des AVP Service-Identifier. Si seule l'AVP Rating-Group-Id est présente, l'AVP Multiple-Services-Credit-Control se rapporte à tous les services qui appartiennent au groupe de tarification spécifié.

L'AVP G-S-U-Pool-Reference permet au serveur de spécifier un G-S-U-Pool-Identifier qui identifie un réservoir de crédit dans lequel les unités du type spécifié sont considérées comme mises en réserve. Si une AVP G-S-U-Pool-Reference est présente, les unités de service réelles du type spécifié DOIVENT aussi être présentes. Par exemple, si l'AVP G-S-U-Pool-Reference spécifie le type d'unité TIME, l'AVP CC-Time DOIT être présente.

L'AVP Requested-Service-Unit PEUT contenir la quantité des unités de service demandées ou la valeur monétaire demandée. Elle DOIT être présente dans l'interrogation initiale et au sein des interrogations intermédiaires dans lesquelles de nouveaux quotas sont demandés. Si le client de contrôle de crédit n'inclut pas d'AVP Requested-Service-Unit dans une commande de demande, parce que par exemple, il a déterminé que l'utilisateur final a terminé le service, le serveur DOIT débiter le montant utilisé du compte de l'utilisateur, mais NE DOIT PAS retourner un nouveau quota dans la réponse correspondante. Les AVP Validity-Time, Result-Code, et Final-Unit-Indication PEUVENT être présentes dans une commande de réponse comme défini aux paragraphes 5.1.2 et 5.6 pour la terminaison de service en douceur.

Lorsque les deux AVP Tariff-Time-Change et Tariff-Change-Usage sont présentes, le serveur DOIT inclure deux instances séparées de l'AVP Multiple-Services-Credit-Control avec l'AVP Granted-Service-Unit associée au même identifiant de service et/ou groupe de tarification. Que les deux quotas soient associés au même réservoir ou à des réservoirs différents, le mécanisme de mise en réserve de crédit défini au paragraphe 5.1.2 s'applique. L'AVP Tariff-Change-Usage NE DOIT PAS être incluse dans les commandes de demandes pour faire rapport des unités utilisées, avant, et après un changement d'horaire de tarif; l'AVP Used-Service-Unit DOIT être utilisée.

Un serveur qui ne met pas en œuvre le contrôle de crédit indépendant de plusieurs fonctionnalités de service DOIT traiter l'AVP Multiple-Services-Credit-Control comme AVP invalide.

L'AVP Multiple-Services-Control est définie comme suit (selon la grouped-avp-def de la [RFC3588]) :

```
Multiple-Services-Credit-Control ::= < en-tête d'AVP : 456 >
                                     [ Granted-Service-Unit ]
                                     [ Requested-Service-Unit ]
                                    *[ Used-Service-Unit ]
                                     [ Tariff-Change-Usage ]
                                    *[ Service-Identifier ]
                                     [ Rating-Group ]
                                    *[ G-S-U-Pool-Reference ]
                                     [ durée de validité ]
                                     [ Result-Code ]
                                     [ Final-Unit-Indication ]
                                    *[ AVP ]
```

8.17 AVP Granted-Service-Unit

L'AVP Granted-Service-Unit (code d'AVP 431) est du type Grouped et contient la quantité d'unités que le client de contrôle de crédit Diameter peut fournir à l'utilisateur final jusqu'à ce que le service doive être libéré ou qu'une nouvelle demande de contrôle de crédit doive être envoyée. Un client n'est pas obligé de mettre en œuvre tous les types d'unités, et il doit traiter les types d'unités inconnus ou non pris en charge dans le message de réponse comme une réponse CCA incorrecte. Dans ce cas, le client DOIT terminer la session de contrôle de crédit et indiquer dans l'AVP Termination-Cause la raison DIAMETER_BAD_ANSWER.
L'AVP Granted-Service-Unit est définie comme suit (selon la grouped-avp-def de la [RFC3588]) :

```
Granted-Service-Unit ::= < en-tête d'AVP : 431 >
                         [ Tariff-Time-Change ]
                         [ CC-Time ]
                         [ CC-Money ]
                         [ CC-Total-Octets ]
                         [ CC-Input-Octets ]
                         [ CC-Output-Octets ]
                         [ CC-Service-Specific-Units ]
                        *[ AVP ]
```

8.18 AVP Requested-Service-Unit

L'AVP Requested-Service-Unit (code d'AVP 437) est du type Grouped et contient la quantité d'unités demandées spécifiée par le client de contrôle de crédit Diameter. Un serveur n'est pas obligé de mettre en œuvre tous les types d'unités, et il doit traiter les types d'unités inconnus ou non pris en charge comme des AVP invalides.
L'AVP Requested-Service-Unit est définie comme suit (selon la grouped-avp-def de la [RFC3588]) :

```
Requested-Service-Unit ::= < en-tête d'AVP : 437 >
                           [ CC-Time ]
                           [ CC-Money ]
                           [ CC-Total-Octets ]
                           [ CC-Input-Octets ]
                           [ CC-Output-Octets ]
                           [ CC-Service-Specific-Units ]
                          *[ AVP ]
```

8.19 AVP Used-Service-Unit

L'AVP Used-Service-Unit est du type Grouped (code d'AVP 446) et contient la quantité d'unités utilisées mesurée depuis le moment où le service est devenu actif ou, si des interrogations intermédiaires sont utilisées durant la session, depuis le moment où s'est terminée la mesure précédente.

L'AVP Used-Service-Unit AVP est définie comme suit (selon la grouped-avp-def de la [RFC3588]) :

```
Used-Service-Unit ::= < en-tête d'AVP : 446 >
                      [ Tariff-Change-Usage ]
                      [ CC-Time ]
                      [ CC-Money ]
                      [ CC-Total-Octets ]
                      [ CC-Input-Octets ]
                      [ CC-Output-Octets ]
                      [ CC-Service-Specific-Units ]
                     *[ AVP ]
```

8.20 AVP Tariff-Time-Change

L'AVP Tariff-Time-Change (code d'AVP 451) est du type Time. Elle est envoyée du serveur au client et inclut le temps en secondes depuis le 1er janvier 1900, 00:00 UTC, où le tarif du service sera changé.

Le mécanisme de changement de tarif est facultatif pour le client et le serveur, et il n'est pas utilisé pour les services fondés sur le temps définis à la Section 5. Si un client ne prend pas en charge le mécanisme de changement d'horaire de tarif, il DOIT traiter l'AVP Tariff-Time-Change dans le message de réponse comme une réponse CCA incorrecte. Dans ce cas, le client termine la session de contrôle de crédit et indique dans l'AVP Termination-Cause la raison DIAMETER_BAD_ANSWER.

L'omission de cette AVP signifie qu'aucun changement de tarif n'est à rapporter.

8.21 AVP CC-Time

L'AVP CC-Time (code d'AVP 420) est du type Unsigned32 et indique la longueur de temps demandée, accordée, ou utilisée, en secondes.

8.22 AVP CC-Money

L'AVP CC-Money (code d'AVP 413) est du type Grouped et spécifie la quantité monétaire dans la monnaie indiquée. L'AVP Currency-Code DEVRAIT être incluse. Elle est définie comme suit (selon la grouped-avp-def de la [RFC3588]) :

```
CC-Money ::= < en-tête d'AVP : 413 >
             { Unit-Value }
             [ Currency-Code ]
```

8.23 AVP CC-Total-Octets

L'AVP CC-Total-Octets (code d'AVP 421) est du type Unsigned64 et contient le nombre total d'octets demandé, accordé ou utilisé sans considération de la direction (envoyée ou reçue).

8.24 AVP CC-Input-Octets

L'AVP CC-Input-Octets AVP (code d'AVP 412) est du type Unsigned64 et contient le nombre d'octets demandé, accordé, ou utilisé qui peut être ou avoir été reçu de l'utilisateur final.

8.25 AVP CC-Output-Octets

L'AVP CC-Output-Octets AVP (code d'AVP 414) est du type Unsigned64 et contient le nombre d'octets demandé, accordé, ou utilisé qui peut être ou avoir été envoyé à l'utilisateur final.

8.26 AVP CC-Service-Specific-Units

L'AVP CC-Service-Specific-Units (code d'AVP 417) est du type Unsigned64 et spécifie le nombre d'unités spécifiques du service (par exemple, nombre d'événements, points) données dans un service choisi. Les unités spécifiques du service se réfèrent toujours au service identifié dans l'AVP Service-Identifier (ou l'AVP Rating-Group quand l'AVP Multiple-Services-Credit-Control est utilisée).

8.27 AVP Tariff-Change-Usage

L'AVP Tariff-Change-Usage (code d'AVP 452) est du type Enumerated et définit si les unités sont utilisées avant ou après un changement de tarif, ou si les unités ont enjambé un changement de tarif durant la période de rapport. L'omission de cette AVP signifie qu'aucun changement de tarif ne s'est produit.

De plus, quand elle est présente dans un message de réponse au titre de l'AVP Multiple-Services-Credit-Control, cette AVP définit si les unités sont allouées pour être utilisées avant ou après un événement de changement de tarif.

Lorsque l'AVP Tariff-Time-Change est présente, l'omission de cette AVP dans les messages de réponse signifie que seul le mécanisme de quota s'applique.

Tariff-Change-Usage peut avoir une des valeur suivantes :

UNIT_BEFORE_TARIFF_CHANGE : 0
Lorsque elle est présente dans l'AVP Multiple-Services-Credit-Control, cette valeur indique la quantité des unités allouée à l'utilisation avant que se produise un changement de tarif. Lorsque elle est présente dans l'AVP Used-Service-Unit, cette valeur indique la quantité d''unités de ressource utilisées avant que se produise un changement de tarif.

UNIT_AFTER_TARIFF_CHANGE : 1
Lorsque elle est présente dans l'AVP Multiple-Services-Credit-Control AVP, cette valeur indique la quantité d'unités allouée pour être utilisées après que se produit un changement de tarif. Lorsque elle est présente dans l'AVP Used-Service-Unit, cette valeur indique la quantité d'unités de ressource utilisée après que s'est produit le changement de tarif.

UNIT_INDETERMINATE : 2
L'unité utilisée contient la quantité d'unités qui enjambent le changement de tarif (par exemple, le processus de mesure fait rapport au client de contrôle de crédit en blocs de n octets, et un bloc enjambe le changement de tarif). Cette valeur n'est utilisée que dans l'AVP Used-Service-Unit.

8.28 AVP Service-Identifier

L'AVP Service-Identifier est du type Unsigned32 (code d'AVP 439) et contient l'identifiant d'un service. Le service spécifique auquel la demande se rapporte est identifié de façon univoque par la combinaison des AVP Service-Context-Id et Service-Identifier.

Un exemple d'usage de cette AVP est illustré à l'Appendice A (Flux IX).

8.29 AVP Rating-Group

L'AVP Rating-Group est du type Unsigned32 (code d'AVP 432) et contient l'identifiant d'un groupe de tarification. Tous les services soumis au même type de tarification font partie du même groupe de tarification. Le groupe de tarification spécifique auquel la demande se rapporte est identifié de façon univoque par la combinaison des AVP Service-Context-Id et Rating-Group.

Un exemple d'utilisation de cette AVP est illustré dans l'Appendice A (Flux IX).

8.30 AVP G-S-U-Pool-Reference

L'AVP G-S-U-Pool-Reference (code d'AVP 457) est du type Grouped. Elle est utilisée dans le message Réponse de contrôle de crédit, et associe l'AVP Granted-Service-Unit au sein de laquelle elle apparaît avec un réservoir de crédit dans la session.

L'AVP G-S-U-Pool-Identifier spécifie le réservoir de crédit duquel est tiré le crédit pour ce type d'unités.

L'AVP CC-Unit-Type spécifie le type d'unités pour lequel le crédit est mis en réserve.

L'AVP Unit-Value spécifie le multiplicateur, qui convertit entre unités de service de type CC-Unit-Type et les unités de service abstraites au sein du réservoir de crédit (et donc en unités de service de tout autre service ou groupe de tarification associé au même réservoir).

L'AVP G-S-U-Pool-Reference est définie comme suit (selon la grouped-avp-def de la [RFC3588]) :

```
G-S-U-Pool-Reference  ::= < en-tête d'AVP : 457 >
                          { G-S-U-Pool-Identifier }
                          { CC-Unit-Type }
                          { Unit-Value }
```

8.31 AVP G-S-U-Pool-Identifier

L'AVP G-S-U-Pool-Identifier (code d'AVP 453) est du type Unsigned32 et identifie un réservoir de crédit au sein de la session.

8.32 AVP CC-Unit-Type

L'AVP CC-Unit-Type (code d'AVP 454) est du type Enumerated et spécifie le type d'unités considérées à mettre en réserve dans un réservoir de crédit.

Les valeurs suivantes sont définies pour l'AVP CC-Unit-Type :
TIME : 0 *(temps)*
MONEY : 1 *(argent)*
TOTAL-OCTETS : 2 *(octets totaux)*
INPUT-OCTETS : 3 *(octets en entrée)*
OUTPUT-OCTETS : 4 *(octets en sortie)*
SERVICE-SPECIFIC-UNITS : 5 *(unités spécifiques du service)*

8.33 AVP Validity-Time

L'AVP Validity-Time est du type Unsigned32 (code d'AVP 448). Elle est envoyée du serveur de contrôle de crédit au client de contrôle de crédit. L'AVP contient la duré de validité des unités de service accordées. La mesure de la durée de validité commence à réception du message Credit-Control-Answer contenant cette AVP. Si les unités de service accordées n'ont pas été consommées pendant la durée de validité spécifiée dans cette AVP, le client de contrôle de crédit DOIT envoyer un message de demande de contrôle de crédit au serveur, avec CC-Request-Type réglé à UPDATE_REQUEST. Le champ de valeur de l'AVP Validity-Time est donné en secondes.

L'AVP Validity-Time est aussi utilisée pour la terminaison de service en douceur (voir au paragraphe 5.6) pour indiquer au client de contrôle de crédit pendant combien de temps l'abonné est autorisé à utiliser les ressources du réseau après le début de l'action spécifiée (c'est-à-dire, REDIRECT ou RESTRICT_ACCESS). Lorsque la durée de validité est écoulée, une nouvelle interrogation intermédiaire est envoyée au serveur.

8.34 AVP Final-Unit-Indication

L'AVP Final-Unit-Indication (code d'AVP 430) est du type Grouped et indique que l'AVP Granted-Service-Unit dans la réponse de contrôle de crédit, ou dans la réponse AA, contient les unités finales pour le service. Après l'expiration de ces unités, le client de contrôle de crédit Diameter est responsable de l'exécution de l'action indiquée dans l'AVP Final-Unit-Action (voir au paragraphe 5.6).

Si plus d'un type d'unité est reçu dans la réponse de contrôle de crédit, le type d'unité qui a d'abord expiré DEVRAIT causer l'exécution de l'action spécifiée par le client de contrôle de crédit.

Dans la première interrogation, l'AVP Final-Unit-Indication avec une Final-Unit-Action de REDIRECT ou de RESTRICT_ACCESS peut aussi être présente sans AVP Granted-Service-Unit dans la réponse de contrôle de crédit ou dans la réponse AA. Cela indique au client de contrôle de crédit Diameter d'exécuter immédiatement l'action spécifiée. Si la politique du fournisseur de service de rattachement est de terminer le service, naturellement, le serveur DEVRAIT retourner la défaillance transitoire appropriée (voir au paragraphe 9.1) afin de mettre en œuvre l'action définie par la politique.

L'AVP Final-Unit-Action AVP définit le comportement de l'élément de service lorsque le compte de l'utilisateur ne peut pas couvrir le coût du service et DOIT toujours être présente si l'AVP Final-Unit-Indication est incluse dans une commande.

Si l'AVP Final-Unit-Action est réglée à TERMINATE, aucune autre AVP ne DOIT être présente.

Si l'AVP Final-Unit-Action est réglée à REDIRECT, au moins l'AVP Redirect-Server DOIT être présente. L'AVP Restriction-Filter-Rule ou l'AVP Filter-Id PEUT être présente dans le message Réponse de contrôle de crédit si il est aussi permis à l'utilisateur d'accéder à d'autres services qui ne sont pas accessibles par l'adresse donnée dans l'AVP Redirect-Server.

Si l'AVP Final-Unit-Action est réglée à RESTRICT_ACCESS, l'AVP Restriction-Filter-Rule ou l'AVP Filter-Id DEVRAIT être présente.

L'AVP Filter-Id est définie dans la [RFC4005]. L'AVP Filter-Id peut être utilisée pour faire référence à une liste de filtres IP installés dans l'appareil d'accès par des moyens autres que l'application Diameter de contrôle de crédit, par exemple, configurés en local ou configurés par une autre entité.

L'AVP Final-Unit-Indication est définie comme suit (selon la grouped-avp-def de la [RFC3588]) :

```
Final-Unit-Indication ::= < en-tête d'AVP : 430 >
                          { Final-Unit-Action }
                         *[ Restriction-Filter-Rule ]
                         *[ Filter-Id ]
                          [ Redirect-Server ]
```

8.35 AVP Final-Unit-Action

L'AVP Final-Unit-Action (code d'AVP 449) est du type Enumerated et indique au client de contrôle de crédit l'action à entreprendre quand le compte de l'utilisateur ne peut pas couvrir le coût du service.

Final-Unit-Action peut avoir une des valeurs suivantes :

TERMINATE : 0
Le client de contrôle de crédit DOIT terminer la session de service. C'est le traitement par défaut, applicable chaque fois que le client de contrôle de crédit reçoit une valeur Final-Unit-Action non prise en charge, et elle DOIT être acceptée par toutes les mises en œuvre de client de contrôle de crédit Diameter qui se conforment à la présente spécification.

REDIRECT : 1
L'élément de service DOIT rediriger l'utilisateur sur l'adresse spécifiée dans l'AVP Redirect-Server-Address. L'action de redirection est définie au paragraphe 5.6.2.

RESTRICT_ACCESS : 2
L'appareil d'accès DOIT restreindre l'accès de l'utilisateur conformément aux filtres de paquet IP définis dans l'AVP Restriction-Filter-Rule ou conformément aux filtres de paquet IP identifiés par l'AVP Filter-Id. Tous les paquets qui ne correspondent pas aux filtres DOIVENT être éliminés (voir le paragraphe 5.6.3).

8.36 AVP Restriction-Filter-Rule

L'AVP Restriction-Filter-Rule (code d'AVP 438) est du type IPFilterRule et fournit des règles de filtre correspondant aux services qui doivent rester accessibles même si il ne reste plus d'unités de service accordées. L'appareil d'accès doit configurer les règles de filtre spécifiées pour l'abonné et DOIT éliminer tous les paquets qui ne correspondent pas à ces filtres. Zéro, une, ou plusieurs de ces AVP PEUVENT être présentes dans un message Réponse de contrôle de crédit ou dans un message de réponse AA.

8.37 AVP Redirect-Server

L'AVP Redirect-Server (code d'AVP 434) est du type Grouped et contient les informations d'adresse du serveur de redirection (par exemple, serveur de redirection HTTP, serveur SIP) avec lequel l'utilisateur final va être connecté lorsque le compte ne peut pas couvrir le coût du service. Elle DOIT être présente lorsque l'AVP Final-Unit-Action est réglée à REDIRECT.

Elle est définie comme suit (selon la grouped-avp-def de la [RFC3588]) :

Redirect-Server ::= < en-tête d'AVP : 434 >
{ Redirect-Address-Type }
{ Redirect-Server-Address }

8.38 AVP Redirect-Address-Type

L'AVP Redirect-Address-Type (code d'AVP 433) est du type Enumerated et définit le type d'adresse de l'adresse donnée dans l'AVP Redirect-Server-Address.

Le type d'adresse peut être un des suivants :

Adresse IPv4 : 0
Le type d'adresse est de la forme "décimal séparé par des points" d'adresse IPv4, comme défini dans la [RFC0791].

Adresse IPv6 : 1
Le type d'adresse est de la forme d'adresse IPv6, comme défini dans la [RFC3513]. L'adresse est une représentation en texte de l'adresse sous la forme préférée ou sous la forme de remplacement texte [RFC3513]. Les mises en œuvre conformes DOIVENT prendre en charge la forme préférée et DEVRAIENT prendre en charge la forme de remplacement texte pour les adresses IPv6.

URL : 2
Le type d'adresse est sous la forme d'un localisateur de ressource universel, comme défini dans la [RFC1738].

SIP URI : 3
Le type d'adresse est sous la forme d'un localisateur de ressource universel SIP, comme défini dans la [RFC3261].

8.39 AVP Redirect-Server-Address

L'AVP Redirect-Server-Address (code d'AVP 435) est du type UTF8String et définit l'adresse du serveur de redirection (par exemple, serveur de redirection HTTP, serveur SIP) avec lequel l'utilisateur final sera connecté lorsque le compte ne peut pas couvrir le coût du service.

8.40 AVP Multiple-Services-Indicator

L'AVP Multiple-Services-Indicator (code d'AVP 455) est du type Enumerated et indique si le client de contrôle de crédit Diameter est capable de traiter indépendamment plusieurs services au sein d'une (sous) session. L'absence de cette AVP signifie que le contrôle de crédit indépendant de plusieurs services n'est pas accepté.

Un serveur qui ne met pas en œuvre le contrôle de crédit indépendant de plusieurs services DOIT traiter l'AVP Multiple-Services-Indicator comme une AVP invalide.

Les valeurs suivantes sont définies pour l'AVP Multiple-Services-Indicator :

MULTIPLE_SERVICES_NOT_SUPPORTED : 0
Le client ne prend pas en charge le contrôle de crédit indépendant de plusieurs services au sein d'une (sous) session.

MULTIPLE_SERVICES_SUPPORTED : 1
Le client prend en charge le contrôle de crédit indépendant de plusieurs services au sein d'une (sous) session.

8.41 AVP Requested-Action

L'AVP Requested-Action (code d'AVP 436) est du type Enumerated et contient l'action demandée envoyée par la commande Demande de contrôle de crédit où le type de demande de contrôle de crédit est réglé à EVENT_REQUEST. Les valeurs suivantes sont définies pour l'AVP Requested-Action:

DIRECT_DEBITING : 0
Cela indique une demande de diminuer le compte de l'utilisateur final selon les informations spécifiées dans l'AVP

Requested-Service-Unit et/ou Service-Identifier (des informations de tarification supplémentaires peuvent être incluses dans des AVP spécifiques de service ou dans l'AVP Service-Parameter-Info). L'AVP Granted-Service-Unit dans la commande Credit-Control-Answer contient les unités débitées.

REFUND_ACCOUNT : 1
Cela indique une demande d'augmenter le compte de l'utilisateur final conformément aux informations spécifiées dans l'AVP Requested-Service-Unit et/ou Service-Identifier (des informations de tarification supplémentaires peuvent être incluses dans des AVP spécifiques de service ou dans l'AVP Service-Parameter-Info). L'AVP Granted-Service-Unit dans la commande Credit-Control-Answer contient les unités reversées.

CHECK_BALANCE : 2
Cela indique une demande de vérification de solde. Dans ce cas, la vérification du solde du compte est faite sans aucune réservation de crédit sur le compte. L'AVP Check-Balance-Result dans la commande Credit-Control-Answer contient le résultat du solde.

PRICE_ENQUIRY : 3
Cela indique une demande de prix. Dans ce cas, ni la vérification du solde du compte ni la réservation sur le compte ne seront faites ; seul le prix du service sera retourné dans l'AVP Cost-Information dans la commande Credit-Control-Answer.

8.42 AVP Service-Context-Id

L'AVP Service-Context-Id est du type UTF8String (code d'AVP 461) et contient un identifiant unique du document spécifique de service de contrôle de crédit Diameter qui s'applique à la demande (comme défini au paragraphe 4.1.2). C'est un identifiant alloué par le fournisseur du service, par le fabricant de l'élément de service, ou par un organisme de normalisation, et DOIT identifier de façon univoque un document spécifique de service de contrôle de crédit Diameter. Le format de Service-Context-Id est :

"service-context" "@" "domaine"
service-context = jeton

Le jeton est une chaîne arbitraire de caractères et chiffres.

"domaine" représente l'entité qui a alloué le Service-Context-Id. Ce peut être ietf.org, 3gpp.org, etc., si l'identifiant est alloué par un organisme de normalisation, ou il peut être le FQDN du fournisseur de service (par exemple, founisseur.exemple.com) ou du fabricant (par exemple, fabricant.exemple.com) si l'identifiant est alloué par une entité privée.

Cette AVP DEVRAIT être placée aussi près que possible de l'en-tête Diameter.

Les documents spécifiques de service qui sont seulement pour utilisation privée (c'est-à-dire, pour le propre usage d'un fournisseur, où aucune interopérabilité n'est supposée utile) peuvent définir des identifiants privés sans qu'il soit besoin de coordination. Cependant, lorsque l'interopérabilité est recherchée, une coordination des identifiants via, par exemple, la publication d'une RFC pour information est RECOMMANDÉE afin de rendre le Service-Context-Id disponible mondialement.

8.43 AVP Service-Parameter-Info

L'AVP Service-Parameter-Info (code d'AVP 440) est du type Grouped et contient des informations spécifiques du service utilisées pour le calcul du prix ou la tarification. L'AVP Service-Parameter-Type définit le type du paramètre de service, et l'AVP Service-Parameter-Value contient la valeur du paramètre. Le contenu réel de ces AVP sort du domaine d'application du présent document et DEVRAIT être défini dans une autre application Diameter, dans des normes écrites par d'autres organismes de normalisation, ou dans des documents spécifiques du service.

Dans le cas d'une demande de service inconnue (par exemple, un Service-Parameter-Type inconnu) le message de réponse correspondant DOIT contenir le code d'erreur DIAMETER_RATING_FAILED. Un message Réponse de contrôle de crédit avec cette erreur DOIT contenir une ou plusieurs AVP Failed-AVP contenant les AVP Service-Parameter-Info qui ont causé la défaillance.

Elle est définie comme suit (selon la grouped-avp-def de la [RFC3588]) :

Service-Parameter-Info ::= < en-tête d'AVP : 440 >

{ Service-Parameter-Type }
{ Service-Parameter-Value }

8.44 AVP Service-Parameter-Type

L'AVP Service-Parameter-Type est du type Unsigned32 (code d'AVP 441) et définit le type de l'événement du paramètre spécifique du service (par exemple, ce peut être la localisation de l'utilisateur final ou le nom du service). Les différents paramètres et leurs types sont spécifique du service, et la signification de ces paramètres n'est pas définie dans le présent document. Celui qui alloue le Service-Context-Id (c'est-à-dire, l'identifiant unique d'un document spécifique du service) est aussi chargé d'allouer les valeurs de Service-Parameter-Type pour le service et de s'assurer de leur unicité au sein de ce service. L'AVP Service-Parameter-Value contient la valeur associée au type du paramètre de service.

8.45 AVP Service-Parameter-Value

L'AVP Service-Parameter-Value est du type OctetString (code d'AVP 442) et contient la valeur du type du paramètre de service.

8.46 AVP Subscription-Id

L'AVP Subscription-Id (code d'AVP 443) est utilisée pour identifier l'abonnement de l'utilisateur final et est du type Grouped. L'AVP Subscription-Id inclut une AVP Subscription-Id-Data qui contient l'identifiant et une AVP Subscription-Id-Type qui définit le type d'identifiant.

Elle est définie comme suit (selon la grouped-avp-def de la [RFC3588]) :

Subscription-Id ::= < en-tête d'AVP : 443 >
{ Subscription-Id-Type }
{ Subscription-Id-Data }

8.47 AVP Subscription-Id-Type

L'AVP Subscription-Id-Type (code d'AVP 450) est du type Enumerated, et elle est utilisée pour déterminer quel type d'identifiant est porté par l'AVP Subscription-Id.

La présente spécification définit les identifiants d'abonnement suivants. Cependant, de nouvelles valeurs de Subscription-Id-Type peuvent être allouées par un expert désigné par l'IANA, comme défini dans la Section 12. Un serveur DOIT mettre en œuvre tous les Subscription-Id-Type nécessaires pour effectuer l'autorisation de crédit pour les services qu'il prend en charge, incluant de possibles valeurs futures. Les Subscription-Id-Type inconnus ou non pris en charge DOIVENT être traités en accord avec la règle de fanion 'M', comme défini dans la [RFC3588].

END_USER_E164 : 0
L'identifiant est en format international E.164 (par exemple, MSISDN), conformément au plan de numérotage UIT-T E.164 défini dans [E164] et [CE164].

END_USER_IMSI : 1
L'identifiant est en format IMSI international, conformément au plan de numérotage UIT-T E.212 comme défini dans [E212] et [CE212].

END_USER_SIP_URI : 2
L'identifiant est de la forme URI SIP, comme défini dans la [RFC3261].

END_USER_NAI : 3
L'identifiant est de la forme d'un identifiant d'accès réseau, comme défini dans la [RFC2486].

END_USER_PRIVATE: 4
L'identifiant est un identifiant privé de serveur de contrôle de crédit.

8.48 AVP Subscription-Id-Data

L'AVP Subscription-Id-Data (code d'AVP 444) est utilisée pour identifier l'utilisateur final et est du type UTF8String.

L'AVP Subscription-Id-Type définit quel type d'identifiant est utilisé.

8.49 AVP User-Equipment-Info

L'AVP User-Equipment-Info (code d'AVP 458) est du type Grouped et permet au client de contrôle de crédit d'indiquer l'identité et les capacités du terminal qu'utilise l'abonné pour la connexion au réseau.

Elle est définie comme suit (selon la grouped-avp-def de la [RFC3588]) :

User-Equipment-Info ::= < en-tête d'AVP : 458 >
{ User-Equipment-Info-Type }
{ User-Equipment-Info-Value }

8.50 AVP User-Equipment-Info-Type

L'AVP User-Equipment-Info-Type est du type Enumerated (code d'AVP 459) et définit le type d'informations d'équipement d'utilisateur contenues dans l'AVP User-Equipment-Info-Value.

La présente spécification définit les types d'équipement d'utilisateur suivants. Cependant, de nouvelles valeurs de User-Equipment-Info-Type peuvent être allouées par un expert désigné par l'IANA, comme défini dans la section 12.

IMEISV : 0
L'identifiant contient l'identifiant international d'équipement mobile et la version de logiciel dans le format international IMEISV conformément à la spécification technique 3GPP TS 23.003 [3GPPIMEI].

MAC : 1
L'adresse MAC de 48 bits est formatée comme décrit dans la [RFC3580].

EUI64 : 2
L'identifiant de 64 bits est utilisé pour identifier une instance matérielle du produit, comme défini dans [EUI64].

MODIFIED_EUI64 : 3
Un certain nombre de types de terminaux ont des identifiants autres que IMEI, MAC IEEE 802, ou EUI-64. Ces identifiants peuvent être convertis en format EUI-64 modifié comme décrit dans la [RFC3513] ou en utilisant d'autres méthodes référencées dans la documentation spécifique du service.

8.51 AVP User-Equipment-Info-Value

L'AVP User-Equipment-Info-Value (code d'AVP 460) est du type OctetString. L'AVP User-Equipment-Info-Type définit quel type d'identifiant est utilisé.

9. Valeurs d'AVP de code de résultat

La présente section définit de nouvelles valeurs d'AVP de code de résultat [RFC3588] qui doivent être prises en charge par toutes les mises en œuvre Diameter qui se conforment à la présente spécification.

Le message Réponse de contrôle de crédit inclut l'AVP Result-Code, qui peut indiquer qu'une erreur était présente dans le message de demande de contrôle de crédit. Un message de demande de contrôle de crédit rejetée DEVRAIT causer la terminaison de la session de l'utilisateur.

9.1 Défaillances temporaires

Les erreurs qui entrent dans la catégorie des défaillances transitoires sont utilisées pour informer un homologue que la demande n'a pas pu être satisfaite au moment de sa réception, mais que la demande PEUT être satisfaite à l'avenir.

DIAMETER_END_USER_SERVICE_DENIED : 4010
Le serveur de contrôle de crédit refuse la demande de service à cause de restrictions de service. Si la CCR contenait des unités de service utilisées, elles sont déduites, si possible.

DIAMETER_CREDIT_CONTROL_NOT_APPLICABLE : 4011
Le serveur de contrôle de crédit détermine que le service peut être accordé à l'utilisateur final mais qu'aucun autre contrôle de crédit n'est nécessaire pour le service (par exemple, le service est gratuit).

DIAMETER_CREDIT_LIMIT_REACHED : 4012
Le serveur de contrôle de crédit refuse la demande de service parce que le compte de l'utilisateur final ne peut pas couvrir le service demandé. Si la CCR contenait des unités de service utilisées, elles sont déduites, si possible.

9.2 Défaillances permanentes

Les erreurs qui entrent dans la catégorie des défaillances permanentes sont utilisées pour informer l'homologue que la demande a échoué et ne devrait pas être tentée à nouveau.

DIAMETER_USER_UNKNOWN : 5030
L'utilisateur final spécifié est inconnu chez le serveur de contrôle de crédit.

DIAMETER_RATING_FAILED : 5031
Ce code d'erreur est utilisé pour informer le client de contrôle de crédit que le serveur de contrôle de crédit ne peut pas tarifer la demande de service à cause d'entrées de tarification insuffisantes, d'une combinaison incorrecte d'AVP, ou d'une AVP ou d'une valeur d'AVP qui n'est pas reconnue ou prise en charge dans la tarification. L'AVP Failed-AVP DOIT être incluse et contient une copie de la ou des AVP entières qui n'ont pas pu être traitées avec succès ou un exemple de l'AVP manquante complète avec le Vendor-Id si applicable. Le champ valeur de l'AVP manquante devrait être la longueur minimum correcte et contenir des zéros.

10. Tableau d'occurrence des AVP

Le tableau qui suit présente les AVP définies dans le présent document et spécifie dans quels messages Diameter elles PEUVENT ou NE PEUT PAS être présentes. Noter que les AVP qui peuvent seulement être présentes au sein d'une AVP Grouped ne sont pas représentées dans ce tableau.

Le tableau utilise 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, une ou plusieurs instances de l'AVP PEUVENT être présentes dans le message. Il est considéré comme une erreur qu'il y ait plus d'une instance de l'AVP.
1 : Une instance de l'AVP DOIT être présente dans le message.
1+ : Au moins une instance de l'AVP DOIT être présente dans le message.

10.1 Tableau des AVP de contrôle de crédit

Ce tableau est utilisé pour représenter quelles AVP spécifiques d'applications de contrôle de crédit définies dans le présent document doivent être présentes dans les messages de contrôle de crédit.

	Code de commande	
Nom d'attribut	**CCR**	**CCA**
Acct-Multi-Session-Id	0-1	0-1
Auth-Application-Id	1	1
CC-Correlation-Id	0-1	0
CC-Session-Failover	0	0-1
CC-Request-Number	1	1
CC-Request-Type	1	1
CC-Sub-Session-Id	0-1	0-1
Check-Balance-Result	0	0-1
Cost-Information	0	0-1
Credit-Control-Failure-Handling	0	0-1
Destination-Host	0-1	0
Destination-Realm	1	0
Direct-Debiting-Failure-Handling	0	0-1
Event-Timestamp	0-1	0-1
Failed-AVP	0	0+

Final-Unit-Indication	0	0-1
Granted-Service-Unit	0	0-1
Multiple-Services-Credit-Control	0+	0+
Multiple-Services-Indicato	0-1	0|
Origin-Host	1	1
Origin-Realm	1	1
Origin-State-Id	0-1	0-1
Proxy-Info	0+	0+
Redirect-Host	0	0+
Redirect-Host-Usage	0	0-1
Redirect-Max-Cache-Time	0	0-1
Requested-Action	0-1	0
Requested-Service-Unit	0-1	0
Route-Record	0+	0+
Result-Code	0	1
Service-Context-Id	1	0
Service-Identifier	0-1	0
Service-Parameter-Info	0+	0
Session-Id	1	1
Subscription-Id	0+	0
Termination-Cause	0-1	0
User-Equipment-Info	0-1	0
Used-Service-Unit	0+	0
User-Name	0-1	0-1
Validity-Time	0	0-1

10.2 Tableau des AVP de Re-Auth-Request/Answer

Ce paragraphe définit les AVP qui sont spécifique de l'application Diameter de contrôle de crédit et qui PEUVENT être incluses dans le message Diameter Re-Auth-Request/Answer (RAR/RAA) [RFC3588].

La commande Re-Auth-Request/Answer PEUT inclure les AVP supplémentaires suivantes :

	Code de commande	
Nom d'attribut	**RAR**	**RAA**
CC-Sub-Session-Id	0-1	0-1
G-S-U-Pool-Identifier	0-1	0-1
Service-Identifier	0-1	0-1
Rating-Group	0-1	0-1

11. Modèle d'interfonctionnement de contrôle de crédit RADIUS/Diameter

Cette section définit les principes de base du modèle d'inter fonctionnement de contrôle de crédit Diameter/RADIUS prepaid ; c'est-à-dire, une traduction de messages entre une solution prépayée fondée sur RADIUS et une application Diameter de contrôle de crédit. Une description complète des traductions de protocole entre RADIUS et l'application Diameter de contrôle de crédit sort du domaine d'application de la présente spécification et DEVRAIT être traitée dans un autre document approprié, comme la spécification de RADIUS prepaid.

L'architecture du contrôle de crédit Diameter peut avoir un agent de traduction capable de traduire entre les protocoles RADIUS prepaid et contrôle de crédit Diameter. Un serveur AAA (généralement le serveur AAA de rattachement) peut agir comme agent de traduction et comme client de contrôle de crédit Diameter pour les éléments de service qui utilisent des mécanismes de contrôle de crédit autres que le contrôle de crédit Diameter, par exemple, RADIUS prepaid. Dans ce cas, le serveur AAA de rattachement contacte le serveur de contrôle de crédit Diameter au titre du processus d'autorisation. L'architecture d'interfonctionnement est illustrée Figure 7, et les flux d'interfonctionnement Figure 8. Dans une situation d'itinérance, l'élément de service (par exemple, le NAS) peut être situé dans le réseau visité, et un serveur AAA visité est généralement contacté. Le serveur AAA visité se connecte alors au serveur AAA de rattachement.

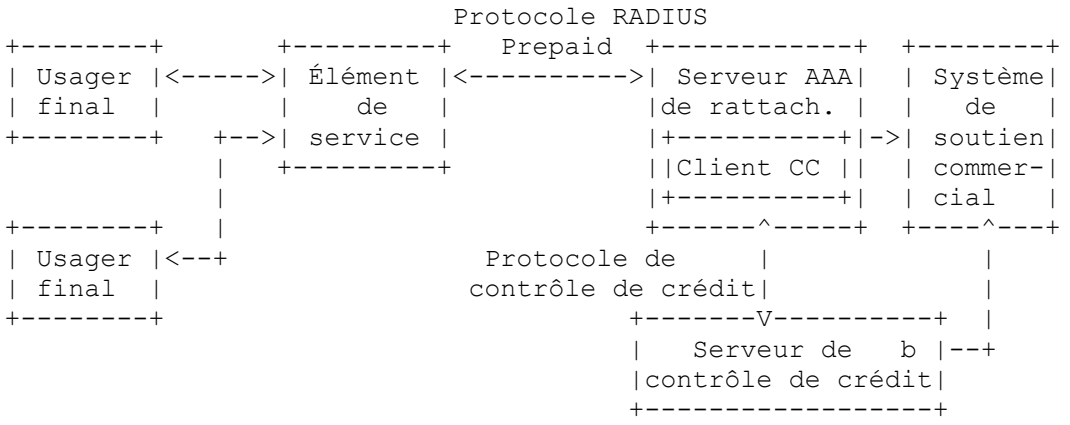
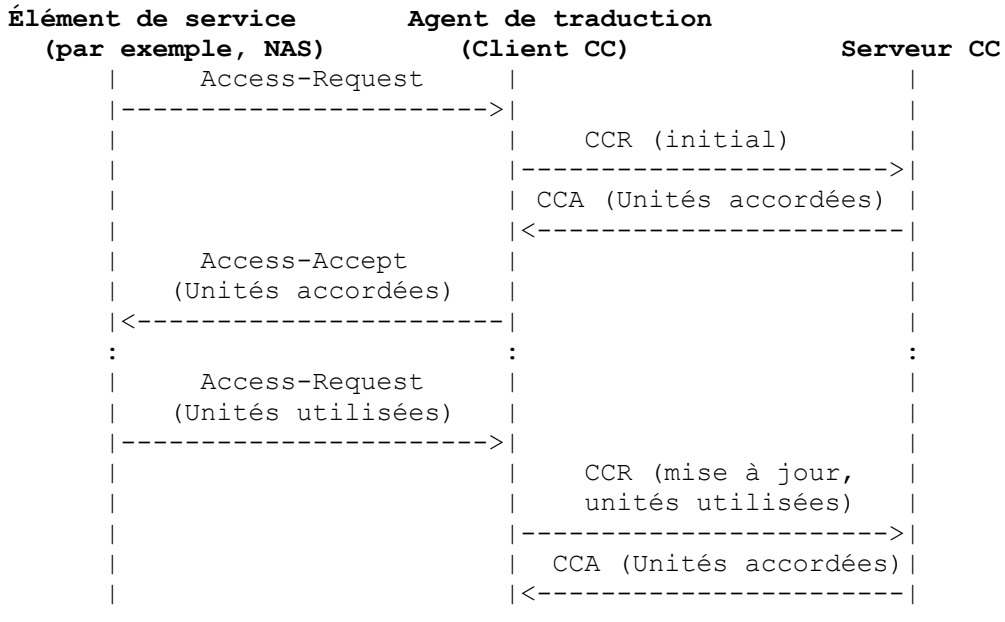


Figure 7 : Architecture de contrôle de crédit avec l'élément de service qui contient l'agent de traduction, traduit le protocole RADIUS prepaid en contrôle de crédit Diameter

Lorsque le serveur AAA agissant comme agent de traduction reçoit un message initial RADIUS Access-Request d'un élément de service (par exemple, un NAS) il effectue une authentification et autorisation régulières. Si le message RADIUS Access-Request indique que l'élément de service est capable de contrôle de crédit, et si le serveur AAA de rattachement trouve que l'abonné est un abonné prépayé, une demande de contrôle de crédit Diameter DEVRAIT être envoyée au serveur de contrôle de crédit pour effectuer l'autorisation de crédit et pour établir une session de contrôle de crédit. Après que le serveur de contrôle de crédit Diameter a vérifié la provision du compte de l'utilisateur final, tarifé le service, et réservé le crédit sur le compte de l'utilisateur final, le quota réservé est retourné au serveur AAA de rattachement dans la réponse de contrôle de crédit Diameter. Ensuite, le serveur AAA de rattachement envoie le quota réservé à l'élément de service dans le message RADIUS Access-Accept.

À l'expiration du quota alloué, l'élément de service envoie une nouvelle demande d'accès RADIUS contenant les unités utilisées jusque là au serveur AAA de rattachement. Le serveur AAA de rattachement devra transposer une demande d'accès RADIUS contenant les unités rapportées au serveur de contrôle de crédit Diameter dans une demande de contrôle de crédit (UPDATE_REQUEST) Diameter. Le serveur de contrôle de crédit Diameter débite les unités utilisées du compte de l'utilisateur final et alloue un nouveau quota qui est retourné au serveur AAA de rattachement dans la réponse de contrôle de crédit Diameter. Le quota est transféré à l'élément de service dans le RADIUS Access-Accept. Lorsque l'AVP d'utilisateur final termine le service, ou lorsque le quota a été entièrement utilisé, l'élément de service envoie une demande d'accès RADIUS. Pour débiter les unités utilisées du compte de l'utilisateur final et pour arrêter la session de contrôle de crédit, le serveur AAA de rattachement envoie une demande de contrôle de crédit Diameter (TERMINATION_REQUEST) au serveur de contrôle de crédit. Le serveur de contrôle de crédit Diameter accuse réception de la terminaison de session en envoyant une réponse de contrôle de crédit Diameter au serveur AAA de rattachement. La RADIUS Access-Accept est envoyée au NAS.

Le diagramme ci-après illustre une séquence d'interfonctionnement RADIUS prepaid - contrôle de crédit Diameter.



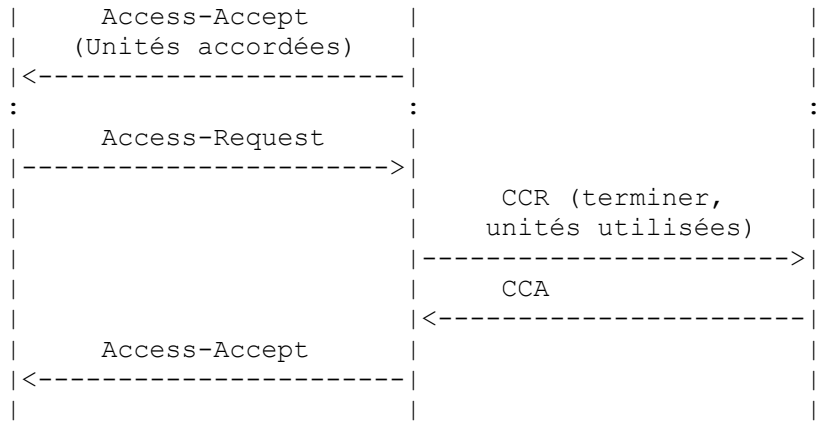


Figure 8 : Exemple de flux de message avec interfonctionnement RADIUS prepaid - Diameter contrôle de crédit

12. Considérations relatives à l'IANA

La présente section contient les espaces de noms qui ont été soit créés dans cette spécification, soit les valeurs allouées aux espaces de noms existants gérés par l'IANA.

Dans les paragraphes qui suivent, quand on parle de revue par un expert désigné, on notera que celui-ci est désigné par l'IESG. Initialement, de telles discussions sur l'expert ont lieu sur la liste de diffusion du groupe de travail AAA.

12.1 Identifiant d'application

La présente spécification alloue la valeur 4, "contrôle de crédit Diameter", à l'espace de nom Identifiant d'application défini dans la [RFC3588]. Voir plus d'informations au paragraphe 1.3.

12.2 Codes de commandes

La présente spécification utilise la valeur 272 de l'espace de noms Codes de commandes défini dans la [RFC3588] pour les commandes Demande de contrôle de crédit (CCR) et Réponse de contrôle de crédit (CCA).

12.3 Codes d'AVP

La présente spécification alloue les valeurs 411 à 461 de l'espace de noms Codes d'AVP défini dans la [RFC3588]. Voir à la Section 8 l'allocation de l'espace de noms dans la présente spécification.

12.4 Valeurs d'AVP Result-Code

La présente spécification alloue les valeurs 4010, 4011, 4012, 5030, 5031 de l'espace de noms Valeurs d'AVP Result-Code défini dans la [RFC3588]. Voir à la Section 9 l'allocation de l'espace de noms dans la présente spécification.

12.5 AVP CC-Request-Type

Comme défini au paragraphe 8.3, l'AVP CC-Request-Type inclut les valeur de type Enumerated 1 - 4. L'IANA a créé et tient un espace de noms pour cette AVP. Toutes les valeurs restantes sont disponibles pour être allouées par un expert désigné [RFC2434].

12.6 AVP CC-Session-Failover

Comme défini au paragraphe 8.4, L'AVP CC-Failover-Supported inclut les valeurs de type Enumerated 0 - 1. L'IANA a créé et tient un espace de noms pour cette AVP. Toutes les valeurs restantes sont disponibles pour allocation par un expert désigné [RFC2434].

12.7 AVP CC-Unit-Type

Comme défini au paragraphe 8.32, l'AVP CC-Unit-Type inclut les valeurs de type Enumerated 0 - 5. L'IANA a créé et tient un espace de noms pour cette AVP. Toutes les valeurs restantes sont disponibles pour allocation par un expert désigné [RFC2434].

12.8 AVP Check-Balance-Result

Comme défini au paragraphe 8.6, l'AVP Check-Balance-Result inclut les valeurs de type Enumerated 0 - 1. L'IANA a créé et tient un espace de noms pour cette AVP. Toutes les valeurs restantes sont disponibles pour allocation par un expert désigné [RFC2434].

12.9 AVP Credit-Control

Comme défini au paragraphe 8.13, l'AVP Credit-Control AVP inclut les valeurs de type Enumerated 0 - 1. L'IANA a créé et tient un espace de noms pour cette AVP. Toutes les valeurs restantes sont disponibles pour allocation par un expert désigné [RFC2434].

12.10 AVP Credit-Control-Failure-Handling

Comme défini au paragraphe 8.14, l'AVP Credit-Control-Failure-Handling inclut les valeurs de type Enumerated 0 - 2. L'IANA a créé et tient un espace de noms pour cette AVP. Toutes les valeurs restantes sont disponibles pour allocation par un expert désigné [RFC2434].

12.11 AVP Direct-Debiting-Failure-Handling

Comme défini au paragraphe 8.15, l'AVP Direct-Debiting-Failure-Handling inclut les valeurs de type Enumerated 0 - 1. L'IANA a créé et tient un espace de noms pour cette AVP. Toutes les valeurs restantes sont disponibles pour allocation par un expert désigné [RFC2434].

12.12 AVP Final-Unit-Action

Comme défini au paragraphe 8.35, l'AVP Final-Unit-Action AVP inclut les valeurs de type Enumerated 0 - 2. L'IANA a créé et tient un espace de noms pour cette AVP. Toutes les valeurs restantes sont disponibles pour allocation par un expert désigné [RFC2434].

12.13 AVP Multiple-Services-Indicator

Comme défini au paragraphe 8.40, l'AVP Multiple-Services-Indicator inclut les valeurs de type Enumerated 0 - 1. L'IANA a créé et tient un espace de noms pour cette AVP. Toutes les valeurs restantes sont disponibles pour allocation par un expert désigné [RFC2434].

12.14 AVP Redirect-Address-Type

Comme défini au paragraphe 8.38, l'AVP Redirect-Address-Type inclut les valeurs de type Enumerated 0 - 3. L'IANA a créé et tient un espace de noms pour cette AVP. Toutes les valeurs restantes sont disponibles pour allocation par un expert désigné [RFC2434].

12.15 AVP Requested-Action

Comme défini au paragraphe 8.41, l'AVP Requested-Action inclut les valeurs de type Enumerated 0 - 3. L'IANA a créé et tient un espace de noms pour cette AVP. Toutes les valeurs restantes sont disponibles pour allocation par un expert désigné[RFC2434].

12.16 AVP Subscription-Id-Type

Comme défini au paragraphe 8.47, l'AVP Subscription-Id-Type inclut les valeurs de type Enumerated 0 - 4. L'IANA a créé et tient un espace de noms pour cette AVP. Toutes les valeurs restantes sont disponibles pour allocation par un expert

désigné [RFC2434].

12.17 AVP Tariff-Change-Usage

Comme défini au paragraphe 8.27, l'AVP Tariff-Change-Usage inclut les valeurs de type Enumerated 0 - 2. L'IANA a créé et tient un espace de noms pour cette AVP. Toutes les valeurs restantes sont disponibles pour allocation par un expert désigné [RFC2434].

12.18 AVP User-Equipment-Info-Type

Comme défini au paragraphe 8.50, l'AVP User-Equipment-Info-Type inclut les valeurs de type Enumerated 0 - 3. L'IANA a créé et tient un espace de noms pour cette AVP. Toutes les valeurs restantes sont disponibles pour allocation par un expert désigné [RFC2434].

13. Paramètres relatifs aux applications de contrôle de crédit

Temporisateur Tx
Lorsque le contrôle de crédit en temps réel est requis, le client de contrôle de crédit contacte le serveur de contrôle de crédit avant et pendant que le service est fourni à un utilisateur final. Du fait de la nature en temps réel de l'application, les délais de communication DEVRAIENT être minimisés ; par exemple, pour éviter que l'utilisateur final subisse un temps d'établissement exagérément long. Le temporisateur Tx est introduit pour contrôler le temps d'attente au client dans l'état "En cours". Lorsque le temporisateur Tx s'écoule, le client de contrôle de crédit effectue une action sur l'utilisateur final conformément à la valeur de l'AVP Credit-Control-Failure-Handling ou Direct-Debiting-Failure-Handling. La valeur recommandée est de 10 secondes.

Temporisateur Tcc
Le temporisateur Tcc supervise une session de contrôle de crédit en cours chez le serveur de contrôle de crédit. Il est RECOMMANDÉ d'utiliser la durée de validité comme entrée pour établir la valeur du temporisateur Tcc. Dans le cas de défaillances transitoires dans le réseau, le serveur de contrôle de crédit Diameter peut passer à l'état Repos. Pour éviter cela, le temporisateur Tcc PEUT être réglé à deux fois la durée de validité.

Credit-Control-Failure-Handling et Direct-Debiting-Failure-Handling
Les mises en œuvre de client peuvent offrir la possibilité de configurer ces AVP en local. Dans ce cas, leur valeur et comportement sont définis au paragraphe 5.7 pour Credit-Control-Failure-Handling et au paragraphe 6.5 pour Direct-Debiting-Failure-Handling.

14. Considérations sur la sécurité

Le protocole de base Diameter [RFC3588] exige que chaque mise en œuvre Diameter utilise la sécurité sous-jacente ; c'est-à-dire, IPsec ou TLS. Ces mécanismes sont estimés fournir une protection suffisante sous le modèle de menaces normal de l'Internet ; c'est-à-dire, en supposant que les nœuds autorisés s'engageant dans le protocole n'ont pas été compromis, mais que l'attaquant a le contrôle complet sur le canal de communication entre eux. Ceci inclut les attaques d'espionnage, de modification de message, d'insertion, d'interposition et de répétition. Noter aussi que cette application inclut un mécanisme pour la protection contre la répétition au niveau application au moyen du Session-Id de la [RFC3588] et du CC-Request-Number, qui est spécifié dans le présent document. L'application Diameter de contrôle de crédit est souvent utilisée au sein d'un seul domaine, et il peut y avoir un seul bond entre les homologues. Dans ces environnements, l'utilisation de TLS ou IPsec est suffisante. Les détails de TLS et IPsec relatifs aux considérations de sécurité sont discutés dans la [RFC3588].

Comme cette application traite des transactions monétaires (directement ou indirectement) elle accroît l'intérêt pour diverses attaques contre la sécurité. Donc, toutes les parties communiquant les unes avec les autres DOIT être authentifiées, incluant, par exemple, l'authentification TLS côté client. De plus, l'autorisation du client DEVRAIT être accentuée ; c'est-à-dire que le client est autorisé à effectuer le contrôle de crédit pour un certain utilisateur. La signification spécifique de l'autorisation sort du domaine d'application de la présente spécification mais peut être, par exemple, une configuration manuelle.

Une autre sorte de menace est la modification malveillante, l'injection, ou la suppression d'AVP ou de messages complets de contrôle de crédit. Les messages de contrôle de crédit contiennent des informations sensibles relatives à la facturation (comme l'identifiant de souscription, les unités accordées, les unités utilisées, les informations de coût) dont la modification

malveillante peut avoir des conséquences financières. Parfois la simple suppression de messages de contrôle de crédit peut causer des perturbations chez le client ou serveur de contrôle de crédit.

Même sans aucune modification des messages, un adversaire peut créer une menace pour la sécurité en espionnant, car les transactions contiennent des informations privées sur l'utilisateur. Aussi, en surveillant les messages de contrôle de crédit, on peut collecter des informations sur les modèles de facturation du serveur de contrôle de crédit et sur les relations d'affaires.

Lorsque des relais ou mandataires tiers sont impliqués, la sécurité bond par bond ne fournit pas nécessairement une protection suffisante pour la session d'utilisateur Diameter. Dans certains cas, il peut être inapproprié d'envoyer des messages Diameter, comme des CCR et CCA, contenant des AVP sensibles via des agents mandataires Diameter qui ne sont pas de confiance, car il n'est pas assuré que des mandataires tiers ne vont pas modifier les commandes ou valeurs d'AVP de contrôle de crédit .

14.1 Connexion directe avec redirections

Un agent de contrôle de crédit Diameter ne peut pas toujours savoir si les agents entre lui et le serveur de contrôle de crédit Diameter de l'utilisateur final sont fiables. Dans ce cas, l'agent de contrôle de crédit Diameter n'a pas une entrée d'acheminement dans son tableau d'acheminement Diameter (défini dans la [RFC3588], paragraphe 2.7) pour le domaine du serveur de contrôle de crédit dans le domaine de rattachement de l'utilisateur final. L'agent Diameter de contrôle de crédit peut avoir un chemin par défaut configuré sur un agent local de redirection, et il redirige le message CCR sur l'agent de redirection. L'agent local de redirection retourne alors une notification de redirection (code de résultat 3006, DIAMETER_REDIRECT_INDICATION) à l'agent de contrôle de crédit, ainsi que les informations de serveur de contrôle de crédit Diameter (AVP Redirect-Host) et des informations (AVP Redirect-Host-Usage) sur la façon dont l'entrée d'acheminement résultant de la Redirect-Host sont à utiliser. L'agent de contrôle de crédit Diameter transmet alors directement le message CCR à un des hôtes identifiés par le message CCA provenant de l'agent de redirection. Si la valeur de l'AVP Redirect-Host-Usage n'est pas égale à zéro, tous les messages qui suivent sont envoyés à l'hôte spécifié dans l'AVP Redirect-Host jusqu'à ce que le délai spécifié par l'AVP Redirect-Max-Cache-Time soit expiré.

Il y a des problèmes d'autorisation même avec les redirections. Il peut y avoir des attaques contre des nœuds qui ont été autorisés à juste titre, mais qui abusent de leur autorisation ou ont été compromis. Ces questions sont discutées plus en détails à la section 8 de la [RFC4072].

15. Références

15.1 Références normatives

[3GPPCHARG] 3rd Generation Partnership Project; "Technical Specification Group Services et System Aspects, Service aspects; Charging et Billing (release 5)", 3GPP TS 22.115 v. 5.2.1, mars 2002.

[3GPPIMEI] 3rd Generation Partnership Project; "Technical Specification Group Core Network, Numbering, addressing et identification, (release 5)", 3GPP TS 23.003 v. 5.8.0, décembre 2003.

[CE164] Complément à la Recommandation UIT-T E.164 (05/1997) :"Liste des codes de pays alloués", juin 2000.

[CE212] Complément à la Recommandation UIT-T E.212 (11/1997):" Liste des codes de pays ou zones géographiques pour les mobiles", février 1999.

[E164] Recommandation UIT-T E.164/I.331 (05/97) " Plan de numérotage des télécommunications publiques internationales". 1997.

[E212] Recommandation UIT-T E.212 (11/98) "Plan d'identification international pour les terminaux mobiles et les utilisateurs mobiles". 1998.

[EUI64] IEEE, "Guidelines for 64-bit Global Identifier (EUI-64) Registration Authority", http://standards.ieee.org/regauth/oui/tutorials/EUI64.html , mars 1997.

[ISO4217] Norme internationale ISO 4217, "Codes pour la représentation des monnaies et des devises", 2001

[RFC0791] J. Postel, éd., "Protocole Internet - Spécification du protocole du programme Internet", STD 5, septembre 1981.

[RFC1738] T. Berners-Lee et autres, "Localisateurs uniformes de ressource (URL)", décembre 1994. *(P.S., Obsolète, voir les* RFC4248 et 4266)

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

[RFC2434] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, octobre, 1998. *(Rendue obsolète par la* RFC5226)

[RFC2486] B. Aboba, M. Beadles, "Identifiant d'accès réseau", janvier 1999. (*Obsolète, voir* RFC4282) *(P.S.)*

[RFC3261] J. Rosenberg et autres, "SIP : Protocole d'initialisation de session", juin 2002. (*Mise à jour par* RFC3265, RFC3853, RFC4320, RFC4916, RFC5393, RFC6665)

[RFC3513] R. Hinden et S. Deering, "Architecture d'adressage du protocole Internet version 6 (IPv6)", avril 2003. (*Obs. voir* RFC4291)

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

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

15.2 Références pour information

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

[RFC3725] J. Rosenberg et autres, "Bonne pratiques actuelles pour la commande d'appel de tiers (3pcc) dans le protocole d'initialisation de session (SIP)", avril 2004. (BCP0085)

[RFC4004] P. Calhoun et autres, "Application IPv4 mobile Diameter", août 2005. *(P.S.)*

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

16. Remerciements

Les auteurs tiennent à remercier Bernard Aboba, Jari Arkko, Robert Ekblad, Pasi Eronen, Benny Gustafsson, Robert Karlsson, Avi Lior, Paco Marin, Jussi Maki, Jeff Meyer, Anne Narhi, John Prudhoe, Christopher Richards, Juha Vallinen, et Mark Watson de leurs commentaires et suggestions.

Appendice A. Séquences de contrôle de crédit

A.1 Flux I

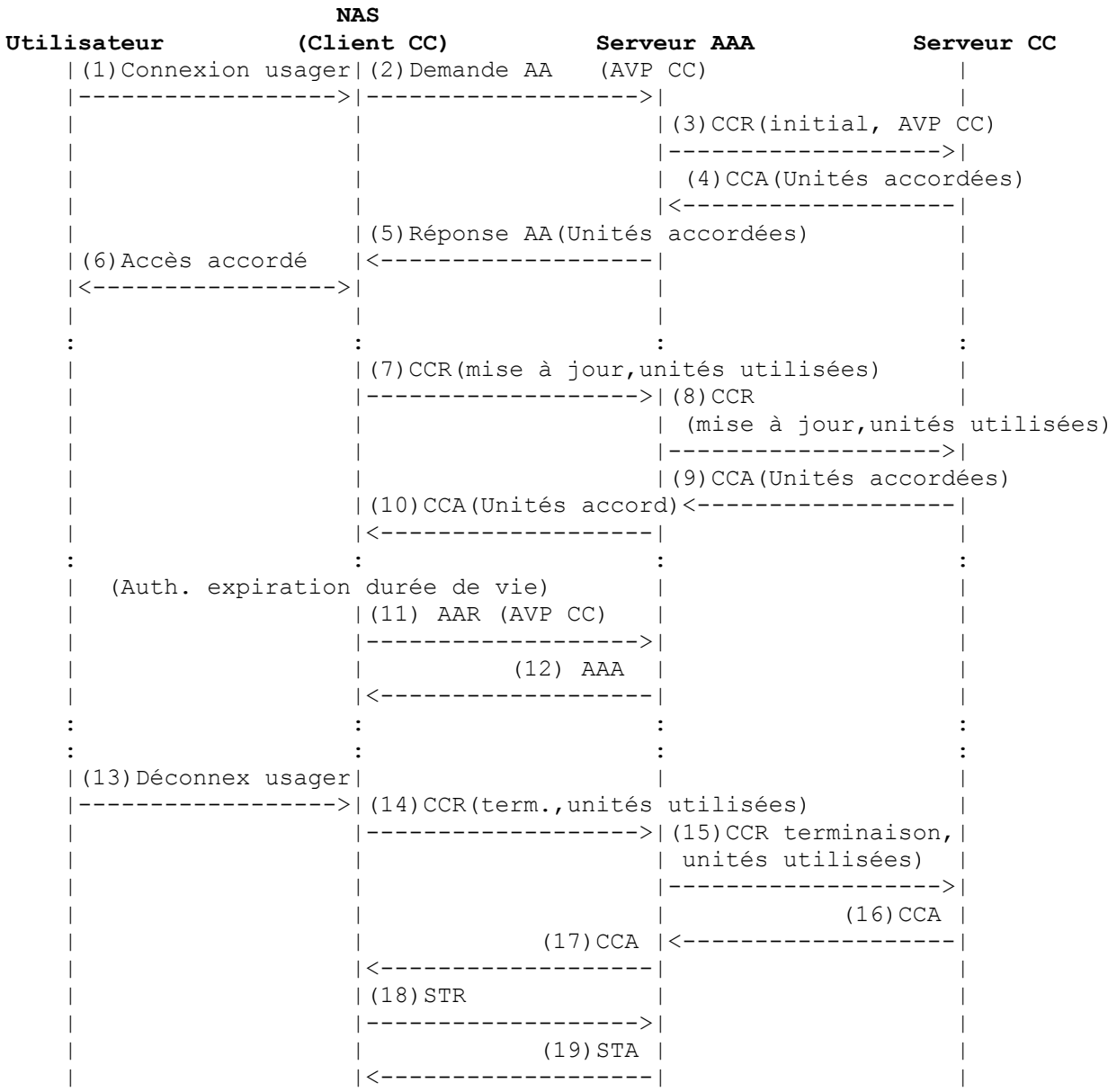


Figure A.1 : Flux I

La Figure A.1.A montre un flux de contrôle de crédit pour des services d'accès réseau prépayés. Diameter [RFC4005] est mis en œuvre dans le serveur d'accès réseau (NAS). L'objet de ce flux est l'autorisation de crédit.

L'usager se connecte sur le réseau (1). Le NAS Diameter envoie une demande Diameter AA (AAR) au serveur AAA Diameter de rattachement. Le client de contrôle de crédit remplit la AAR avec l'AVP Credit-Control réglée à CREDIT_AUTHORIZATION, et des AVP spécifiques du service sont incluses, comme d'habitude [RFC4005]. Le serveur AAA Diameter de rattachement effectue l'authentification et l'autorisation spécifiques du service, comme d'habitude. Le serveur AAA Diameter de rattachement détermine que l'utilisateur est un usager prépayé et remarque à partir de l'AVP Credit-Control que le NAS a des capacités de contrôle de crédit. Il envoie une demande de contrôle de crédit Diameter avec CC-Request-Type réglé à INITIAL_REQUEST au serveur de contrôle de crédit Diameter pour effectuer l'autorisation de crédit (3) et pour établir une session de contrôle de crédit. (Le serveur AAA Diameter de rattachement peut transmettre des AVP spécifiques du service reçues du NAS en entrée du processus de tarification.) Le serveur de contrôle de crédit Diameter vérifie la provision du compte de l'utilisateur final, tarifie le service, et réserve du crédit sur le compte de l'utilisateur final. Le quota réservé est retourné au serveur AAA Diameter de rattachement dans la réponse de contrôle de crédit Diameter (4). Le serveur AAA Diameter de rattachement envoie le quota réservé au NAS dans la réponse AA

Diameter (AAA). Lorsque AAA réussit, le NAS commence la session de contrôle de crédit et commence à surveiller les unités accordées (5).

Le NAS accorde l'accès à l'utilisateur final (6). À l'expiration du quota alloué, le NAS envoie une demande de contrôle de crédit Diameter avec le CC-Request-Type réglé à UPDATE_REQUEST au serveur AAA Diameter de rattachement (7). Ce message contient les unités utilisées jusque alors. Le serveur AAA Diameter de rattachement transmet la CCR au serveur de contrôle de crédit Diameter (8). Le serveur de contrôle de crédit Diameter débite les unités utilisées du compte de l'utilisateur final et alloue un nouveau quota qui est retourné au serveur AAA Diameter de rattachement dans la réponse de contrôle de crédit Diameter (9). Le message est transmis au NAS (10). Durant la session de contrôle de crédit en cours, la durée de vie de l'autorisation arrive à expiration, et le client d'autorisation/authentification dans le NAS effectue une réautorisation spécifique du service au serveur AAA Diameter de rattachement, comme usuel. Le client de contrôle de crédit remplit l'AAR avec l'AVP Credit-Control réglée à RE_AUTHORIZATION, indiquant que le serveur de contrôle de crédit ne devra pas être contacté, car l'autorisation de crédit est contrôlée par le taux de consommation des unités accordées (11). Le serveur AAA Diameter de rattachement effectue une réautorisation spécifique du service comme usuel et retourne la réponse AA au NAS (12). L'utilisateur final se déconnecte du réseau (13). Pour débiter les unités utilisées du compte de l'utilisateur final et arrêter la session de contrôle de crédit, le NAS envoie une demande de contrôle de crédit Diameter avec le CC-Request-Type réglé à TERMINATION_REQUEST au serveur AAA Diameter de rattachement (14). Le serveur AAA Diameter de rattachement transmet la CCR au serveur de contrôle de crédit (15). Le serveur de contrôle de crédit Diameter accuse réception de la terminaison de la session en envoyant une réponse de contrôle de crédit Diameter au serveur AAA Diameter de rattachement (16). Le serveur AAA Diameter de rattachement transmet la réponse au NAS (17). STR/STA a lieu entre le NAS et le serveur AAA Diameter de rattachement, comme usuel (18-19).

A.2 Flux II

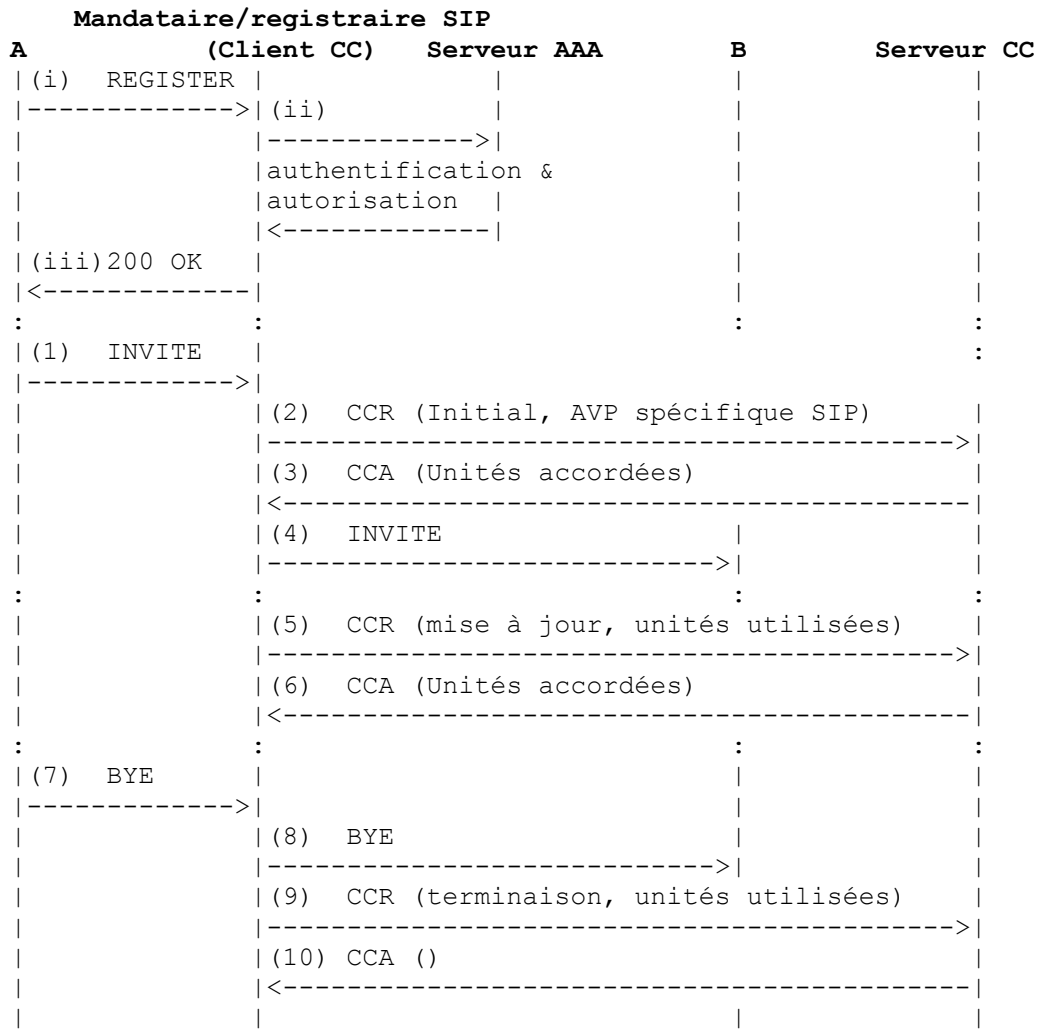


Figure A.2 : Flux II

Ceci est un exemple de contrôle de crédit Diameter pour sessions SIP. Bien que le flux se concentre sur l'illustration de l'usage des messages de contrôle de crédit, la signalisation SIP est imprécise, et le diagramme ne tente en aucune façon de définir le réseau SIP d'un fournisseur de service. Cependant, pour les besoins de cet exemple, on fait ci-dessous certaines

hypothèses.

Normalement les services prépayés fondés, par exemple, sur la durée d'usage pour la session SIP, exigent qu'une entité dans le réseau du fournisseur de service intercepte toutes les demandes au sein du dialogue SIP afin de détecter les événements, comme un établissement de session et une libération de session, qui sont essentiels pour effectuer les opérations de contrôle de crédit avec le serveur de contrôle de crédit. Donc, dans cet exemple, on suppose que le mandataire SIP ajoute un en-tête Record-Route dans le INVITE initial SIP pour s'assurer que toutes les futures demandes dans le dialogue créé le traversent (pour les définitions de 'Record-Route' et 'dialog' prière de se reporter à la [RFC3261]). Finalement, le degré de mesure de contrôle de crédit du support par le mandataire dépend de la conception du modèle d'affaires utilisé dans l'établissement du système d'extrémité et des mandataires dans le réseau SIP.

L'utilisateur final (agent d'utilisateur SIP A) envoie un REGISTER avec des accréditifs (i). Le mandataire SIP envoie une demande au serveur AAA de rattachement pour effectuer une authentification et autorisation multimédia en utilisant, par exemple, l'application Diameter Multimédia (ii). Le serveur AAA de rattachement vérifie que les accréditifs sont corrects et vérifie le profil de l'utilisateur. Finalement, une réponse 200 OK (iii) est envoyée à l'UA. Noter que l'authentification et l'autorisation sont valides pour la durée de la période de validité de l'enregistrement (c'est-à-dire, jusqu'à ce que le réenregistrement soit effectué). Plusieurs sessions SIP peuvent être établies sans réautorisation.

L'UA A envoie un INVITE (1). Le mandataire SIP envoie une demande de contrôle de crédit Diameter (INITIAL_REQUEST) au serveur de contrôle de crédit Diameter (2). La demande de contrôle de crédit contient les informations obtenues de la signalisation SIP décrivant le service demandé (par exemple, l'appelant, l'appelé, les attributs du protocole de description de session). Le serveur de contrôle de crédit Diameter vérifie la provision du compte de l'utilisateur final, tarifie le service, et réserve le crédit sur le compte de l'utilisateur final. Le quota réservé est retourné au mandataire SIP dans la réponse de contrôle de crédit Diameter (3). Le mandataire SIP transmet le SIP INVITE à l'UA B (4). Le téléphone de B sonne, et B répond. Le support s'écoule entre eux, et le mandataire SIP commence à mesurer le quota. À l'expiration du quota alloué, le mandataire SIP envoie une demande de contrôle de crédit Diameter (UPDATE_REQUEST) au serveur de contrôle de crédit Diameter (5). Ce message contient les unités utilisées jusque alors. Le serveur de contrôle de crédit Diameter débite les unités utilisées du compte de l'utilisateur final et alloue un nouveau crédit qui est retourné au mandataire SIP dans la réponse de contrôle de crédit Diameter (6). L'utilisateur final termine le service en envoyant un BYE (7). Le mandataire SIP transmet le message BYE à l'UA B (8) et envoie une demande de contrôle de crédit Diameter (TERMINATION_REQUEST) au serveur de contrôle de crédit (9). Le serveur de contrôle de crédit Diameter accuse réception de la terminaison de session en envoyant une réponse de contrôle de crédit Diameter au mandataire SIP (10).

A.3 Flux III

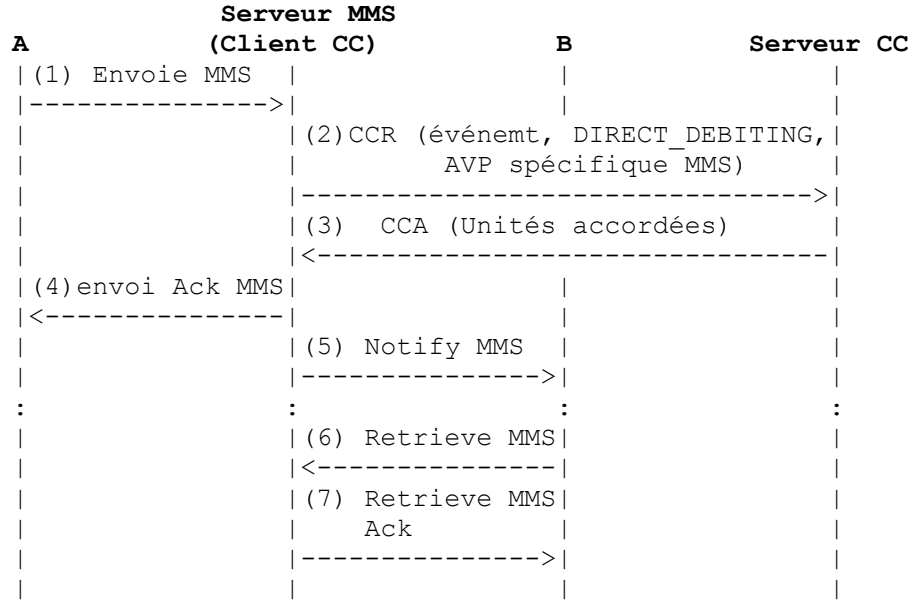


Figure A.3 : Flux III

La Figure A.3 montre un flux de contrôle de crédit pour les services de messagerie multimédia. L'envoyeur est facturé aussitôt que le serveur de messagerie réussit à mémoriser le message.

L'utilisateur final A envoie un message multimédia (MMS, *Multimedia Message Service*) au serveur MMS (1). Le serveur

MMS mémorise le message et envoie une demande de contrôle de crédit Diameter (EVENT_REQUEST avec l'action demandée DIRECT_DEBITING) au serveur Diameter de contrôle de crédit (2). La demande de contrôle de crédit contient les informations sur le message MMS (par exemple, taille, adresse du receveur, type de codage d'image). Le serveur de contrôle de crédit Diameter vérifie la provision du compte de l'utilisateur final, tarifie le service, et débite le service du compte de l'utilisateur final. Le quota accordé est retourné au serveur MMS dans la réponse de contrôle de crédit Diameter (3). Le serveur MMS accuse bonne réception du message MMS (4). Le serveur MMS notifie au receveur le nouveau MMS (5), et l'utilisateur final B récupère le message de la mémorisation de messages MMS (6),(7).

A.4 Flux IV

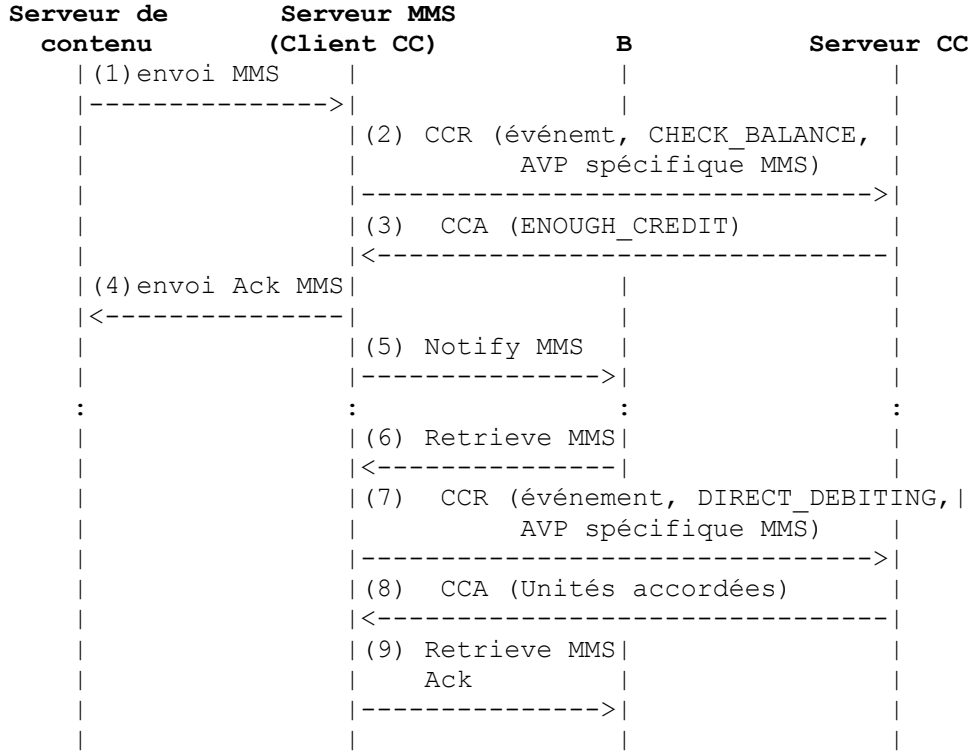


Figure A.4 : Flux IV

Voici un exemple de contrôle de crédit Diameter pour débit direct utilisant l'environnement du service de messagerie multimédia. Bien que le flux se concentre sur l'illustration de l'usage de messages de contrôle de crédit, la signalisation MMS est imprécise, et le diagramme n'essaye en aucune façon de définir une configuration MMS de fournisseur de service ou de modèle de facturation.
Un flux de contrôle de crédit pour le service de messagerie multimédia est montré à la Figure A.4. Le receveur est facturé à la livraison du message.
Un serveur de contenu envoie un message multimédia (MMS) au serveur MMS (1) qui mémorise le message. Le receveur du message sera facturé pour le message MMS dans ce cas. Comme il peut y avoir un délai substantiellement long entre la réception du message au serveur MMS et la restitution réelle du message, le serveur MMS n'établit aucune session de contrôle de crédit avec le serveur de contrôle de crédit Diameter mais effectue d'abord seulement une vérification du solde (sans aucune réservation de crédit) en envoyant une demande de contrôle de crédit Diameter (EVENT_REQUEST avec l'action demandée CHECK_BALANCE) pour vérifier que l'utilisateur final B peut couvrir le coût du MMS (2). Le serveur de contrôle de crédit Diameter vérifie la provision du compte de l'utilisateur final et retourne la réponse au serveur MMS dans la réponse de contrôle de crédit Diameter (3). Le serveur MMS accuse réception du message MMS (4). Le serveur MMS notifie au receveur le nouveau MMS (5), et après un certain temps, l'utilisateur final B restitue le message de la mémorisation de messages MMS (6). Le serveur MMS envoie une demande de contrôle de crédit Diameter (EVENT_REQUEST avec l'action demandée : DIRECT_DEBITING) au serveur de contrôle de crédit Diameter (7). La demande de contrôle de crédit contient les informations sur le message MMS (par exemple, taille, adresse du receveur, type de codage). Le serveur de contrôle de crédit Diameter vérifie la provision du compte de l'utilisateur final, tarifie le service, et débite le service du compte de l'utilisateur final. Le quota accordé est retourné au serveur MMS dans la demande de contrôle de crédit Diameter (8). Le MMS est transféré à l'utilisateur final B (9).

Noter que le transfert du message MMS peut prendre un long délai et peut échouer ; dans ce cas, une action de récupération est nécessaire. Le serveur MMS devrait retourner les unités déjà débitées au compte de l'utilisateur en utilisant

l'action REFUND décrite au paragraphe 6.4.

A.5 Flux V

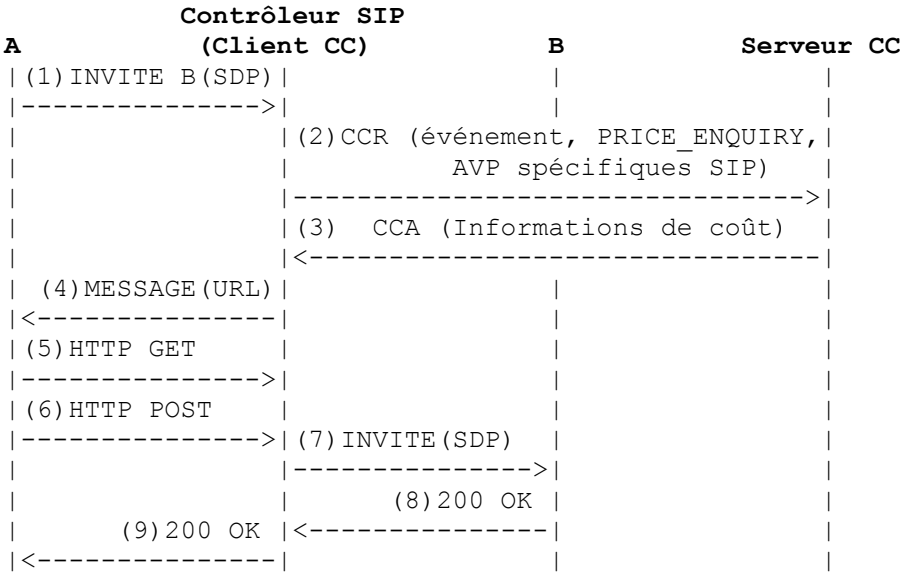


Figure A.5 : Flux V

Voici un exemple de contrôle de crédit Diameter pour sessions SIP. Bien que le flux se concentre sur l'illustration de l'usage de messages de contrôle de crédit, la signalisation SIP est imprécise, et le diagramme n'essaye en aucune façon de définir le réseau SIP d'un fournisseur de service.

La Figure A.5 est un exemple de service d'avis de taxation (AoC, *Advice of Charge*) pour les appels SIP. L'usager A peut être un abonné prépayé ou qui paye à posteriori qui utilise le service AoC. On suppose que le contrôleur SIP a aussi la capacité HTTP et délivre une page AoC interactive sur la Toile avec, par exemple, les informations de coût, les détails de l'appel déduits de SDP, et un bouton pour accepter ou ne pas accepter les charges. (Il peut y avoir de nombreuses autres façons de livrer les informations sur AoC ; cependant, ce flux se concentre sur l'utilisation de messages de contrôle de crédit.) L'usager a été authentifié et autorisé avant l'initialisation de l'appel et a souscrit au service AoC.

L'UA A envoie un INVITE avec SDP à B (1). Le contrôleur SIP détermine que l'utilisateur est abonné au service AoC et envoie une demande de contrôle de crédit Diameter (EVENT_REQUEST avec l'action demandée : PRICE_ENQUIRY) au serveur de contrôle de crédit Diameter (2). La demande de contrôle de crédit contient les AVP spécifiques de SIP déduites de la signalisation SIP, décrivant le service demandé (par exemple, appelant, demandé, attributs du protocole de description de session). Le serveur de contrôle de crédit Diameter détermine le coût du service et retourne la réponse de contrôle de crédit incluant l'AVP Cost-Information (3). Le contrôleur SIP fabrique la page AoC sur la Toile avec les informations reçues dans la signalisation SIP et avec les informations de coût reçues du serveur de contrôle de crédit. Il envoie ensuite un message SIP qui contient un URL pointant sur la page d'informations AoC de la Toile (4). À réception du message SIP, l'UA de A invoque automatiquement le navigateur de la Toile qui restitue les informations d'AoC (5). L'usager clique sur le bouton approprié et accepte les charges (6). Le contrôleur SIP continue la session et envoie le INVITE à la partie B, qui accepte l'appel (7, 8, 9).

A.6 Flux VI

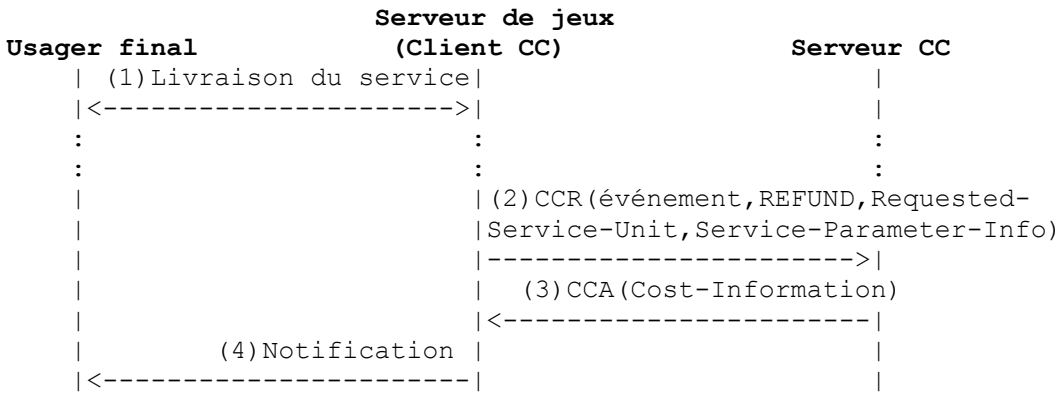


Figure A.6 : Flux VI

La Figure A.6 illustre un flux de contrôle de crédit pour le cas REFUND. On suppose qu'il y a une relation de confiance et une connexion sûre entre le serveur de jeux et le serveur de contrôle de crédit Diameter. L'utilisateur final peut être un abonné prépayé ou un abonné qui paye à posteriori.

Pendant que l'utilisateur final exécute le jeu (1), il passe à un nouveau niveau qui lui donne droit à un bonus. Le serveur de jeux envoie une demande de contrôle de crédit Diameter (EVENT_REQUEST avec l'action demandée : REFUND_ACCOUNT) au serveur de contrôle de crédit Diameter (2). La demande de contrôle de crédit contient l'AVP Requested-Service-Unit avec le CC-Service-Specific-Units contenant le nombre de points que l'utilisateur vient de gagner. L'AVP Service-Parameter-Info est aussi incluse dans la demande et spécifie l'événement de service à tarifier (par exemple, Bonus Tetris). À partir des informations reçues, le serveur de contrôle de crédit Diameter détermine le montant à créditer, le reverse sur le compte de l'utilisateur, et retourne la Credit-Control-Answer, incluant l'AVP Cost-Information (3). Cost-Information indique le montant crédité. À la première opportunité, le serveur de jeux notifie à l'utilisateur final le montant crédité (4).

A.7 Flux VII

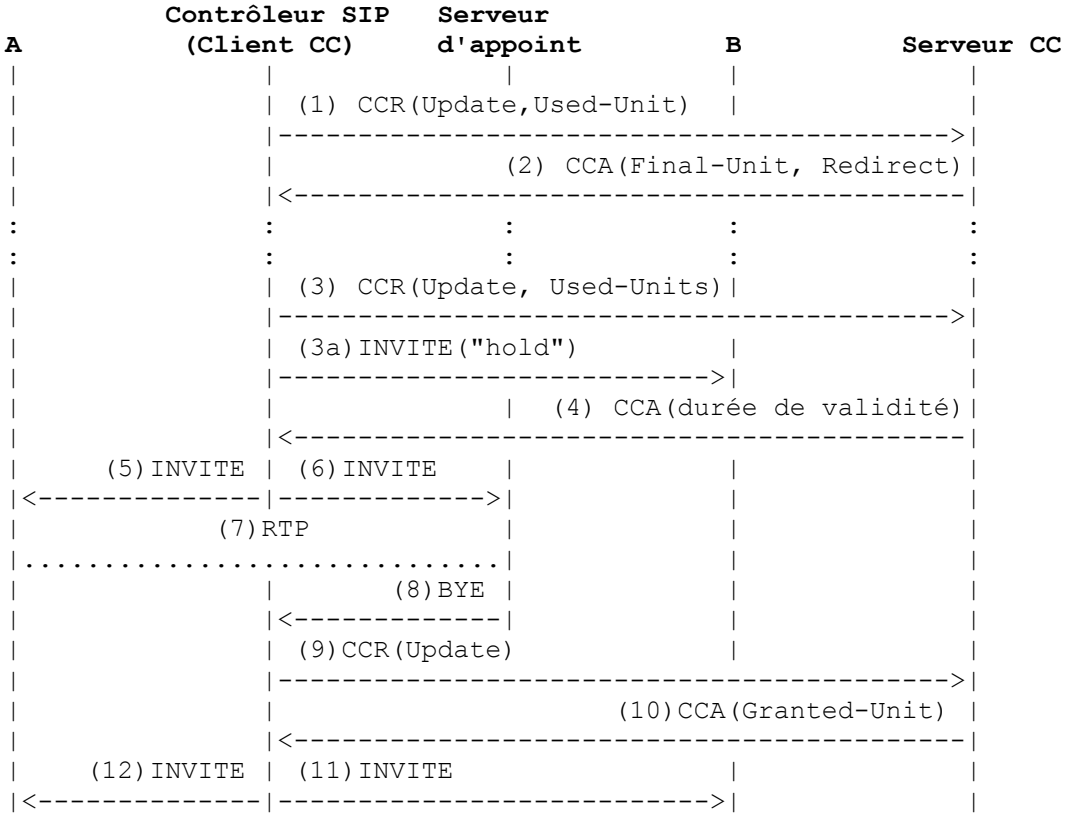


Figure A.7 : Flux VII

La Figure A.7 est un exemple de la terminaison de service en douceur pour un appel SIP. On suppose que l'appel est établi de façon que le contrôleur soit dans l'appel comme un agent d'utilisateur de boucle locales (B2BUA, *Back to Back User Agent*) qui effectue une commande d'appel de tiers (3PCC, *third-party call control*). Noter que la signalisation SIP est imprécise, car l'objet de ce flux est la terminaison de service en douceur et l'autorisation de contrôle de crédit. Les bonnes pratiques pour 3PCC sont définies dans la [RFC3725].

L'appel est en cours entre les usagers A et B ; l'usager A a un abonnement prépayé. À l'expiration du quota alloué, le contrôleur SIP envoie une demande de contrôle de crédit Diameter (UPDATE_REQUEST) au serveur de contrôle de crédit Diameter (1). Ce message contient les unités utilisées jusque là. Le serveur de contrôle de crédit Diameter débite les unités utilisées du compte de l'utilisateur final et alloue le quota final retourné au contrôleur SIP dans la réponse de contrôle de crédit Diameter (2). Ce message contient l'AVP Final-Unit-Indication avec la Final-Unit-Action réglée à REDIRECT, la Redirect-Address-Type réglée à SIP URI, et la Redirect-Server-Address réglée au nom du serveur d'appoint (par exemple, sip:sip-serveur-d'appoint@domaine.com). À l'expiration du quota final alloué, le contrôleur SIP envoie une demande de contrôle de crédit Diameter (UPDATE_REQUEST) au serveur de contrôle de crédit Diameter (3) et place l'appelé "en garde" en envoyant un INVITE avec l'adresse de connexion appropriée dans le SDP (3a). La demande de message de

contrôle de crédit contient les unités utilisées jusque là. Le serveur de contrôle de crédit Diameter débite les unités utilisées du compte de l'utilisateur final, mais ne fait aucune réservation de crédit. Le message Réponse de contrôle de crédit, qui contient la durée de validité pour superviser la terminaison de service en douceur, est retournée au contrôleur SIP (4). Le contrôleur SIP établit une session SIP entre l'usager prépayé et le serveur d'appoint (5, 6). Le serveur d'appoint fait une annonce et invite l'utilisateur à entrer un numéro de carte de crédit et la somme à utiliser pour réapprovisionner le compte (7). Le serveur d'appoint valide le numéro de carte de crédit et réapprovisionne le compte de l'utilisateur (en utilisant des moyens qui sortent du domaine d'application de la présente spécification) et libère la session SIP (8). Le contrôleur SIP peut maintenant supposer que la communication entre l'usager prépayé et le serveur d'appoint a eu lieu. Il envoie une demande de contrôle de crédit spontanée (UPDATE_REQUEST) au serveur de contrôle de crédit Diameter pour vérifier si le compte a été réapprovisionné (9). Le serveur de contrôle de crédit Diameter réserve le crédit sur le compte de l'utilisateur final et retourne le quota réservé au contrôleur SIP dans la réponse de contrôle de crédit (10). À ce point, le contrôleur SIP reconnecte l'appelant et l'appelé (11, 12).

A.8 Flux VIII

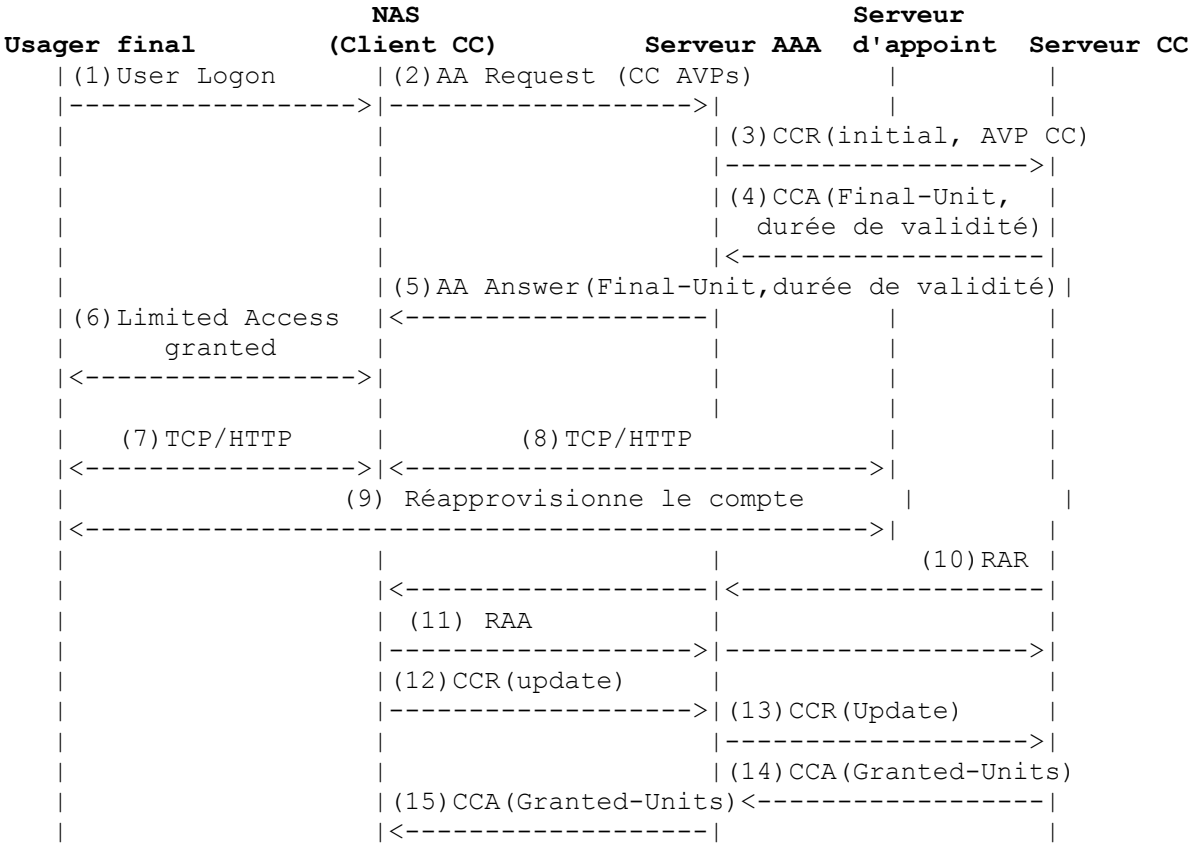


Figure A.8 : Flux VIII

La Figure A.8 est un exemple de terminaison de service en douceur initiée lorsque la première interrogation a lieu parce que le compte de l'utilisateur est vide. Dans cet exemple, le serveur de contrôle de crédit prend en charge la réautorisation de crédit initiée par le serveur. Diameter [RFC4005] est mis en œuvre dans le serveur d'accès réseau (NAS).

L'usager se connecte au réseau (1). Le NAS Diameter envoie une demande AA Diameter au serveur AAA Diameter de rattachement. Le client de contrôle de crédit remplit la AAR avec l'AVP Credit-Control réglée à CREDIT_AUTHORIZATION, et des AVP spécifiques du service sont incluses, comme usuel [RFC4005]. Le serveur AAA Diameter de rattachement effectue l'authentification et l'autorisation spécifiques du service, comme usuel. Le serveur AAA Diameter de rattachement détermine que l'utilisateur a un abonnement prépayé et remarque de l'AVP Credit-Control que le NAS a des capacités de contrôle de crédit. Il envoie une demande de contrôle de crédit Diameter avec CC-Request-Type réglée à INITIAL_REQUEST au serveur de contrôle de crédit Diameter pour effectuer l'autorisation de crédit (3) et pour établir une session de contrôle de crédit. (Le serveur AAA Diameter de rattachement peut transmettre des AVP spécifiques du service reçues du NAS en entrée du processus de tarification.) Le serveur de contrôle de crédit Diameter vérifie la provision du compte de l'utilisateur final, détermine que le compte ne peut pas couvrir le coût du service, et initie la terminaison de service en douceur. La réponse de contrôle de crédit est retournée au serveur AAA Diameter de rattachement (4). Ce message contient l'AVP Final-Unit-Indication et l'AVP durée de validité réglée à une durée raisonnable pour donner à l'utilisateur une chance de réapprovisionner son compte (par exemple, 10 minutes). L'AVP Final-Unit-

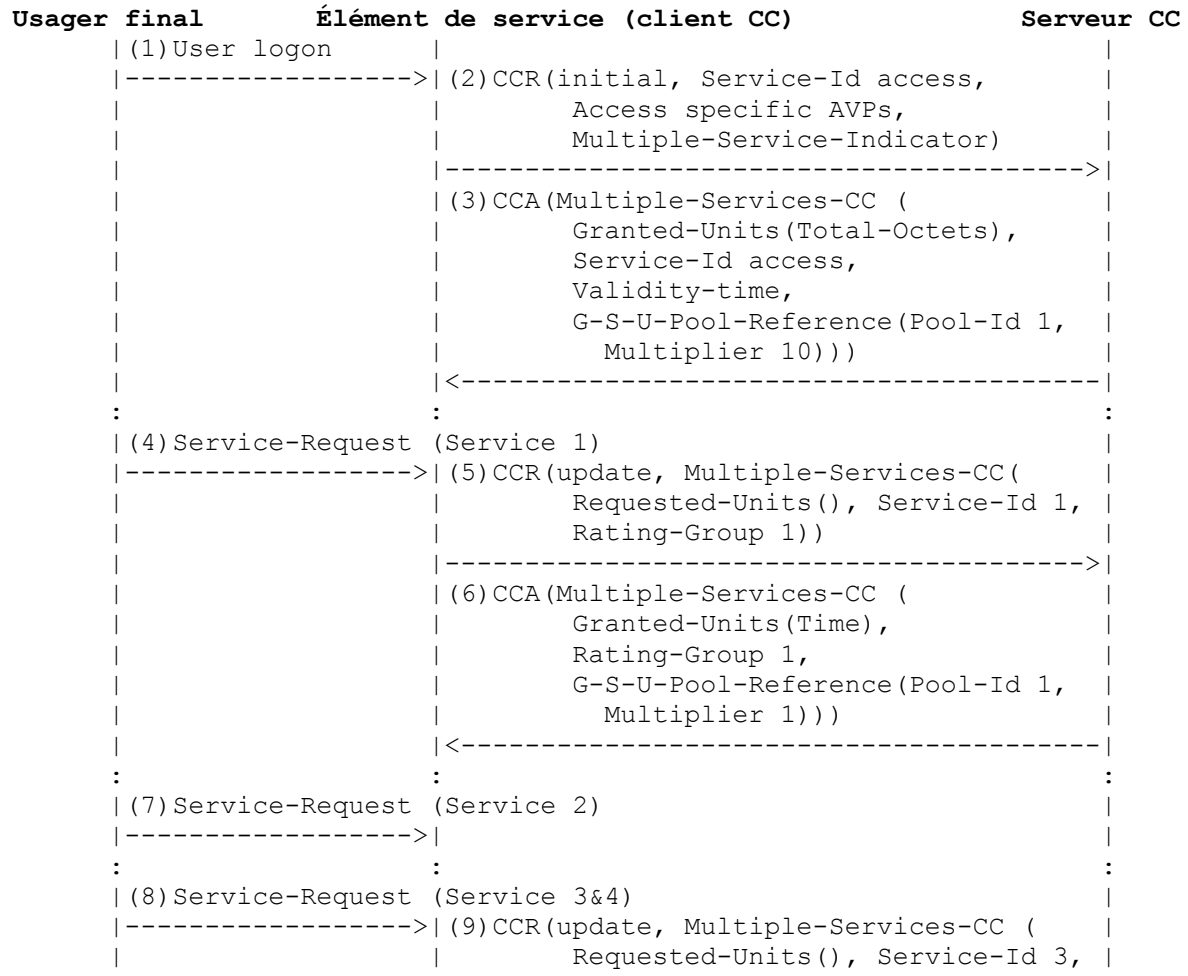
Indication inclut la Final-Unit-Action réglée à REDIRECT, la Redirect-Address-Type réglée à URL, et la Redirect-Server-Address réglée au nom du serveur d'appoint HTTP. Le serveur AAA Diameter de rattachement envoie les AVP de contrôle de crédit reçues au NAS dans la réponse AA Diameter (5). AAA ayant réussi, le NAS commence la session de contrôle de crédit et commence immédiatement la terminaison de service en douceur, selon les instructions du serveur. Le NAS accorde un accès limité à l'utilisateur (6). Le logiciel de client HTTP qui fonctionne dans l'appareil de l'utilisateur ouvre la connexion de transport redirigée par le NAS sur le serveur d'appoint (7, 8). Une page de la Toile appropriée est affichée à l'usager sur laquelle entrer son numéro de carte de crédit, et la somme à utiliser pour réapprovisionner le compte, et avec un message de notification qu'il lui est donné un accès illimité si l'opération de réapprovisionnement est exécutée avec succès dans les prochaines, par exemple, 10 minutes. Le serveur d'appoint valide le numéro de carte de crédit et réapprovisionne le compte de l'utilisateur (en utilisant des moyens qui sortent du domaine d'application de la présente spécification) (9). Après la réussite du réapprovisionnement du compte, le serveur de contrôle de crédit envoie un message Re-Auth-Request au NAS (10). Le NAS accuse réception de la demande en retournant le message Re-Auth-Answer (11) et initie la réautorisation de crédit en envoyant une Credit-Control-request (UPDATE_REQUEST) au serveur de contrôle de crédit Diameter (12, 13).

Le serveur de contrôle de crédit Diameter réserve le crédit sur le compte de l'utilisateur final et retourne le quota réservé au NAS via le serveur AAA Diameter de rattachement dans la réponse de contrôle de crédit (14, 15). Le NAS supprime les restrictions placées par la terminaison de service en douceur et commence à surveiller les unités accordées.

A.9 Flux IX

L'application Diameter de contrôle de crédit définit l'AVP Multiple-Services-Credit-Control qui peut être utilisée pour la prise en charge du contrôle de crédit indépendant de plusieurs services dans une seule (sous) session de contrôle de crédit pour des éléments de service qui ont de telles capacités. Il est possible de demander et allouer des ressources dans un réservoir de crédit qui est partagé entre services ou groupes de tarification.

L'exemple de flux ci-dessous illustre un scénario d'utilisation où le client et le serveur de contrôle de crédit prennent en charge le contrôle de crédit indépendant de plusieurs services, comme défini au paragraphe 5.1.2. On suppose que les identifiants de service, les groupes de tarification et leurs paramètres associés (par exemple, quintuplés IP) sont configurés en local dans l'élément de service ou provisionnés par une entité autre que le serveur de contrôle de crédit.



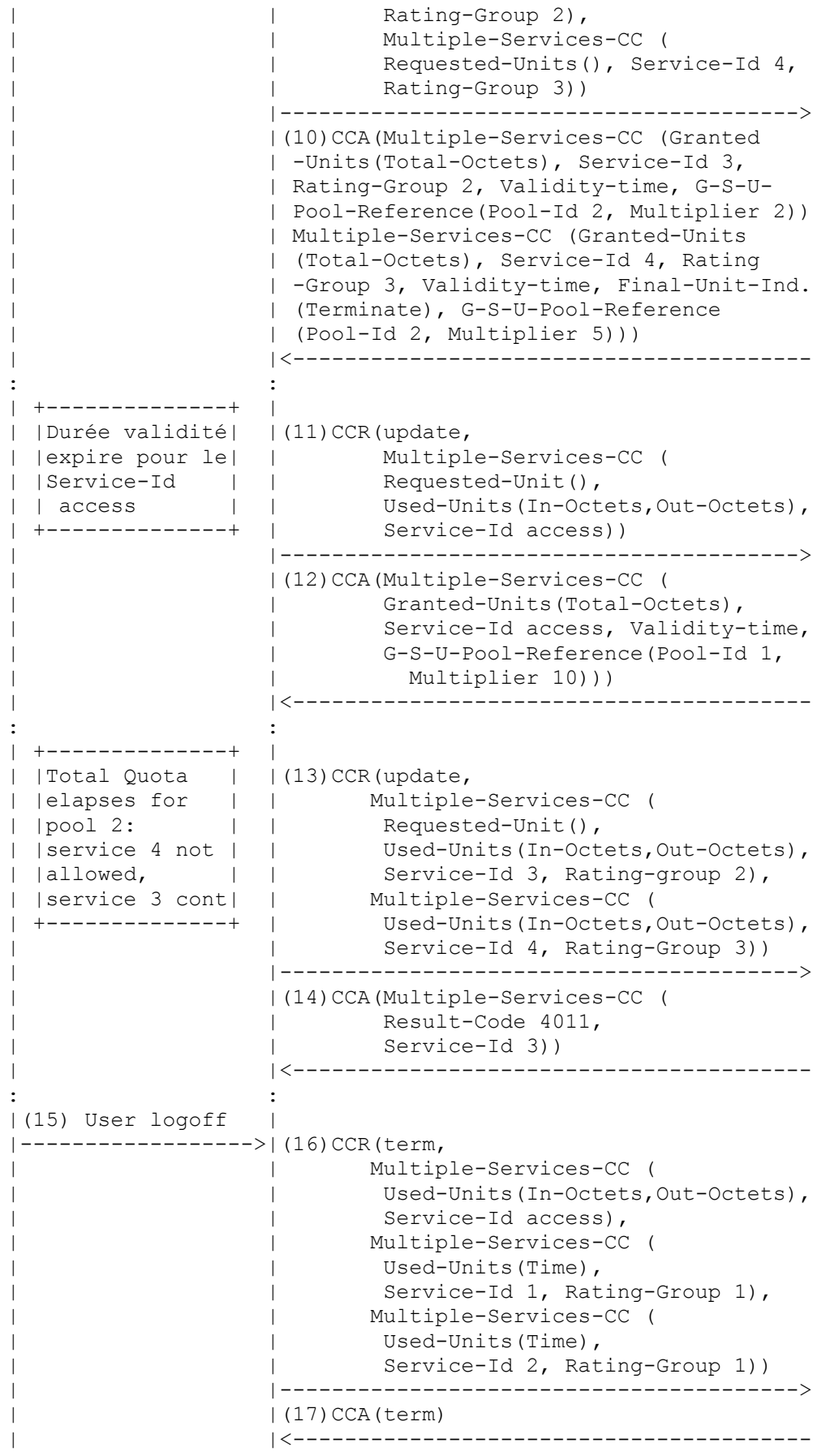


Figure A.9 : Exemple de flux indépendant de contrôle de crédit de plusieurs services dans une (sous) session de contrôle de crédit

L'usager se connecte au réseau (1). L'élément de service envoie une demande de contrôle de crédit Diameter avec le type de

demande de contrôle de crédit réglé à INITIAL_REQUEST au serveur de contrôle de crédit Diameter pour effectuer une autorisation de crédit pour le service support (par exemple, service d'accès Internet) et pour établir une session de contrôle de crédit (2). Dans ce message, le client de contrôle de crédit indique la prise en charge du contrôle de crédit indépendant de plusieurs services au sein de la session en incluant l'AVP Multiple-Service-Indicator. Le serveur de contrôle de crédit Diameter vérifie la provision du compte de l'utilisateur final, avec les informations de tarification reçues du client (c'est-à-dire, les AVP Service-Id et spécifiques de l'accès) tarifie la demande, et réserve le crédit sur le compte de l'utilisateur final. Supposons que le serveur réserve 5 € et détermine que le coût est 1 € /Moctet. Il retourne alors à l'élément de service un message Réponse de contrôle de crédit qui inclut l'AVP Multiple-Services-Credit-Control avec un quota de 5 Moctets associé à l'identifiant de service (accès) une valeur de multiplicateur de 10, et le Pool-Id 1 (3).

L'usager utilise le Service 1 (4). L'élément de service envoie une demande de contrôle de crédit Diameter avec CC-Request-Type réglé à UPDATE_REQUEST au serveur de contrôle de crédit pour effectuer l'autorisation de crédit pour le Service 1 (5). Ce message inclut l'AVP Multiple-Services-Credit-Control pour demander les unités de service pour Service 1 qui appartient au groupe de tarification 1. Le serveur de contrôle de crédit Diameter détermine que Service 1 tire ses ressources de crédit du même compte que le service d'accès (c'est-à-dire, le réservoir 1). Il tarifie la demande conformément à l'identifiant de service/groupe de tarification et met à jour la réservation existante en demandant plus de crédit. Supposons que le serveur réserve 5 € de plus (la réservation est maintenant de 10 €) et détermine que le coût est de 0,1 €/minute. Le serveur autorise tout le groupe de tarification. Il retourne alors à l'élément de service un message Réponse de contrôle de crédit qui inclut l'AVP Multiple-Services-Credit-Control avec un quota de 50 minutes associé au groupe de tarification 1, à une valeur de multiplicateur de 1, et au Pool-Id 1 (6). Le client ajuste la quantité totale de ressources pour le réservoir 1 conformément au quota reçu, qui donne S pour Pool 1 = 100.

L'usager utilise le Service 2, qui appartient au groupe de tarification autorisé 1 (7). Les ressources sont alors consommées sur le réservoir 1.

L'usager demande maintenant aussi les services 3 et 4, qui ne sont pas autorisés (8). L'élément de service envoie une demande de contrôle de crédit Diameter avec CC-Request-Type réglé à UPDATE_REQUEST au serveur de contrôle de crédit afin d'effectuer l'autorisation de crédit pour les services 3 et 4 (9). Ce message inclut deux instances de l'AVP Multiple-Services-Credit-Control pour demander des unités de service pour Service 3 qui appartient au groupe de tarification 2 et pour Service 4 qui appartient au groupe de tarification 3. Le serveur de contrôle de crédit Diameter détermine que les services 3 et 4 tirent des ressources de crédit d'un autre compte (c'est-à-dire, pool 2). Il vérifie la provision du compte de l'utilisateur final et, conformément aux informations des Service-Id/Rating-Group, tarifie la demande. Il réserve ensuite le crédit sur le réservoir 2.

Par exemple, le serveur réserve 5 € et détermine que Service 3 coûte 0,2 €/Moctet et Service 4 coûte 0,5 €/Moctet. Le serveur autorise seulement les services 3 et 4. Il retourne à l'élément de service un message Réponse de contrôle de crédit qui inclut deux instances de l'AVP Multiple-Services-Credit-Control (10). Une instance accorde un quota de 12,5 Moctets associé au Service-Id 3, à une valeur de multiplicateur de 2 et au Pool-Id 2. L'autre instance accorde un quota de 5 Moctets associé au Service-Id 4, à une valeur de multiplicateur de 5 et au Pool-Id 2.

Le serveur détermine aussi que pool 2 est épuisé et Service 4 n'a pas la permission de continuer après que ces unités seront consommées. Donc l'AVP Final-Unit-Indication avec l'action TERMINATE est associée au Service-Id 4. Le client calcule la quantité totale de ressources qui peuvent être utilisées pour pool 2 conformément aux quotas et multiplicateurs reçus, qui donne S pour Pool 2 = 50.

La durée de validité pour le service "access" expire. L'élément de service envoie une demande de message de contrôle de crédit au serveur afin d'effectuer la réautorisation de crédit pour Service-Id (access) (11). Ce message porte une instance de l'AVP Multiple-Services-Credit-Control qui inclut les unités utilisées par ce service. Supposons que la quantité totale d'unités utilisée soit de 4 Moctets. Le client ajuste en conséquence la quantité totale de ressources pour le réservoir 1, ce qui donne S pour Pool 1 = 60.

Le serveur déduit 4 € du compte de l'utilisateur et met à jour la réservation en demandant plus de crédit. Supposons que le serveur réserve 5 € de plus (la réservation est maintenant de 11 €) et qu'il connaisse déjà le coût du Service-Id (access), qui est de 1 €/Moctet. Il retourne alors à l'élément de service un message Réponse de contrôle de crédit qui inclut l'AVP Multiple-Services-Credit-Control avec un quota de 5 Moctets associé au Service-Id (access), à une valeur de multiplicateur de 10, et au Pool-Id 1 (12). Le client ajuste la quantité totale de ressources pour le réservoir 1 conformément au quota reçu, qui donne S pour Pool 1 = 110.

Les services 3 et 4 consomment le montant total des ressources de crédit du réservoir 2 (c'est-à-dire, C1*2 + C2*5 ≥ S). L'élément de service commence immédiatement l'action TERMINATE concernant Service 4 et envoie une demande de message de contrôle de crédit avec CC-Request-Type réglé à UPDATE_REQUEST au serveur de contrôle de crédit afin d'effectuer la réautorisation de crédit pour Service 3 (13). Ce message contient deux instances de l'AVP Multiple-Services-Credit-Control pour faire rapport des unités utilisées par les services 3 et 4. Le serveur déduit les derniers 5 € du compte de

l'utilisateur (pool 2) et retourne la réponse avec le code de résultat 4011 dans l'AVP Multiple-Services-Credit-Control pour indiquer que Service 3 peut continuer sans contrôle de crédit (14).

L'utilisateur final se déconnecte du réseau (15). Pour débiter les unités utilisées du compte de l'utilisateur final et arrêter la session de contrôle de crédit, l'élément de service envoie une demande de contrôle de crédit Diameter avec le CC-Request-Type réglé à 3 TERMINATION_REQUEST au serveur de contrôle de crédit (16). Ce message contient les unités consommée par chacun des services utilisés dans les instances de l'AVP Multiple-Services-Credit-Control. Les unités utilisées sont associées à l'identifiant de service et groupe de tarification pertinents. Le serveur de contrôle de crédit Diameter débite les unités utilisées du compte de l'utilisateur (Pool 1) et accuse réception de la terminaison de session en envoyant une réponse de contrôle de crédit Diameter à l'élément de service (17).

Adresse des auteurs

Harri Hakala
Oy L M Ericsson Ab
Joukahaisenkatu 1
20520 Turku
Finland
téléphone : +358 2 265 3722
mél : Harri.Hakala@ericsson.com

Leena Mattila
Oy L M Ericsson Ab
Joukahaisenkatu 1
20520 Turku
Finland
téléphone : +358 2 265 3731
mél : Leena.Mattila@ericsson.com

Juha-Pekka Koskinen
Nokia Networks
Hatanpaanvaltatie 30
33100 Tampere
Finland
téléphone : +358 7180 74027
mél : juha-pekka.koskinen@nokia.com

Marco Stura
Nokia Networks
Hiomotie 32
00380 Helsinki
Finland
téléphone : +358 7180 64308
mél : marco.stura@nokia.com

John Loughney
Nokia Research Center
Itamerenkatu 11-13
00180 Helsinki
Finland
téléphone : +358 50 483 642
mél : John.Loughney@nokia.com

Déclaration complète de droits de reproduction

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