Internet Engineering Task Force (IETF)
Request for Comments: 8506
Obsoletes: 4006
Category: Standards Track
ISSN: 2070-1721

L. Bertz, Ed.
Sprint
D. Dolson, Ed.
Y. Lifshitz, Ed.
Sandvine

March 2019

Diameter Credit-Control Application

Abstract

This document specifies a Diameter application that can be used to implement real-time credit-control for a variety of end-user services such as network access, Session Initiation Protocol (SIP) services, messaging services, and download services. The Diameter Credit-Control application as defined in this document obsoletes RFC 4006, and it must be supported by all new Diameter Credit-Control application implementations.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8506.

Table of Contents

1. Introduction

This document specifies a Diameter application that can be used to implement real-time credit-control for a variety of end-user services such as network access, Session Initiation Protocol (SIP) services, messaging services, and download services. ("Credit-control" is sometimes abbreviated as "CC" in figures and tables throughout this document.) The Diameter Credit-Control application as defined in this document obsoletes [RFC4006], and it must be supported by all new Diameter Credit-Control application implementations. This document provides a general solution to real-time cost and credit-control.

The prepaid model has been shown to be very successful -- for instance, in GSM networks, where network operators offering prepaid services have experienced a substantial growth of their customer base and revenues. Prepaid services are now cropping up in many other wireless and wire-line-based networks.

In mobile networks, additional functionality is required beyond that specified in the Diameter base protocol [RFC6733]. For example, the 3GPP charging and billing requirements document [TGPPCHARG] states that an application must be able to rate service information in real time. In addition, it is necessary to check that the end user's account provides coverage for the requested service prior to initiation of that service. When an account is exhausted or expired, the user must be denied the ability to compile additional chargeable events.

A mechanism has to be provided to allow the user to be informed of the charges to be levied for a requested service. In addition, there are services such as gaming and advertising that may credit as well as debit a user account.

The other Diameter applications provide service-specific authorization, and they do not provide credit authorization for prepaid users. The credit authorization shall be generic and applicable to all the service environments required to support prepaid services.

To fulfill these requirements, it is necessary to facilitate credit-control communication between the network element providing the service (e.g., Network Access Server (NAS), SIP Proxy, Application Server) and a credit-control server.

The scope of this specification is credit authorization. Service-specific authorization and authentication are out of scope.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

1.2. Terminology

AAA: Authentication, Authorization, and Accounting.

AA-Answer: "AA-Answer" generically refers to a service-specific authorization and authentication answer. AA-Answer commands are defined in service-specific authorization applications, e.g., [RFC7155] [RFC4004].

AA-Request: "AA-Request" generically refers to a service-specific authorization and authentication request. AA-Request commands are defined in service-specific authorization applications, e.g., [RFC7155] [RFC4004].

Credit-control: "Credit-control" is a mechanism that directly interacts in real time with an account and controls or monitors the charges related to service usage. Credit-control is a process of (1) checking whether or not credit is available, (2) credit reservation, (3) deduction of credit from the end-user account when service is completed, and (4) refunding of reserved credit that is not used.

Diameter Credit-Control server: A Diameter Credit-Control server acts as a prepaid server, performing real-time rating and credit-control. It is located in the home domain and is accessed by Service Elements or Diameter AAA servers in real time, for the purpose of price determination and credit-control before the service event is delivered to the end user. It may also interact with Business Support Systems.

Diameter Credit-Control client: A Diameter Credit-Control client is an entity that interacts with a credit-control server. It monitors the usage of the granted quota according to instructions returned by the credit-control server.

Interrogation: The Diameter Credit-Control client uses interrogation to initiate a session-based credit-control process. During the credit-control process, it is used to report the used quota and request a new one. An interrogation maps to a request/answer transaction.

One-time event: A charging transaction session comprising a single request and single response.

Rating: The act of determining the cost of the service event.

Service: A type of task performed by a Service Element for an end user.

Service Element: A network element that provides a service to the end users. The Service Element may include the Diameter Credit-Control client or another entity (e.g., a RADIUS AAA server) that can act as a credit-control client on behalf of the Service Element. In the latter case, the interface between the Service Element and the Diameter Credit-Control client is outside the scope of this specification. Examples of Service Elements include NASs, SIP Proxies, and Application Servers such as messaging servers, content servers, and gaming servers.

Service event: An event relating to a service provided to the end user.

Session-based credit-control: A credit-control process that makes use of several interrogations: the first, a possible intermediate, and the final. The first interrogation is used to reserve money from the user's account and to initiate the process. Intermediate interrogations (if any) may be needed to request a new quota while the service is being rendered. The final interrogation is used to exit the process. The credit-control server is required to maintain session state for session-based credit-control.

1.3. Advertising Application Support

Diameter nodes conforming to this specification MUST advertise support by including the value of 4 in the Auth-Application-Id of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands [RFC6733].

2. Architecture Models

The current accounting models specified in the RADIUS accounting and Diameter base specifications [RFC2866] [RFC6733] are not sufficient for real-time credit-control, where creditworthiness is to be determined prior to service initiation. Also, the existing Diameter authorization applications [RFC7155] [RFC4004] only provide service authorization; they do not provide credit authorization for prepaid users. In order to support real-time credit-control, a new type of server is needed in the AAA infrastructure: the Diameter Credit-Control server. The Diameter Credit-Control server is the entity responsible for credit authorization for prepaid subscribers.

A Service Element may authenticate and authorize the end user with the AAA server by using AAA protocols, e.g., RADIUS or the Diameter base protocol (possibly extended via a Diameter application).

Accounting protocols such as RADIUS accounting and the Diameter base accounting protocol can be used to provide accounting data to the accounting server after service is initiated and to provide possible interim reports until service completion. However, for real-time credit-control, these authorization and accounting models are not sufficient.

When real-time credit-control is required, the credit-control client contacts the credit-control server with information about a possible service event. The credit-control process is performed to determine potential charges and to verify whether the end user's account balance is sufficient to cover the cost of the service being rendered.

Figure 1 illustrates the typical credit-control architecture, which consists of a Service Element with an embedded Diameter Credit-Control client, a Diameter Credit-Control server, and a AAA server. A Business Support System is usually deployed; at a minimum, it includes billing functionality. The credit-control server and AAA server in this architecture model are logical entities. The real configuration can combine them into a single host. The credit-control protocol is the Diameter base protocol [RFC6733] with the Diameter Credit-Control application.

When an end user requests services such as SIP or messaging, the request is typically forwarded to a Service Element (e.g., a SIP Proxy) in the user's home realm as defined in [RFC6733]. In some cases, it might be possible that the Service Element in the local realm [RFC6733] can offer services to the end user; however, a commercial agreement must exist between the local realm and the home realm. Network access is an example of a service offered in the local realm where the NAS, through a AAA infrastructure, authenticates and authorizes the user with the user's home network.

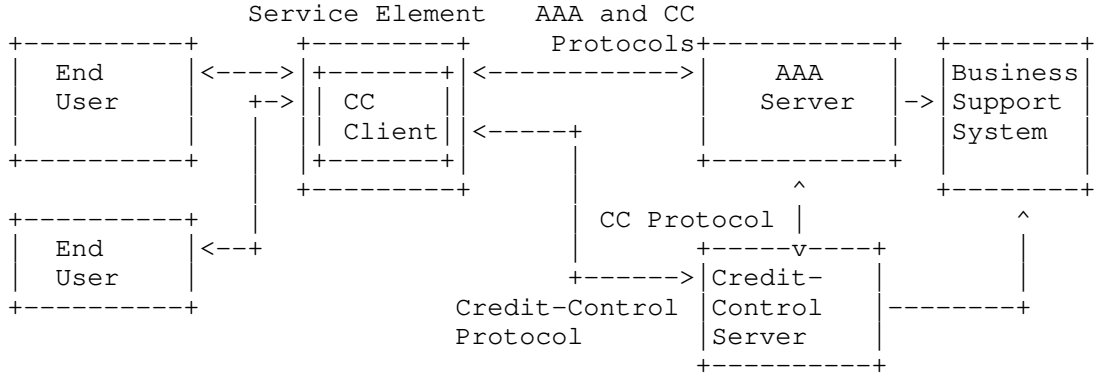


Figure 1: Typical Credit-Control Architecture

There can be multiple credit-control servers in the system for redundancy and load balancing. The system can also contain separate rating server(s), and accounts can be located in a centralized database. To ensure that the end user's account is not debited or credited multiple times for the same service event, only one entity in the credit-control system should perform duplicate detection. System-internal interfaces can exist to relay messages between servers and an account manager. However, the detailed architecture of the credit-control system and its interfaces is implementation specific and is out of scope for this specification.

Protocol-transparent Diameter relays can exist between the credit-control client and credit-control server. Also, Diameter redirect agents that refer credit-control clients to credit-control servers and allow them to communicate directly can exist. These agents transparently support the Diameter Credit-Control application. The different roles of Diameter agents are defined in Diameter base [RFC6733], Section 2.8.

If Diameter Credit-Control proxies exist between the credit-control client and the credit-control server, they MUST advertise support for the Diameter Credit-Control application.

3. Credit-Control Messages

This section defines new Diameter message Command Code values that MUST be supported by all Diameter implementations that conform to this specification. The Command Codes are as follows:

Command Name	Abbrev.	Code	Reference
Credit-Control-Request	CCR	272	Section 3.1
Credit-Control-Answer	CCA	272	Section 3.2

Table 1: Credit-Control Commands

Section 3.2 of [RFC6733] (Diameter base) defines the Command Code Format specification. These formats are observed in credit-control messages.

3.1. Credit-Control-Request (CCR) Command

The Credit-Control-Request message (CCR) is indicated by the Command Code field being set to 272 and the 'R' bit being set in the Command Flags field. It is used between the Diameter Credit-Control client and the credit-control server to request credit authorization for a given service.

The Auth-Application-Id MUST be set to the value 4, indicating the Diameter Credit-Control application.

The CCR is extensible via the inclusion of one or more Attribute-Value Pairs (AVPs).

Message Format:

```
<Credit-Control-Request> ::= < Diameter Header: 272, REQ, PXY >
                             < Session-Id >
                             { Origin-Host }
                             { Origin-Realm }
                             { Destination-Realm }
                             { Auth-Application-Id }
                             { Service-Context-Id }
                             { CC-Request-Type }
                             { CC-Request-Number }
                             [ Destination-Host ]
                             [ User-Name ]
                             [ CC-Sub-Session-Id ]
                             [ Acct-Multi-Session-Id ]
```

```
                                 [ Origin-State-Id ]
                                 [ Event-Timestamp ]
                                *[ Subscription-Id ]
                                *[ Subscription-Id-Extension ]
                                 [ Service-Identifier ]
                                 [ Termination-Cause ]
                                 [ Requested-Service-Unit ]
                                 [ Requested-Action ]
                                *[ Used-Service-Unit ]
                                 [ Multiple-Services-Indicator ]
                                *[ Multiple-Services-Credit-Control ]
                                *[ Service-Parameter-Info ]
                                 [ CC-Correlation-Id ]
                                 [ User-Equipment-Info ]
                                 [ User-Equipment-Info-Extension ]
                                *[ Proxy-Info ]
                                *[ Route-Record ]
                                *[ AVP ]
```

3.2. Credit-Control-Answer (CCA) Command

The Credit-Control-Answer message (CCA) is indicated by the Command Code field being set to 272 and the 'R' bit being cleared in the Command Flags field. It is used between the credit-control server and the Diameter Credit-Control client to acknowledge a Credit-Control-Request command.

Message Format:

```
     <Credit-Control-Answer> ::= < Diameter Header: 272, PXY >
                                 < Session-Id >
                                 { Result-Code }
                                 { Origin-Host }
                                 { Origin-Realm }
                                 { Auth-Application-Id }
                                 { CC-Request-Type }
                                 { CC-Request-Number }
                                 [ User-Name ]
                                 [ CC-Session-Failover ]
                                 [ CC-Sub-Session-Id ]
                                 [ Acct-Multi-Session-Id ]
                                 [ Origin-State-Id ]
                                 [ Event-Timestamp ]
                                 [ Granted-Service-Unit ]
                                *[ Multiple-Services-Credit-Control ]
                                 [ Cost-Information ]
                                 [ Final-Unit-Indication ]
                                 [ QoS-Final-Unit-Indication ]
```

```
                                  [ Check-Balance-Result ]
                                  [ Credit-Control-Failure-Handling ]
                                  [ Direct-Debiting-Failure-Handling ]
                                  [ Validity-Time ]
                                 *[ Redirect-Host ]
                                  [ Redirect-Host-Usage ]
                                  [ Redirect-Max-Cache-Time ]
                                 *[ Proxy-Info ]
                                 *[ Route-Record ]
                                 *[ Failed-AVP ]
                                 *[ AVP ]
```

4. Credit-Control Application Overview

The credit authorization process takes place before and during service delivery to the end user and generally requires the user's authentication and authorization before any requests are sent to the credit-control server. The credit-control application defined in this specification supports two different credit authorization models: credit authorization with money reservation and credit authorization with direct debiting. In both models, the credit-control client requests credit authorization from the credit-control server prior to allowing any services to be delivered to the end user.

In the first model, the credit-control server rates the request, reserves a suitable amount of money from the user's account, and returns the amount of credit reserved. Note that credit resources may not imply actual monetary credit; credit resources may be granted to the credit-control client in the form of units (e.g., data volume or time) to be metered.

Upon receipt of a successful credit authorization answer with a certain amount of credit resources, the credit-control client allows service delivery to the end user and starts monitoring the usage of the granted resources. When the credit resources granted to the user have been consumed or the service has been successfully delivered or terminated, the credit-control client reports back to the server the used amount. The credit-control server deducts the used amount from the end user's account; it may perform rating and make a new credit reservation if the service delivery is continuing. This process is accomplished with session-based credit-control that includes the first interrogation, possible intermediate interrogations, and the final interrogation. For session-based credit-control, both the credit-control client and the credit-control server are required to maintain credit-control session state. Session-based credit-control is described in more detail, with more variations, in Section 5.

In contrast, credit authorization with direct debiting is a single-transaction process wherein the credit-control server directly deducts a suitable amount of money from the user's account as soon as the credit authorization request is received. Upon receipt of a successful credit authorization answer, the credit-control client allows service delivery to the end user. This process is accomplished with the one-time event. Session state is not maintained.

In a multi-service environment, an end user can issue an additional service request (e.g., data service) during an ongoing service (e.g., voice call) toward the same account. Alternatively, during an active multimedia session, an additional media type is added to the session, causing a new simultaneous request toward the same account. Consequently, this needs to be considered when credit resources are granted to the services.

The credit-control application also supports operations such as service price inquiries, user's balance checks, and refunds of credit on the user's account. These operations are accomplished with the one-time event. Session state is not maintained.

Flexible failure handling, specific to the credit-control application, is defined in the application. This allows the service provider to control the credit-control client's behavior according to its own risk management policy.

The Credit-Control-Failure-Handling AVP (also referred to as the CCFH) and the Direct-Debiting-Failure-Handling AVP (also referred to as the DDFH) are defined to determine what is done if the sending of credit-control messages to the credit-control server has been temporarily prevented. The usage of the CCFH and the DDFH allows flexibility, as failure handling for the credit-control session and one-time event direct debiting may be different.

4.1. Service-Specific Rating Input and Interoperability

The Diameter Credit-Control application defines the framework for credit-control; it provides generic credit-control mechanisms supporting multiple service applications. The credit-control application therefore does not define AVPs that could be used as input in the rating process. Listing the possible services that could use this Diameter application is out of scope for this generic mechanism.

It is reasonable to expect that a service level agreement will exist between providers of the credit-control client and the credit-control server covering the charging, services offered, roaming agreements, agreed-upon rating input (i.e., AVPs), and so on.

Therefore, it is assumed that a Diameter Credit-Control server will provide service only for Diameter Credit-Control clients that have agreed beforehand as to the content of credit-control messages. Naturally, it is possible that any arbitrary Diameter Credit-Control client can interchange credit-control messages with any Diameter Credit-Control server, but with a higher likelihood that unsupported services/AVPs could be present in the credit-control message, causing the server to reject the request with an appropriate Result-Code.

4.1.1. Specifying Rating Input AVPs

There are two ways to provide rating input to the credit-control server: by either using AVPs or including the rating input in the Service-Parameter-Info AVP. The general principles for sending rating parameters are as follows:

1. Using AVPs:

   A. The service SHOULD reuse existing AVPs if it can use AVPs defined in existing Diameter applications (e.g., [RFC7155] for network access services). [RFC6733] strongly recommends the reuse of existing AVPs.

      For AVPs of type Enumerated, the service may require a new value to be defined. Allocation of new AVP values is done as specified in [RFC6733], Section 1.3.

   B. New AVPs can be defined if the existing AVPs do not provide sufficient rating information. In this case, the procedures defined in [RFC6733] for creating new AVPs MUST be followed.

   C. For services specific only to one vendor's implementation, a vendor-specific AVP code for private use can be used. Where a vendor-specific AVP is implemented by more than one vendor, allocation of global AVPs is encouraged instead; refer to [RFC6733].

2. The Service-Parameter-Info AVP MAY be used as a container to pass legacy rating information in its original encoded form (e.g., ASN.1 BER). This method can be used to avoid unnecessary conversions from an existing data format to an AVP format. In this case, the rating input is embedded in the Service-Parameter-Info AVP as defined in Section 8.43.

New service applications SHOULD favor the use of explicitly defined AVPs as described in items 1a and 1b, to simplify interoperability.

4.1.2. Service-Specific Documentation

The service-specific rating input AVPs, and the contents of the Service-Parameter-Info AVP or Service-Context-Id AVP (defined in Section 8.42), are not within the scope of this document. To facilitate interoperability, it is RECOMMENDED that the rating input and the values of the Service-Context-Id be coordinated via an informational RFC or other permanent and readily available reference (preferably that of another cooperative standardization body, e.g., 3GPP, the Open Mobile Alliance (OMA), or 3GPP2). However, private services may be deployed that are subject to agreements between providers of the credit-control server and client. In this case, vendor-specific AVPs can be used.

This specification, together with the above-mentioned service-specific documents, governs the credit-control message. Service-specific documents (i.e., those documents that do not define new credit-control applications) define which existing AVPs or new AVPs are used as input to the rating process; thus, the AVPs in question have to be included in the Credit-Control-Request command by a Diameter Credit-Control client supporting a given service as "* [AVP]". Should the Service-Parameter-Info AVP be used, the service-specific document MUST specify the exact content of this Grouped AVP.

The Service-Context-Id AVP MUST be included at the command level of a Credit-Control-Request to identify the service-specific document that applies to the request. The specific service or rating-group the request relates to is uniquely identified by the combination of Service-Context-Id and Service-Identifier or rating-group.

4.1.3. Handling of Unsupported/Incorrect Rating Input

Diameter Credit-Control implementations are required to support mandatory rating-related AVPs defined in service-specific documents for the services they support, according to the 'M' bit rules in [RFC6733].

If a rating input required for the rating process is incorrect in the Credit-Control-Request or if the credit-control server does not support the requested service context (identified by the Service-Context-Id AVP at the command level), the Credit-Control-Answer MUST contain the error code DIAMETER_RATING_FAILED. A CCA message with this error MUST contain one or more Failed-AVP AVPs containing the missing and/or unsupported

AVPs that caused the failure. A Diameter Credit-Control client that receives the error code DIAMETER_RATING_FAILED in response to a request MUST NOT send similar requests in the future.

4.1.4. RADIUS Vendor-Specific Rating Attributes

When service-specific documents include RADIUS vendor-specific attributes that could be used as input in the rating process, the rules described in [RFC7155] for formatting the Diameter AVP MUST be followed.

For example, if the AVP code used is the vendor attribute type code, the Vendor-Specific flag MUST be set to 1 and the Vendor-Id MUST be set to the IANA Vendor identification value. The Diameter AVP Data field contains only the attribute value of the RADIUS attribute.

5. Session-Based Credit-Control

5.1. General Principles

For session-based credit-control, several interrogations are needed: the first, the intermediate (optional), and the final. This is illustrated in Figures 3 and 4 (Sections 5.2.1 and 5.2.2).

If the credit-control client performs credit reservation before granting service to the end user, it MUST use several interrogations toward the credit-control server (i.e., session-based credit-control). In this case, the credit-control server MUST maintain the credit-control session state.

Each credit-control session MUST have a globally unique Session-Id as defined in [RFC6733]; this Session-Id MUST NOT be changed during the lifetime of a credit-control session.

Certain applications require multiple credit-control sub-sessions. These applications would send messages with a constant Session-Id AVP but with a different CC-Sub-Session-Id AVP. If several credit sub-sessions will be used, all sub-sessions MUST be closed separately before the main session is closed so that units per sub-session may be reported. The absence of the CC-Sub-Session-Id AVP implies that no sub-sessions are in use.

Note that the Service Element might send a service-specific re-authorization message to the AAA server due to expiration of the authorization lifetime during an ongoing credit-control session. However, the service-specific re-authorization does not influence the credit authorization that is ongoing between the credit-control client and credit-control server, as credit authorization is controlled by the burning rate of the granted quota.

If service-specific re-authorization fails, the user will be disconnected, and the credit-control client MUST send a final interrogation to the credit-control server.

The Diameter Credit-Control server may seek to control the validity time of the granted quota and/or the production of intermediate interrogations. Thus, it MAY include the Validity-Time AVP in the Answer message to the credit-control client. Upon expiration of the Validity-Time, the credit-control client MUST generate a credit-control update request and report the used quota to the credit-control server. It is up to the credit-control server to determine the value of the Validity-Time to be used for consumption of the granted service unit(s) (G-S-U). If the Validity-Time is used, its value SHOULD be given as input to set the session supervision timer Tcc (the session supervision timer MAY be set to two times the value of the Validity-Time, as defined in Section 13). Since credit-control update requests are also produced at the expiry of granted service units and/or for mid-session service events, the omission of Validity-Time does not mean that intermediate interrogation for the purpose of credit-control is not performed.

5.1.1. Basic Support for Tariff Time Change

The Diameter Credit-Control server and client MAY optionally support a tariff change mechanism. The Diameter Credit-Control server may include a Tariff-Time-Change AVP in the Answer message. Note that the granted units should be allocated based on the worst-case scenario, so that the overall reported used units would never exceed the credit reservation. For example, in the case of a forthcoming tariff change, in which the new rate is higher, the allocation should be given so it does not exceed the credit, assuming that all of it is used after the tariff changed.

When the Diameter Credit-Control client reports the used units and a tariff change has occurred during the reporting period, the Diameter Credit-Control client MUST separately itemize the units used before and after the tariff change. If the client is unable to distinguish whether units straddling the tariff change were used before or after the tariff change, the credit-control client MUST itemize those units in a third category.

If a client does not support the tariff change mechanism and it receives a CCA message carrying the Tariff-Time-Change AVP, it MUST terminate the credit-control session, giving a reason of DIAMETER_BAD_ANSWER in the Termination-Cause AVP.

For time-based services, the quota is consumed at the rate of the passage of real time (ignoring leap seconds). That is, precisely 1 second of quota is consumed per second of real time. At the time when credit resources are allocated, the server already knows how many units will be consumed before the tariff time change and how many units will be consumed afterward. Similarly, the server can determine the units consumed at the "before" rate and the units consumed at the "afterward" rate in the event that the end user closes the session before the consumption of the allotted quota. There is no need for additional traffic between the client and server in the case of tariff time changes for continuous time-based service. Therefore, the tariff change mechanism is not used for such services. For time-based services in which the quota is NOT continuously consumed at a regular rate, the tariff change mechanism described for volume and event units MAY be used.

5.1.2. Credit-Control for Multiple Services within a (Sub-)Session

When multiple services are used within the same user session and each service or group of services is subject to different cost, it is necessary to perform credit-control for each service independently. Making use of credit-control sub-sessions to achieve independent credit-control will result in increased signaling load and usage of resources in both the credit-control client and the credit-control server. For instance, during one network access session, the end user may use several HTTP-based services that could be charged with different costs. The network-access-specific attributes, such as Quality of Service (QoS), are common to all the services carried within the access bearer, but the cost of the bearer may vary, depending on its content.

To support these scenarios optimally, the credit-control application enables independent credit-control of multiple services in a single credit-control (sub-)session. This is achieved by including the optional Multiple-Services-Credit-Control AVP in Credit-Control-Request/Credit-Control-Answer messages. It is possible to request and allocate resources as a credit pool shared between multiple services. The services can be grouped into rating-groups in order to achieve even further aggregation of credit allocation. It is also possible to request and allocate quotas on a per-service basis. Where quotas are allocated to a pool by means of the Multiple-Services-Credit-Control AVP, the quotas remain independent objects

that can be re-authorized independently at any time. Quotas can also be given independent result codes, validity times, and Final-Unit-Indication AVP values or QoS-Final-Unit-Indication AVP values.

A rating-group gathers a set of services, identified by a Service-Identifier and subject to the same cost and rating type (e.g., $0.1/minute). It is assumed that the Service Element is provided with rating-groups, service-identifiers, and their associated parameters that define what has to be metered by means outside the scope of this specification. (Examples of parameters associated to service-identifiers are IP 5-tuples and HTTP URLs.) Service-identifiers enable authorization on a per-service-based credit as well as itemized reporting of service usage. It is up to the credit-control server whether to authorize credit for one or more services or for the whole rating-group. However, the client SHOULD always report used units at the finest supported level of granularity. Where a quota is allocated to a rating-group, all the services belonging to that group draw from the allotted quota. Figure 2 provides a graphical representation of the relationship between service-identifiers, rating-groups, credit pools, and credit-control (sub-)sessions.

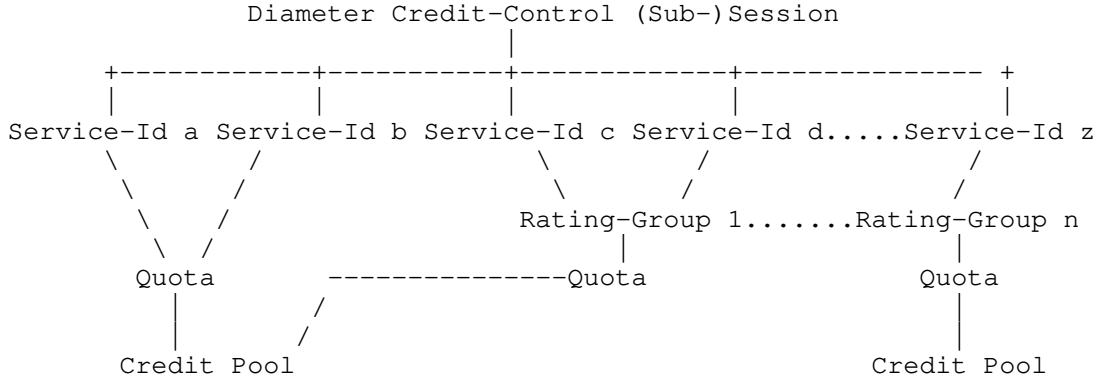


Figure 2: Multiple-Service (Sub-)Session Example

If independent credit-control of multiple services is used, the Validity-Time AVP, and the Final-Unit-Indication AVP or QoS-Final-Unit-Indication AVP, SHOULD be present either in the Multiple-Services-Credit-Control AVP(s) or at the command level as single AVPs. However, the Result-Code AVP MAY be present both at the command level and within the Multiple-Services-Credit-Control AVP. If the Result-Code AVP at the command level indicates a value other than SUCCESS, then the Result-Code AVP at the command level takes precedence over any other AVPs included in the Multiple-Services-Credit-Control AVP.

The credit-control client MUST indicate support for independent credit-control of multiple services within a (sub-)session by including the Multiple-Services-Indicator AVP in the first interrogation. A credit-control server not supporting this feature MUST treat the Multiple-Services-Indicator AVP and any received Multiple-Services-Credit-Control AVPs as invalid AVPs.

If the client indicated support for independent credit-control of multiple services, a credit-control server that wishes to use the feature MUST return the granted units within the Multiple-Services-Credit-Control AVP associated to the corresponding service-identifier and/or rating-group.

To avoid a situation where several parallel (and typically also small) credit reservations must be made on the same account (i.e., credit fragmentation), and also to avoid unnecessary load on the credit-control server, it is possible to provide service units as a pool that applies to multiple services or rating-groups. This is achieved by providing the service units in the form of a quota for a particular service or rating-group in the Multiple-Services-Credit-Control AVP, and also by including a reference to a credit pool for that unit type.

The reference includes a multiplier derived from the rating parameter, which translates from service units of a specific type to the abstract service units in the pool. For instance, if the rating parameter for service 1 is $1/MB and the rating parameter for service 2 is $0.5/MB, the multipliers could be 10 and 5 for services 1 and 2, respectively.

If (1) S is the total service units within the pool, (2) M1, M2, ..., Mn are the multipliers provided for services 1, 2, ..., n, and (3) C1, C2, ..., Cn are the used resources within the session, then the pool's credit is exhausted and re-authorization MUST be sought when:

```
C1*M1 + C2*M2 + ... + Cn*Mn >= S
```

The total credit in the pool, S, is calculated from the quotas, which are currently allocated to the pool as follows:

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

If services or rating-groups are added to or removed from the pool, then the total credit is adjusted appropriately. Note that when the total credit is adjusted because services or rating-groups are removed from the pool, the value that needs to be removed is the consumed one (i.e., Cx*Mx).

Re-authorizations for an individual service or rating-group may be sought at any time -- for example, if a "non-pooled" quota is used up or the Validity-Time expires.

Where multiple G-S-U-Pool-Reference AVPs (Section 8.30) with the same G-S-U-Pool-Identifier are provided within a Multiple-Services-Credit-Control AVP (Section 8.16) along with the Granted-Service-Unit AVP, these AVPs MUST have different CC-Unit-Type values, and they all draw from the credit pool separately. For instance, if one multiplier for time (M1t) and one multiplier for volume (M1v) are given, then the used resources from the pool yield the sum of C1t*M1t + C1v*M1v, where C1t is the time unit and C1v is the volume unit.

Where service units are provided within a Multiple-Services-Credit-Control AVP without a corresponding G-S-U-Pool-Reference AVP, these units are handled independently from any credit pools and from any other services or rating-groups within the session.

The "credit pool" concept is an optimal tool to avoid the over-reservation effect of the basic single-quota tariff time change mechanism (Section 5.1.1). Therefore, Diameter Credit-Control clients and servers implementing the independent credit-control of multiple services SHOULD leverage the credit pool concept when supporting the tariff time change. The Diameter Credit-Control server SHOULD include both the Tariff-Time-Change AVP and the Tariff-Change-Usage AVP in two quota allocations in the Answer message (i.e., two instances of the Multiple-Services-Credit-Control AVP). One of the grants is allocated to be used before the potential tariff change, while the second grant is for use after a tariff change. Both granted unit quotas MUST contain the same Service-Identifier and/or rating-group. This dual-quota mechanism ensures that the overall reported used units would never exceed the credit reservation. The Diameter Credit-Control client reports the used units both before and after the tariff change in a single instance of the Multiple-Services-Credit-Control AVP.

Failure handling for credit-control sessions is defined in Section 5.7 and reflected in the basic credit-control state machines defined in Section 7. Credit-control clients and servers implementing the functionality of independent credit-control of multiple services in a (sub-)session MUST ensure failure handling and general behavior fully consistent with Sections 5.7 and 7 while maintaining the ability to handle parallel ongoing credit re-authorization within a (sub-)session. Therefore, it is RECOMMENDED that Diameter Credit-Control clients maintain a PendingU message queue (Section 7) and restart the Tx timer (Section 13) every time a CCR message with the value UPDATE_REQUEST is sent while they are in PendingU state. When answers to all pending messages are

received, the state machine moves to Open state, and the Tx timer is stopped. Naturally, when a problem is detected and acted upon per Section 5.7, all of the ongoing services are affected (e.g., failover to a backup server affects all of the CCR messages in the PendingU queue).

Since the client may send CCR messages with the value UPDATE_REQUEST while in PendingU state (i.e., without waiting for an answer to ongoing credit re-authorization), the time space between these requests may be very short, and the server may not have received the previous request(s) yet. Therefore, in this situation the server may receive out-of-sequence requests and SHOULD NOT consider this an error condition. A proper answer is to be returned to each of those requests.

5.2. First Interrogation

When session-based credit-control is required (e.g., the authentication server indicated a prepaid user), the first interrogation MUST be sent before the Diameter Credit-Control client allows any service events for the end user. The CC-Request-Type AVP is set to the value INITIAL_REQUEST in the request message.

If the Diameter Credit-Control client knows the cost of the service event (e.g., a content server delivering ringing tones may know their cost) the monetary amount to be charged is included in the Requested-Service-Unit AVP. If the Diameter Credit-Control client does not know the cost of the service event, the Requested-Service-Unit AVP MAY contain the number of requested service events. Where the Multiple-Services-Credit-Control AVP is used, it MUST contain the Requested-Service-Unit AVP to indicate that the quota for the associated service/rating-group is requested. In the case of multiple services, the Service-Identifier AVP or the Rating-Group AVP within the Multiple-Services-Credit-Control AVP always indicates the service concerned. Additional service event information to be rated MAY be sent as service-specific AVPs or MAY be sent within the Service-Parameter-Info AVP at the command level. The Service-Context-Id AVP indicates the service-specific document applicable to the request.

The Event-Timestamp AVP SHOULD be included in the request and contains the time when the service event is requested in the Service Element. The Subscription-Id AVP or the Subscription-Id-Extension AVP SHOULD be included to identify the end user in the credit-control server. The credit-control client MAY include the User-Equipment-Info AVP or User-Equipment-Info-Extension AVP so that the

credit-control server has some indication of the type and capabilities of the end-user access device. How the credit-control server uses this information is outside the scope of this document.

The credit-control server SHOULD rate the service event and make a credit reservation from the end user's account that covers the cost of the service event. If the type of the Requested-Service-Unit AVP is "money", no rating is needed, but the corresponding monetary amount is reserved from the end user's account.

The credit-control server returns the Granted-Service-Unit AVP in the Answer message to the Diameter Credit-Control client. The Granted-Service-Unit AVP contains the amount of service units that the Diameter Credit-Control client can provide to the end user until a new Credit-Control-Request MUST be sent to the credit-control server. If several unit types are sent in the Answer message, the credit-control client MUST handle each unit type separately. The type of the Granted-Service-Unit AVP can be time, volume, service-specific, or money, depending on the type of service event. The unit type(s) SHOULD NOT be changed within an ongoing credit-control session.

There MUST be a maximum of one instance of the same unit type in one Answer message. However, if multiple quotas are conveyed to the credit-control client in the Multiple-Services-Credit-Control AVPs, it is possible to carry two instances of the same unit type associated to a service-identifier/rating-group. This is typically the case when a tariff time change is expected and the credit-control server wants to make a distinction between the granted quota before the tariff change and the granted quota after the tariff change.

If the credit-control server determines that no further control is needed for the service, it MAY include the result code indicating that the credit-control is not applicable (e.g., if the service is free of charge). This result code, at the command level, implies that the credit-control session is to be terminated.

The Credit-Control-Answer message MAY also include the Final-Unit-Indication AVP or the QoS-Final-Unit-Indication AVP to indicate that the Answer message contains the final units for the service. After the end user has consumed these units, the Diameter Credit-Control client MUST behave as described in Section 5.6.

This document defines two different approaches for performing the first interrogation to be used in different network architectures. The first approach uses credit-control messages after the user's authorization and authentication take place. The second approach uses (1) service-specific authorization messages to perform the first

interrogation during the user's authorization/authentication phase and (2) credit-control messages for the intermediate and final interrogations. If an implementation of the credit-control client supports both methods, determining which method to use SHOULD be configurable.

In service environments such as NAS environments, it is desired to perform the first interrogation as part of the authorization/ authentication process for the sake of protocol efficiency. Further credit authorizations after the first interrogation are performed with credit-control commands defined in this specification. Implementations of credit-control clients operating in the environments mentioned in this document SHOULD support this method. If the credit-control server and AAA server are separate physical entities, the Service Element sends the request messages to the AAA server, which then issues an appropriate request or proxies the received request forward to the credit-control server.

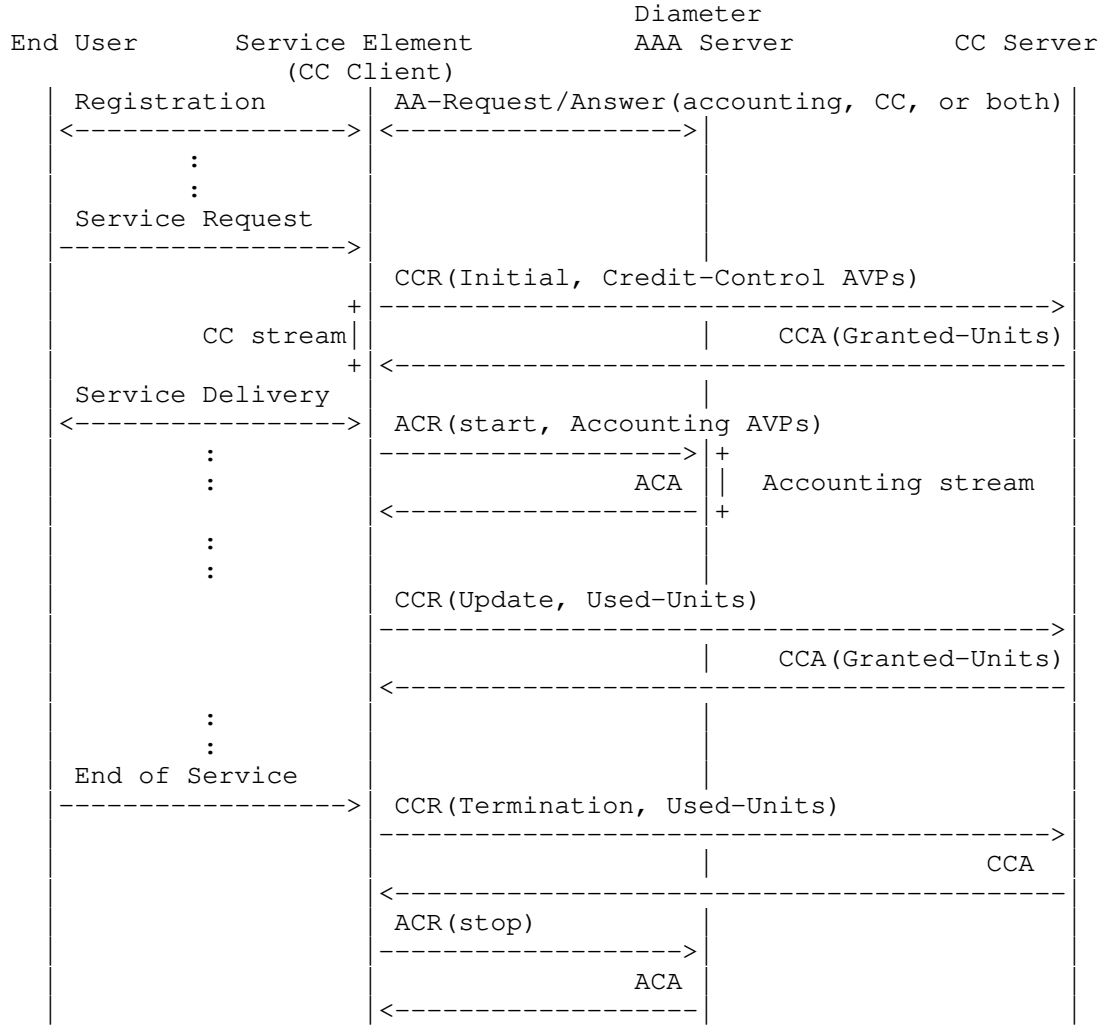
In other service environments, such as the 3GPP network and some SIP scenarios, there is a substantial decoupling between registration/ access to the network and the actual service request (i.e., the authentication/authorization is executed once during registration/ access to the network and is not executed for every service event requested by the subscriber). In these environments, it is more appropriate to perform the first interrogation after the user has been authenticated and authorized. The first, intermediate, and final interrogations are executed with credit-control commands defined in this specification.

Other IETF standards or standards developed by other standardization bodies may define the most suitable method in their architectures.

5.2.1. First Interrogation after Authorization and Authentication

The Diameter Credit-Control client in the Service Element may get information from the authorization server as to whether credit-control is required, based on its knowledge of the end user. If credit-control is required, the credit-control server needs to be contacted prior to initiating service delivery to the end user. The accounting protocol and the credit-control protocol can be used in parallel. The authorization server may also determine whether the parallel accounting stream is required.

Figure 3 illustrates the case where both protocols are used in parallel and the Service Element sends credit-control messages directly to the credit-control server. More credit-control sequence examples are given in Appendix A.



ACR: Accounting-Request
ACA: Accounting-Answer

Figure 3: Protocol Example with First Interrogation after User's Authorization/Authentication

5.2.2. First Interrogation Included with Authorization Messages

The Diameter Credit-Control client in the Service Element MUST actively co-operate with the authorization/authentication client in the construction of the AA-Request by adding appropriate Credit-Control AVPs. The credit-control client MUST add the Credit-Control AVP to indicate credit-control capabilities and MAY add other relevant credit-control-specific AVPs to the proper authorization/authentication command to perform the first interrogation toward the home Diameter AAA server. The Auth-Application-Id is set to the appropriate value, as defined in service-specific authorization/authentication application document (e.g., [RFC7155] [RFC4004]). The home Diameter AAA server authenticates/authorizes the subscriber and determines whether credit-control is required.

If credit-control is not required for the subscriber, the home Diameter AAA server will respond as usual, with an appropriate AA-Answer message. If credit-control is required for the subscriber and the Credit-Control AVP with the value set to CREDIT_AUTHORIZATION was present in the authorization request, the home AAA server MUST contact the credit-control server to perform the first interrogation. If credit-control is required for the subscriber and the Credit-Control AVP was not present in the authorization request, the home AAA server MUST send an authorization reject Answer message.

The Diameter AAA server supporting credit-control is required to send the Credit-Control-Request command (CCR) defined in this document to the credit-control server. The Diameter AAA server populates the CCR based on service-specific AVPs used for input to the rating process, and possibly on Credit-Control AVPs received in the AA-Request. The credit-control server will reserve money from the user's account, will rate the request, and will send a Credit-Control-Answer message to the home Diameter AAA server. The Answer message includes the Granted-Service-Unit AVP(s) and MAY include other credit-control-specific AVPs, as appropriate. Additionally, the credit-control server MAY set the Validity-Time and MAY include the CCFH and the DDFH to determine what to do if the sending of credit-control messages to the credit-control server has been temporarily prevented.

Upon receiving the Credit-Control-Answer message from the credit-control server, the home Diameter AAA server will populate the AA-Answer with the received Credit-Control AVPs and with the appropriate service attributes according to the authorization/authentication-specific application (e.g., [RFC7155] [RFC4004]). It will then forward the packet to the credit-control client. If the home Diameter AAA server receives a credit-control reject message, it

will simply generate an appropriate authorization reject message to the credit-control client, including the credit-control-specific error code.

In this model, the credit-control client sends further credit-control messages to the credit-control server via the home Diameter AAA server. Upon receiving a successful authorization Answer message with the Granted-Service-Unit AVP(s), the credit-control client will grant the service to the end user and will generate an intermediate Credit-Control-Request, if required, by using credit-control commands. The CC-Request-Number of the first UPDATE_REQUEST MUST be set to 1 (for details regarding how to produce a unique value for the CC-Request-Number AVP, see Section 8.2).

If service-specific re-authorization is performed (i.e., the authorization lifetime expires), the credit-control client MUST add to the service-specific re-authorization request the Credit-Control AVP with a value set to RE_AUTHORIZATION to indicate that the credit-control server MUST NOT be contacted. When session-based credit-control is used for the subscriber, a constant credit-control message stream flows through the home Diameter AAA server. The home Diameter AAA server can make use of this credit-control message flow to deduce that the user's activity is ongoing; therefore, it is recommended to set the authorization lifetime to a reasonably high value when credit-control is used for the subscriber.

In this scenario, the home Diameter AAA server MUST advertise support for the credit-control application to its peers during the capability exchange process.

Figure 4 illustrates the use of authorization/authentication messages to perform the first interrogation. The parallel accounting stream is not shown in the figure.

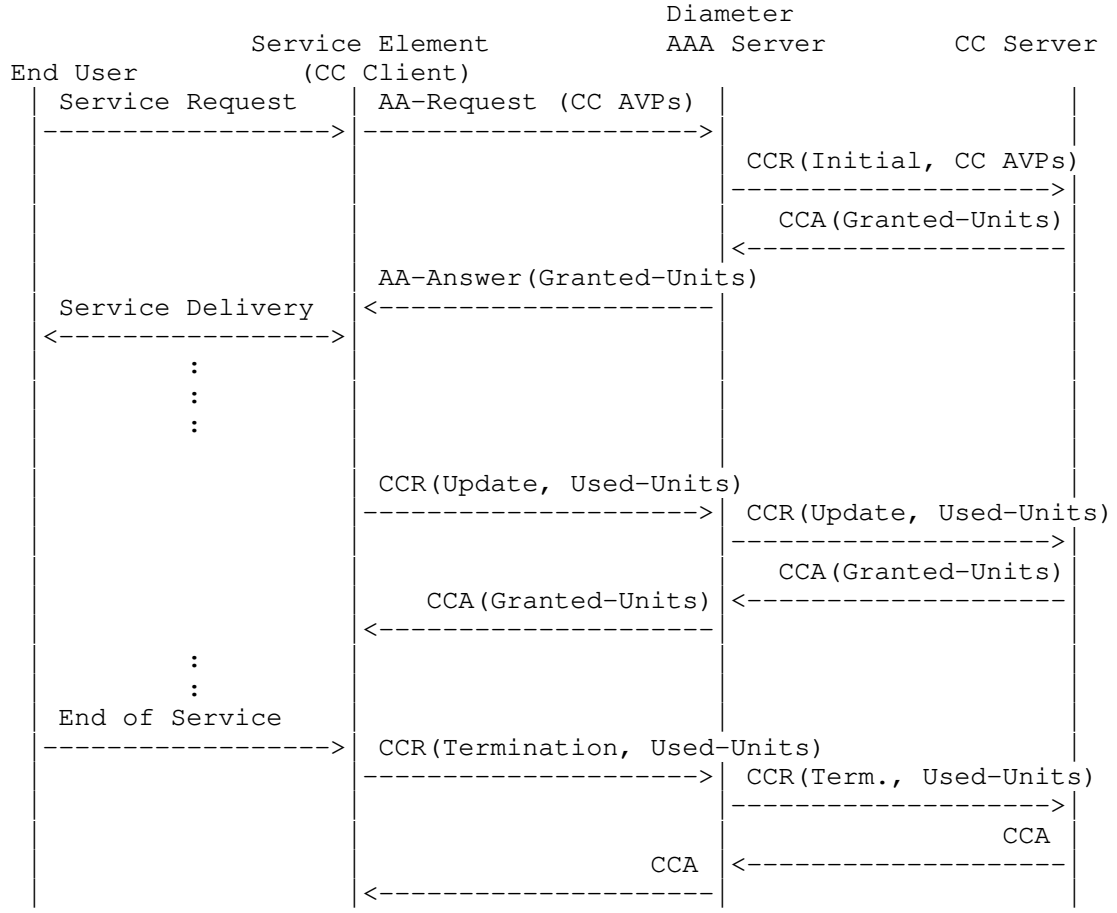


Figure 4: Protocol Example with Use of Authorization Messages for the First Interrogation

5.3. Intermediate Interrogation

When all the granted service units for one unit type are spent by the end user or the Validity-Time has expired, the Diameter Credit-Control client MUST send a new Credit-Control-Request to the credit-control server. In the event that credit-control for multiple services is applied in one credit-control session (i.e., units associated to Service-Identifier(s) or the rating-group are granted), a new Credit-Control-Request MUST be sent to the credit-control

server when the credit reservation has been wholly consumed or upon expiration of the Validity-Time. It is always up to the Diameter Credit-Control client to send a new request well in advance of the expiration of the previous request in order to avoid interruption in the Service Element. Even if the granted service units reserved by the credit-control server have not been spent upon expiration of the Validity-Time, the Diameter Credit-Control client MUST send a new Credit-Control-Request to the credit-control server.

There can also be mid-session service events, which might affect the rating of the current service events. In this case, a spontaneous update (a new Credit-Control-Request) SHOULD be sent, including information related to the service event, even if all the granted service units have not been spent or the Validity-Time has not expired.

When the used units are reported to the credit-control server, the credit-control client will not have any units in its possession before new granted units are received from the credit-control server. When the new granted units are received, these units apply from the point where the measurement of the reported used units stopped. Where independent credit-control of multiple services is supported, this process may be executed for one or more services, a single rating-group, or a pool within the (sub-)session.

The CC-Request-Type AVP is set to the value UPDATE_REQUEST in the intermediate request message. The Subscription-Id AVP or Subscription-Id-Extension AVP SHOULD be included in the intermediate message to identify the end user in the credit-control server. The Service-Context-Id AVP indicates the service-specific document applicable to the request.

The Requested-Service-Unit AVP MAY contain the new amount of requested service units. Where the Multiple-Services-Credit-Control AVP is used, it MUST contain the Requested-Service-Unit AVP if a new quota is requested for the associated service/rating-group. The Used-Service-Unit AVP contains the amount of used service units measured from the point when the service became active or, if interim interrogations are used during the session, from the point when the previous measurement ended. The same unit types used in the previous message SHOULD be used. If several unit types were included in the previous Answer message, the used service units for each unit type MUST be reported.

The Event-Timestamp AVP SHOULD be included in the request and contains the time of the event that triggered the sending of the new Credit-Control-Request.

The credit-control server MUST deduct the used amount from the end user's account. It MAY rate the new request and make a new credit reservation from the end user's account that covers the cost of the requested service event.

A Credit-Control-Answer message with the CC-Request-Type AVP set to the value UPDATE_REQUEST MAY include the Cost-Information AVP containing the accumulated cost estimation for the session, without taking any credit reservations into account.

The Credit-Control-Answer message MAY also include the Final-Unit-Indication AVP or the QoS-Final-Unit-Indication AVP to indicate that the Answer message contains the final units for the service. After the end user has consumed these units, the Diameter Credit-Control client MUST behave as described in Section 5.6.

There can be several intermediate interrogations within a session.

5.4. Final Interrogation

When the end user terminates the service session or when graceful service termination (described in Section 5.6) takes place, the Diameter Credit-Control client MUST send a final Credit-Control-Request message to the credit-control server. The CC-Request-Type AVP is set to the value TERMINATION_REQUEST. The Service-Context-Id AVP indicates the service-specific document applicable to the request.

The Event-Timestamp AVP SHOULD be included in the request and contains the time when the session was terminated.

The Used-Service-Unit AVP contains the amount of used service units measured from the point when the service became active or, if interim interrogations are used during the session, from the point when the previous measurement ended. If several unit types were included in the previous Answer message, the used service units for each unit type MUST be reported.

After final interrogation, the credit-control server MUST refund the reserved credit amount not used to the end user's account and deduct the used monetary amount from the end user's account.

A Credit-Control-Answer message with the CC-Request-Type AVP set to the value TERMINATION_REQUEST MAY include the Cost-Information AVP containing the estimated total cost for the session in question.

If the user logs off during an ongoing credit-control session or if the user becomes logged off for some other reason (e.g., a final-unit indication causes user logoff according to local policy), the Service Element, according to application-specific policy, may send a Session-Termination-Request (STR) to the home Diameter AAA server as usual [RFC6733]. Figure 5 illustrates the case when the final-unit indication causes user logoff upon consumption of the final granted units and the generation of an STR.

The Diameter AAA server responds with a Session-Termination-Answer (STA).

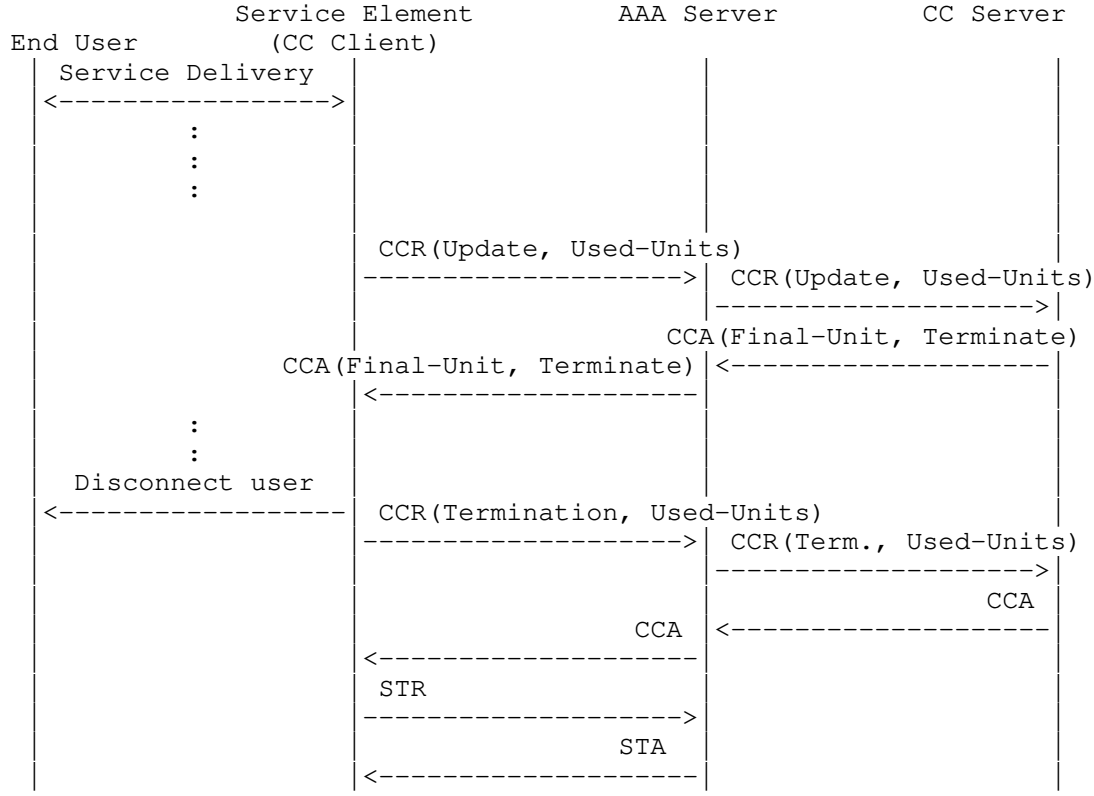


Figure 5: User Disconnected Due to Exhausted Account

5.5. Server-Initiated Credit Re-authorization

The Diameter Credit-Control application supports server-initiated re-authorization. The credit-control server MAY optionally initiate the credit re-authorization by issuing a Re-Auth-Request (RAR) as defined in the Diameter base protocol [RFC6733]. The

Auth-Application-Id in the RAR message is set to 4 to indicate "Diameter Credit Control", and the Re-Auth-Request-Type is set to AUTHORIZE_ONLY.

Section 5.1.2 defines the feature to enable credit-control for multiple services within a single (sub-)session where the server can authorize credit usage at a different level of granularity. Further, the server may provide credit resources to multiple services or rating-groups as a pool (see Section 5.1.2 for details and definitions). Therefore, the server, based on its service logic and its knowledge of the ongoing session, can decide to request credit re-authorization for a whole (sub-)session, a single credit pool, a single service, or a single rating-group. To request credit re-authorization for a credit pool, the server includes in the RAR message the G-S-U-Pool-Identifier AVP indicating the affected pool. To request credit re-authorization for a service or a rating-group, the server includes in the RAR message the Service-Identifier AVP or the Rating-Group AVP, respectively. To request credit re-authorization for all the ongoing services within the (sub-)session, the server includes none of the above-mentioned AVPs in the RAR message.

If a credit re-authorization is not already ongoing (i.e., the credit-control session is in Open state), a credit-control client that receives an RAR message with Session-Id equal to a currently active credit-control session MUST acknowledge the request by sending the Re-Auth-Answer (RAA) message and MUST initiate the credit re-authorization toward the server by sending a Credit-Control-Request message with the CC-Request-Type AVP set to the value UPDATE_REQUEST. The Result-Code 2002 (DIAMETER_LIMITED_SUCCESS) SHOULD be used in the RAA message to indicate that an additional message (i.e., a CCR message with the value UPDATE_REQUEST) is required to complete the procedure. If a quota was allocated to the service, the credit-control client MUST report the used quota in the Credit-Control-Request. Note that the end user does not need to be prompted for the credit re-authorization, since the credit re-authorization is transparent to the user (i.e., it takes place exclusively between the credit-control client and the credit-control server).

Where multiple services in a user’s session are supported, the procedure in the above paragraph will be executed at the granularity requested by the server in the RAR message.

If credit re-authorization is ongoing at the time when the RAR message is received (i.e., an RAR-CCR collision), the credit-control client successfully acknowledges the request but does not initiate a new credit re-authorization. The Result-Code 2001 (DIAMETER_SUCCESS)

SHOULD be used in the RAA message to indicate that a credit re-authorization procedure is already ongoing (i.e., the client was in PendingU state when the RAR was received). The credit-control server SHOULD process the Credit-Control-Request as if it was received in answer to the server-initiated credit re-authorization and should consider the server-initiated credit re-authorization process successful upon reception of the RAA message.

When multiple services are supported in a user's session, the server may request credit re-authorization for a credit pool (or for the (sub-)session) while a credit re-authorization is already ongoing for some of the services or rating-groups. In this case, the client acknowledges the server request with an RAA message and MUST send a new Credit-Control-Request message to perform re-authorization for the remaining services/rating-groups. The Result-Code 2002 (DIAMETER_LIMITED_SUCCESS) SHOULD be used in the RAA message to indicate that an additional message (i.e., a CCR message with the value UPDATE_REQUEST) is required to complete the procedure. The server processes the received requests and returns an appropriate answer to both requests.

The above-defined procedures are enabled for each of the possibly active Diameter Credit-Control sub-sessions. The server MAY request re-authorization for an active sub-session by including the CC-Sub-Session-Id AVP in the RAR message in addition to the Session-Id AVP.

5.6. Graceful Service Termination

When the user's account runs out of money, the user may not be allowed to compile additional chargeable events. However, the home service provider may offer some services -- for instance, access to a service portal where it is possible to refill the account -- from which the user is allowed to benefit for a limited time. The length of this time is usually dependent on the home service provider policy.

This section defines the optional graceful service termination feature. This feature MAY be supported by the credit-control server. Credit-control client implementations MUST support the Final-Unit-Indication AVP or QoS-Final-Unit-Indication AVP with at least the teardown of the ongoing service session once the subscriber has consumed all the final granted units.

Where independent credit-control of multiple services in a single credit-control (sub-)session is supported, it is possible to use graceful service termination for each of the services/rating-groups independently. Naturally, the graceful service termination process defined in the following subsections will apply to the specific service/rating-group as requested by the server.

In some service environments (e.g., NAS), graceful service termination may be used to redirect the subscriber to a service portal for online balance refill or other services offered by the home service provider. In this case, the graceful service termination process installs a set of packet filters to restrict the user's access capability only to/from the specified destinations. All the IP packets not matching the filters will be dropped or, possibly, redirected to the service portal. The user may also be sent an appropriate notification as to why the access has been limited. These actions may be communicated explicitly from the server to the client or may be configured "per service" at the client. Explicitly signaled redirection or restriction instructions always take precedence over configured ones.

It is also possible to use graceful service termination to connect the prepaid user to a top-up server that plays an announcement and prompts the user to replenish the account. In this case, the credit-control server sends only the address of the top-up server where the prepaid user shall be connected after the final granted units have been consumed. An example of this case is given in Appendix A.7.

The credit-control server MAY initiate graceful service termination by including the Final-Unit-Indication AVP or the QoS-Final-Unit-Indication AVP in the Credit-Control-Answer to indicate that the message contains the final units for the service.

When the credit-control client receives the Final-Unit-Indication AVP or the QoS-Final-Unit-Indication AVP in the answer from the server, its behavior depends on the value indicated in the Final-Unit-Action AVP. The server may request the following actions: TERMINATE, REDIRECT, or RESTRICT_ACCESS.

Figure 6 illustrates the graceful service termination procedure described in the following subsections.

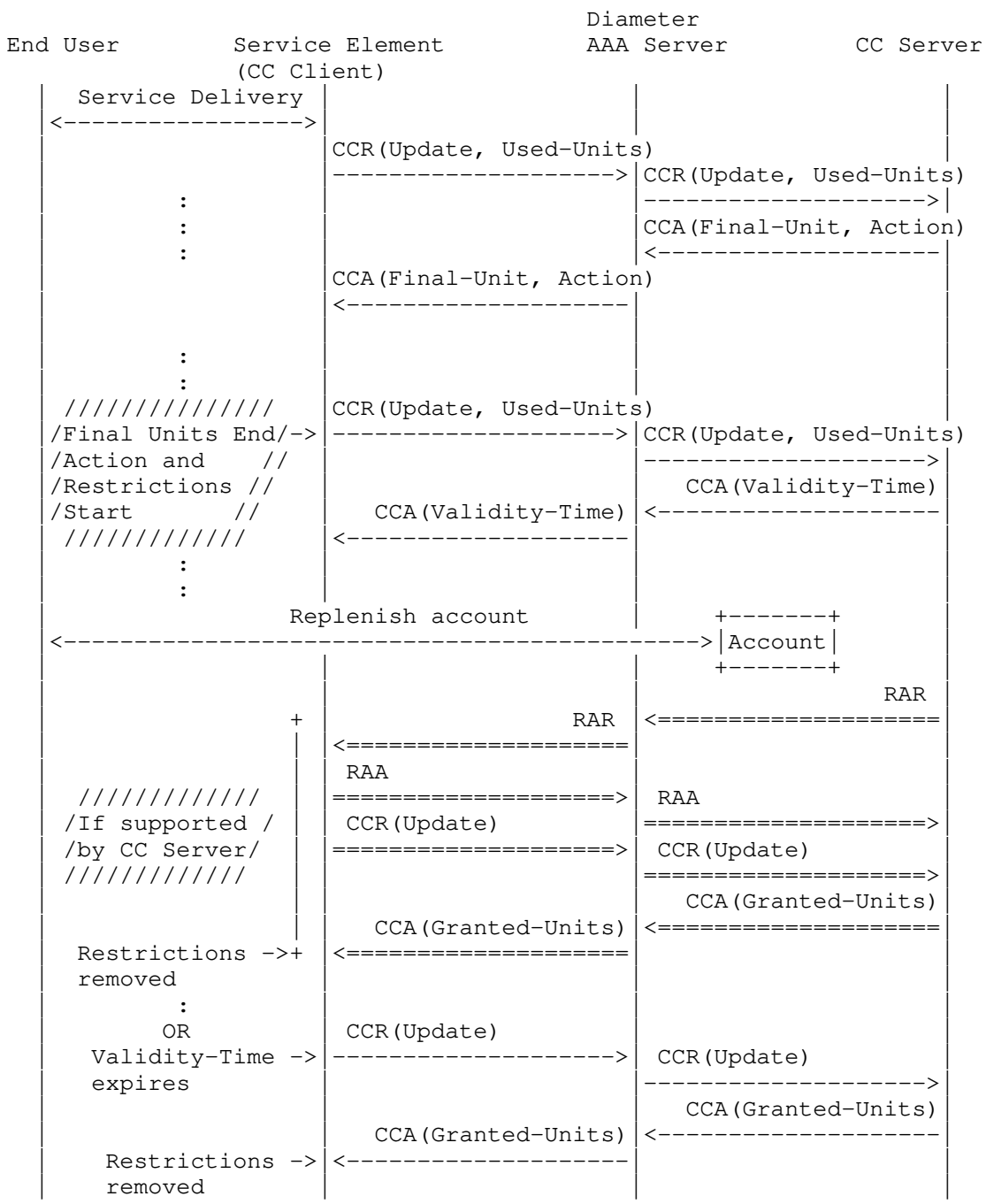


Figure 6: Optional Graceful Service Termination Procedure

In addition, the credit-control server MAY reply with the Final-Unit-Indication AVP or QoS-Final-Unit-Indication AVP holding a Granted-Service-Unit (G-S-U) with a zero grant, indicating that the service SHOULD be terminated immediately, and no further reporting is required. Figure 7 illustrates a graceful service termination procedure that applies immediately after receiving a zero grant.

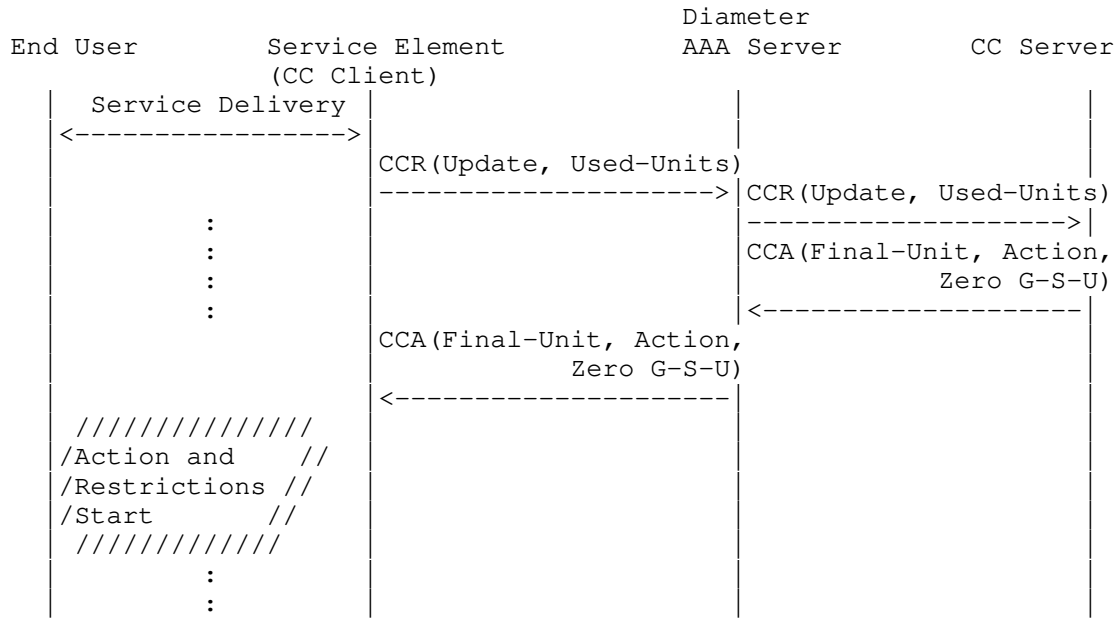


Figure 7: Optional Immediate Graceful Service Termination Procedure

5.6.1. Terminate Action

The Final-Unit-Indication AVP or the QoS-Final-Unit-Indication AVP with Final-Unit-Action set to TERMINATE does not include any other information. When the subscriber has consumed the final granted units, the Service Element MUST terminate the service. This is the default handling applicable whenever the credit-control client receives an unsupported Final-Unit-Action value and MUST be supported by all the Diameter Credit-Control client implementations conforming to this specification. A final Credit-Control-Request message to the credit-control server MUST be sent if the Final-Unit-Indication AVP or the QoS-Final-Unit-Indication AVP indicating action TERMINATE was present at the command level. The CC-Request-Type AVP in the request is set to the value TERMINATION_REQUEST.

5.6.2. Redirect Action

The Final-Unit-Indication AVP or the QoS-Final-Unit-Indication AVP with Final-Unit-Action set to REDIRECT indicates to the Service Element supporting this action that, upon consumption of the final granted units, the user MUST be redirected to the address specified in the Redirect-Server AVP or Redirect-Server-Extension AVP as follows.

The credit-control server sends the Redirect-Server AVP or Redirect-Server-Extension AVP in the Credit-Control-Answer message. In such a case, the Service Element MUST redirect or connect the user to the destination specified in the Redirect-Server AVP or Redirect-Server-Extension AVP, if possible. When the end user is redirected (by using protocols other than Diameter) to the specified server or connected to the top-up server, an additional authorization (and possibly authentication) may be needed before the subscriber can replenish the account; however, this scenario is out of scope for this specification.

In addition to the Redirect-Server AVP or Redirect-Server-Extension AVP, the credit-control server MAY include one or more Restriction-Filter-Rule AVPs, one or more Filter-Rule AVPs, or one or more Filter-Id AVPs in the Credit-Control-Answer message to enable the user to access other services (for example, zero-rated services). In such a case, the access device MUST treat all packets according to the Restriction-Filter-Rule AVPs, Filter-Rule AVPs, and the rules referred to by the Filter-Id AVP. After treatment is applied according to these rules, all traffic that has not been dropped or already forwarded MUST be redirected to the destination specified in the Redirect-Server AVP or Redirect-Server-Extension AVP.

An entity other than the credit-control server may provision the access device with appropriate IP packet filters to be used in conjunction with the Diameter Credit-Control application. This case is considered in Section 5.6.3.

When the final granted units have been consumed, the credit-control client MUST perform an intermediate interrogation. The purpose of this interrogation is to indicate to the credit-control server that the specified action started and to report the used units. The credit-control server MUST deduct the used amount from the end user's account but MUST NOT make a new credit reservation. The credit-control client, however, may send intermediate interrogations before all the final granted units have been consumed for which rating and money reservation may be needed -- for instance, upon Validity-Time expiration or upon mid-session service events that affect the rating of the current service. Therefore, the

credit-control client MUST NOT include any rating-related AVPs in the request sent once all the final granted units have been consumed, as an indication to the server that (1) the requested final unit action started and (2) rating and money reservation are not required (when the Multiple-Services-Credit-Control AVP is used, the Service-Identifier AVP or the Rating-Group AVP is included to indicate the services concerned). Naturally, the Credit-Control-Answer message does not contain any granted service units and MUST include the Validity-Time AVP to indicate to the credit-control client how long the subscriber is allowed to use network resources before a new intermediate interrogation is sent to the server.

At the expiry of Validity-Time, the credit-control client sends a Credit-Control-Request (UPDATE_REQUEST) as usual. This message does not include the Used-Service-Unit AVP, as there is no allotted quota to report. The credit-control server processes the request and MUST perform the credit reservation. If during this time the subscriber did not replenish their account, whether they will be disconnected or will be granted access to services not controlled by a credit-control server for an unlimited time is dependent on the home service provider policy. (Note: The latter option implies that the Service Element should not remove the restriction filters upon termination of the credit-control.) The server will return the appropriate Result-Code (see Section 9.1) in the Credit-Control-Answer message in order to implement the policy-defined action. Otherwise, a new quota will be returned, and the Service Element MUST remove all the possible restrictions activated by the graceful service termination process and continue the credit-control session and service session as usual.

The credit-control client may not wait until the expiration of the Validity-Time and may send a spontaneous update (a new Credit-Control-Request) if the Service Element can determine, for instance, that communication between the end user and the top-up server took place. An example of this case is given in Appendix A.8 (Figure 18).

Note that the credit-control server may already have initiated the above-described process for the first interrogation. However, the user's account might be empty when this first interrogation is performed. In this case, the subscriber can be offered a chance to replenish the account and continue the service. When the credit-control client receives (at either the session level or a service-specific level) a Final-Unit-Indication AVP or QoS-Final-Unit-Indication AVP, together with Validity-Time AVPs, but without a Granted-Service-Unit AVP, it immediately starts the graceful service termination process without sending any messages to the server. An example of this case is illustrated in Appendix A.8 (Figure 18).

5.6.3. Restrict Access Action

A Final-Unit-Indication AVP with Final-Unit-Action set to RESTRICT_ACCESS indicates to the device supporting this action that, upon consumption of the final granted units, the user's access MUST be restricted according to the IP packet filters given in the Restriction-Filter-Rule AVP(s) or according to the IP packet filters identified by the Filter-Id AVP(s). The credit-control server SHOULD include either the Restriction-Filter-Rule AVP or the Filter-Id AVP in the Final-Unit-Indication group AVP of the Credit-Control-Answer message.

A QoS-Final-Unit-Indication AVP with Final-Unit-Action set to RESTRICT_ACCESS indicates to the device supporting this action that, upon consumption of the final granted units, the actions specified in Filter-Rule AVP(s) MUST restrict the traffic according to the classifiers in the Filter-Rule AVP(s). If one or more Filter-Id AVPs are provided in the Credit-Control-Answer message, the credit-control client MUST restrict the traffic according to the IP packet filters identified by the Filter-Id AVP(s). The credit-control server SHOULD include either the Filter-Rule AVP or the Filter-Id AVP in the QoS-Final-Unit-Indication group AVP of the Credit-Control-Answer message.

If both the Final-Unit-Indication AVP and the QoS-Final-Unit-Indication AVP exist in the Credit-Control-Answer message, a credit-control client that supports the QoS-Final-Unit-Indication AVP SHOULD follow the directives included in the QoS-Final-Unit-Indication AVP and SHOULD ignore the Final-Unit-Indication AVP.

An entity other than the credit-control server may provision the access device with appropriate IP packet filters to be used in conjunction with the Diameter Credit-Control application. Such an entity may, for instance, configure the access device with IP flows to be passed when the Diameter Credit-Control application indicates RESTRICT_ACCESS or REDIRECT. The access device passes IP packets according to the filter rules that may have been received in the Credit-Control-Answer message, in addition to those rules that may have been configured by the other entity. However, when the user's account cannot cover the cost of the requested service, the action taken is the responsibility of the credit-control server that controls the prepaid subscriber.

If another entity working in conjunction with the Diameter Credit-Control application already provisions the access device with all the required filter rules for the end user, the credit-control server presumably need not send any additional filters. Therefore, it is RECOMMENDED that credit-control server implementations

supporting graceful service termination be configurable for sending the Restriction-Filter-Rule AVP, the Filter-Rule AVP, the Filter-Id AVP, or none of the above.

When the final granted units have been consumed, the credit-control client MUST perform an intermediate interrogation. The credit-control client and the credit-control server process this intermediate interrogation and execute subsequent procedures, as specified in Section 5.6.2.

The credit-control server may initiate graceful service termination when replying with the action RESTRICT_ACCESS for the first interrogation. This is similar to the behavior specified in Section 5.6.2.

5.6.4. Usage of the Server-Initiated Credit Re-authorization

Once the subscriber replenishes the account, they presumably expect all the restrictions applied by the graceful service termination procedure to be removed immediately and unlimited service access to be resumed. For the best user experience, the credit-control server implementation MAY support the server-initiated credit re-authorization (see Section 5.5). In such a case, upon the successful account top-up, the credit-control server sends the Re-Auth-Request (RAR) message to solicit the credit re-authorization. The credit-control client initiates the credit re-authorization by sending the Credit-Control-Request message with the CC-Request-Type AVP set to the value UPDATE_REQUEST. The Used-Service-Unit AVP is not included in the request, as there is no allotted quota to report. The Requested-Service-Unit AVP MAY be included in the request. After the credit-control client successfully receives the Credit-Control-Answer with a new Granted-Service-Unit AVP, all the possible restrictions activated for the purpose of graceful service termination MUST be removed in the Service Element. The credit-control session and the service session continue as usual.

5.7. Failure Procedures

The CCFH, as described in this section, determines the behavior of the credit-control client in fault situations. The CCFH may be (1) received from the Diameter home AAA server, (2) received from the credit-control server, or (3) configured locally. The CCFH value received from the home AAA server overrides the locally configured value. The CCFH value received from the credit-control server in the Credit-Control-Answer message always overrides any existing values.

The authorization server MAY include the Accounting-Realtime-Required AVP to determine what to do if the sending of accounting records to the accounting server has been temporarily prevented, as defined in [RFC6733]. It is RECOMMENDED that the client complement the credit-control failure procedures with a backup accounting flow toward an accounting server. By using different combinations of the Accounting-Realtime-Required AVP and the CCFH, different safety levels can be built. For example, by choosing a CCFH equal to CONTINUE for the credit-control flow and an Accounting-Realtime-Required AVP equal to DELIVER_AND_GRANT for the accounting flow, the service can be granted to the end user even if the connection to the credit-control server is down, as long as the accounting server is able to collect the accounting information and information exchange is taking place between the accounting server and credit-control server.

As the credit-control application is based on real-time bidirectional communication between the credit-control client and the credit-control server, the usage of alternative destinations and the buffering of messages may not be sufficient in the event of communication failures. Because the credit-control server has to maintain session states, moving the credit-control message stream to a backup server requires a complex context transfer solution. Whether the credit-control message stream is moved to a backup credit-control server during an ongoing credit-control session depends on the value of the CC-Session-Failover AVP. However, failover may occur at any point in the path between the credit-control client and the credit-control server if a transport failure is detected with a peer, as described in [RFC6733]. As a consequence, the credit-control server might receive duplicate messages. These duplicate or out-of-sequence messages can be detected in the credit-control server based on the credit-control server session state machine (Section 7), Session-Id AVP, and CC-Request-Number AVP.

If a failure occurs during an ongoing credit-control session, the credit-control client may move the credit-control message stream to an alternative server if the credit-control server indicated FAILOVER_SUPPORTED in the CC-Session-Failover AVP. A secondary credit-control server name, either received from the home Diameter AAA server or configured locally, can be used as an address of the backup server. If the CC-Session-Failover AVP is set to FAILOVER_NOT_SUPPORTED, the credit-control message stream MUST NOT be moved to a backup server.

For new credit-control sessions, failover to an alternative credit-control server SHOULD be performed, if possible. For instance, if an implementation of the credit-control client can determine primary credit-control server unavailability, it can establish the new credit-control sessions with a possibly available secondary credit-control server.

The AAA transport profile [RFC3539] defines an application-layer watchdog algorithm that enables failover from a peer that has failed and is controlled by a watchdog timer (Tw) (defined in [RFC3539]). The recommended default initial value for Tw (Twinit) is 30 seconds. Twinit may be set as low as 6 seconds; however, according to [RFC3539], setting too low a value for Twinit is likely to result in an increased probability of duplicates, as well as an increase in spurious failover and failback attempts. The Diameter base protocol [RFC6733] is common to several different types of Diameter AAA applications that may be run in the same Service Element. Therefore, tuning the timer for Twinit to a lower value in order to satisfy the requirements of real-time applications, such as the Diameter Credit-Control application, will certainly cause the above-mentioned problems. For prepaid services, however, the end user expects an answer from the network in a reasonable time. Thus, the Diameter Credit-Control client will react more quickly than would the underlying base protocol. Therefore, this specification defines the Tx timer (as defined in Section 13), which is used by the credit-control client to supervise communication with the credit-control server. When the Tx timer elapses, the credit-control client takes action for the end user according to the CCFH.

When the Tx timer expires, the Diameter Credit-Control client always terminates the service if the CCFH is set to the value TERMINATE. The credit-control session may be moved to an alternative server only if a protocol error DIAMETER_TOO_BUSY or DIAMETER_UNABLE_TO_DELIVER is received before the Tx timer expires. Therefore, the value TERMINATE is not appropriate if proper failover behavior is desired.

If the CCFH is set to the value CONTINUE or RETRY_AND_TERMINATE, the service will be granted to the end user when the Tx timer expires. An Answer message with granted units may arrive later if the base protocol transport failover occurred in the path to the credit-control server. (The Twinit default value is 3 times more than the recommended Tx timeout value.) The credit-control client SHOULD grant the service to the end user, start monitoring resource usage, and wait for the possible late answer until the timeout of the request (e.g., 120 seconds). If the request fails and the CC-Session-Failover AVP is set to FAILOVER_NOT_SUPPORTED, the

credit-control client terminates or continues the service -- depending on the value set in the CCFH -- and MUST free all the reserved resources for the credit-control session. If the protocol error DIAMETER_UNABLE_TO_DELIVER or DIAMETER_TOO_BUSY is received or the request times out and the CC-Session-Failover AVP is set to FAILOVER_SUPPORTED, the credit-control client MAY send the request to a backup server, if possible. If the credit-control client receives a successful answer from the backup server, it continues the credit-control session with such a server. If the retransmitted request also fails, the credit-control client terminates or continues the service -- depending on the value set in the CCFH -- and MUST free all the reserved resources for the credit-control session.

If a communication failure occurs during the graceful service termination procedure, the Service Element SHOULD always terminate the ongoing service session.

If the credit-control server detects a failure during an ongoing credit-control session, it will terminate the credit-control session and return the reserved units back to the end user's account.

The supervision session timer Tcc (as defined in Section 13) is used in the credit-control server to supervise the credit-control session.

In order to support failover between credit-control servers, information transfer about the credit-control session and account state SHOULD take place between the primary and secondary credit-control servers. Implementations supporting credit-control session failover MUST also ensure proper detection of duplicate or out-of-sequence messages. Communication between the servers is regarded as an implementation issue and is outside the scope of this specification.

6. One-Time Event

The one-time event is used when there is no need to maintain any state in the Diameter Credit-Control server -- for example, inquiring about the price of the service. The use of a one-time event implies that the user has been authenticated and authorized beforehand.

The one-time event can be used when the credit-control client wants to know the cost of the service event or to check the account balance without any credit reservations. It can also be used for refunding service units on the user's account or for direct debiting without any credit reservations. The one-time event is shown in Figure 8.

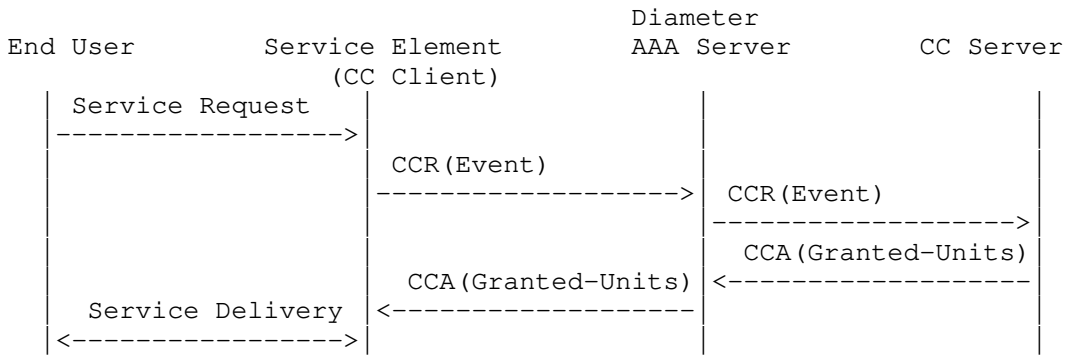


Figure 8: One-Time Event

In environments such as the 3GPP architecture, the one-time event can be sent from the Service Element directly to the credit-control server.

6.1. Service Price Inquiry

The credit-control client may need to know the price of the service event. Services offered by application service providers whose prices are not known in the credit-control client might exist. The end user might also want to get an estimate of the price of a service event before requesting it.

A Diameter Credit-Control client requesting the cost information MUST set the CC-Request-Type AVP equal to EVENT_REQUEST, include the Requested-Action AVP set to PRICE_ENQUIRY, and set the requested service event information in the Service-Identifier AVP in the Credit-Control-Request message. Additional service event information may be sent as service-specific AVPs or within the Service-Parameter-Info AVP. The Service-Context-Id AVP indicates the service-specific document applicable to the request.

The credit-control server calculates the cost of the requested service event, but it does not perform any account-balance checks or credit reservations from the account.

The estimated cost of the requested service event is returned to the credit-control client in the Cost-Information AVP in the Credit-Control-Answer message.

6.2. Balance Checks

The Diameter Credit-Control client may only have to verify that the end user's account balance covers the cost of a certain service without reserving any units from the account at the time of the inquiry. This method does not guarantee that credit would be left when the Diameter Credit-Control client requests the debiting of the account with a separate request.

A Diameter Credit-Control client requesting a balance check MUST set the CC-Request-Type AVP equal to EVENT_REQUEST, include a Requested-Action AVP set to CHECK_BALANCE, and include the Subscription-Id AVP or Subscription-Id-Extension AVP in order to identify the end user in the credit-control server. The Service-Context-Id AVP indicates the service-specific document applicable to the request.

The credit-control server makes the balance check, but it does not make any credit reservations from the account.

The result of the balance check (ENOUGH_CREDIT/NO_CREDIT) is returned to the credit-control client in the Check-Balance-Result AVP in the Credit-Control-Answer message.

6.3. Direct Debiting

There are certain service events for which service execution is always successful in the service environment. The delay between the service invocation and the actual service delivery to the end user can be sufficiently long that the use of session-based credit-control would lead to unreasonably long credit-control sessions. In these cases, the Diameter Credit-Control client can use the one-time event scenario for direct debiting. The Diameter Credit-Control client SHOULD be sure that the requested service event execution would be successful when this scenario is used.

In the Credit-Control-Request message, the CC-Request-Type AVP is set to the value EVENT_REQUEST and the Requested-Action AVP is set to DIRECT_DEBITING. The Subscription-Id AVP or Subscription-Id-Extension AVP SHOULD be included to identify the end user in the credit-control server. The Event-Timestamp AVP SHOULD be included in the request and contain the time when the service event is requested in the Service Element. The Service-Context-Id AVP indicates the service-specific document applicable to the request.

If it knows the cost of the service event, the Diameter Credit-Control client MAY include in the Requested-Service-Unit AVP the monetary amount to be charged. If the Diameter Credit-Control client does not know the cost of the service event, the Requested-Service-Unit AVP MAY contain the number of requested service events. The Service-Identifier AVP always indicates the service concerned. Additional service event information to be rated MAY be sent as service-specific AVPs or within the Service-Parameter-Info AVP.

The credit-control server SHOULD rate the service event and deduct the corresponding monetary amount from the end user's account. If the type of the Requested-Service-Unit AVP is "money", no rating is needed, but the corresponding monetary amount is deducted from the end user's account.

The credit-control server returns the Granted-Service-Unit AVP in the Credit-Control-Answer message to the Diameter Credit-Control client. The Granted-Service-Unit AVP contains the amount of service units that the Diameter Credit-Control client can provide to the end user. The type of the Granted-Service-Unit can be time, volume, service-specific, or money, depending on the type of service event.

If the credit-control server determines that no credit-control is needed for the service, it can include the result code indicating that the credit-control is not applicable (e.g., the service is free of charge).

For informative purposes, the Credit-Control-Answer message MAY also include the Cost-Information AVP containing the estimated total cost of the requested service.

6.4. Refunds

Some services may refund service units to the end user's account -- for example, gaming services.

The credit-control client MUST set the CC-Request-Type AVP to the value EVENT_REQUEST and the Requested-Action AVP to REFUND_ACCOUNT in the Credit-Control-Request message. The Subscription-Id AVP or Subscription-Id-Extension AVP SHOULD be included to identify the end user in the credit-control server. The Service-Context-Id AVP indicates the service-specific document applicable to the request.

The Diameter Credit-Control client MAY include the monetary amount to be refunded in the Requested-Service-Unit AVP. The Service-Identifier AVP always indicates the service concerned. If the Diameter Credit-Control client does not know the monetary amount to

be refunded, in addition to the Service-Identifier AVP it MAY send service-specific AVPs or the Service-Parameter-Info AVP containing additional service event information to be rated.

For informative purposes, the Credit-Control-Answer message MAY also include the Cost-Information AVP containing the estimated monetary amount of refunded units.

6.5. Failure Procedure

Failover to an alternative credit-control server is allowed for a one-time event, as the server is not maintaining session states. For instance, if the credit-control client receives a protocol error DIAMETER_UNABLE_TO_DELIVER or DIAMETER_TOO_BUSY, it can resend the request to an alternative server, if possible. There MAY be protocol-transparent Diameter relays and redirect agents or Diameter Credit-Control proxies between the credit-control client and credit-control server. Failover may occur at any point in the path between the credit-control client and the credit-control server if a transport failure is detected with a peer, as described in [RFC6733]. Because there can be duplicate requests for various reasons, the credit-control server is responsible for real-time duplicate detection. Implementation issues for duplicate detection are discussed in [RFC6733], Appendix C.

When the credit-control client detects a communication failure with the credit-control server, its behavior depends on the requested action. The Tx timer (as defined in Section 13) is used in the credit-control client to supervise communication with the credit-control server.

If the requested action is PRICE_ENQUIRY or CHECK_BALANCE and a communication failure is detected, the credit-control client SHOULD forward the request messages to an alternative credit-control server, if possible. The secondary credit-control server name, if received from the home Diameter AAA server, can be used as an address of the backup server.

If the requested action is DIRECT_DEBITING, the DDFH controls the credit-control client's behavior. The DDFH may be received from the home Diameter AAA server or may be locally configured. The credit-control server may also send the DDFH in any CCA messages to be used for direct-debiting events compiled thereafter. The DDFH value received from the home Diameter AAA server overrides the locally configured value, and the DDFH value received from the credit-control server in a Credit-Control-Answer message always overrides any existing values.

If the DDFH is set to TERMINATE_OR_BUFFER, the credit-control client SHOULD NOT grant the service if, after a possible retransmission attempt to an alternative credit-control server, the credit-control client can eventually determine from the result code or error code in the Answer message that units have not been debited. Otherwise, the credit-control client SHOULD grant the service to the end user and store the request in credit-control application-level non-volatile storage. (Note that resending the request at a later time is not a guarantee that the service will be debited, as the user's account may be empty when the server successfully processes the request.) The credit-control client MUST mark these request messages as possible duplicates by setting the T flag in the command header as described in [RFC6733], Section 3.

If the DDFH is set to CONTINUE, the service SHOULD be granted, even if credit-control messages cannot be delivered and messages are not buffered.

If the Tx timer expires, the credit-control client MUST continue the service and wait for a possible late answer. If the request times out, the credit-control client retransmits the request (marked with the T flag) to a backup credit-control server, if possible. If the retransmitted request also times out or if a temporary error is received in answer, the credit-control client buffers the request if the value of the DDFH is set to TERMINATE_OR_BUFFER. If a failed answer is received for the retransmitted request, the credit-control client frees all the resources reserved for the event message and deletes the request regardless of the value of the DDFH.

The Credit-Control-Request with the requested action REFUND_ACCOUNT should always be stored in credit-control application-level non-volatile storage in case a temporary failure occurs. The credit-control client MUST mark the retransmitted request message as a possible duplicate by setting the T flag in the command header as described in [RFC6733], Section 3.

For stored requests, the implementation may choose to limit the number of retransmission attempts and to define a retransmission interval.

Note that only one entity in the credit-control system SHOULD be responsible for duplicate detection. If there is only one credit-control server within the given realm, the credit-control server may perform duplicate detection. If there is more than one credit-control server in a given realm, only one entity in the credit-control system should be responsible, to ensure that the end user's account is not debited or credited multiple times for the same service event.

7. Credit-Control Application State Machines

This section defines five credit-control application state machines. The first four state machines are to be observed by credit-control clients.

The first state machine describes session-based credit-control where the first interrogation is executed as part of the authorization/authentication process. The second state machine describes session-based credit-control where the first interrogation is executed after the authorization/authentication process. The requirements regarding what has to be supported for these two state machines are discussed in Section 5.2.

The third state machine describes session-based credit-control for the intermediate and final interrogations. The fourth state machine describes event-based credit-control. These two state machines are to be observed by all implementations that conform to this specification.

The fifth state machine describes the credit-control session from a credit-control server's perspective.

Any event not listed in the state machines MUST be considered an error condition, and a corresponding answer, if applicable, MUST be returned to the originator of the message.

In Tables 3, 4, and 5, the event "failure to send" means that the Diameter Credit-Control client is unable to communicate with the desired destination or, if a failover procedure is supported, with a possibly defined alternative destination (e.g., the request times out and the Answer message is not received). This could be due to (1) the peer being down or (2) a physical link failure in the path to or from the credit-control server.

The event "temporary error" means that the Diameter Credit-Control client received a protocol error notification (DIAMETER_TOO_BUSY, DIAMETER_UNABLE_TO_DELIVER, or DIAMETER_LOOP_DETECTED) in the Result-Code AVP of the Credit-Control-Answer command. This type of notification may ultimately be received in answer to the retransmitted request to a defined alternative destination, if failover is supported.

The event "failed answer" means that the Diameter Credit-Control client received a non-transient failure (permanent failure) notification in the Credit-Control-Answer command. This type of notification may ultimately be received in answer to the retransmitted request to a defined alternative destination, if failover is supported.

The action "store request" means that a request is stored in credit-control application-level non-volatile storage.

The event "not successfully processed" means that the credit-control server could not process the message, e.g., due to an unknown end user, an account being empty, or errors defined in [RFC6733].

The event "user service terminated" can be triggered for various reasons, e.g., normal user termination, network failure, and ASR (Abort-Session-Request). The Termination-Cause AVP contains information about the reason for termination, as specified in [RFC6733].

The Tx timer, which is used to control the waiting time in the credit-control client in the Pending state, is stopped upon exit of the Pending state. The stopping of the Tx timer is omitted in the state machine when the new state is Idle, as moving to Idle state implies the clearing of the session and all the variables associated to it.

The states PendingI, PendingU, PendingT, PendingE, and PendingB stand for pending states to wait for an answer to a credit-control request related to Initial, Update, Termination, Event, or Buffered request, respectively.

In Table 2, failover to a secondary server upon "temporary error" or "failure to send" is not explicitly described. However, moving an ongoing credit-control message stream to an alternative server is possible if the CC-Session-Failover AVP is set to FAILOVER_SUPPORTED, as described in Section 5.7.

Resending a credit-control event to an alternative server is supported as described in Section 6.5.

State	Event	Action	New State
Idle	Client or device requests access/service	Send AA-Request with added CC AVPs, start Tx timer	PendingI
PendingI	Successful answer to AA-Request received	Grant service to end user, stop Tx timer	Open
PendingI	Tx timer expired	Disconnect user/dev	Idle
PendingI	Failed AA-Answer received	Disconnect user/dev	Idle
PendingI	AA-Answer received with Result-Code equal to CREDIT_CONTROL_NOT_APPLICABLE	Grant service to end user	Idle
PendingI	User service terminated	Queue termination event	PendingI
PendingI	Change in rating condition	Queue changed rating condition event	PendingI

Table 2: Session-Based Client State Machine for the First Interrogation with AA-Request

State	Event	Action	New State
Idle	Client or device requests access/service	Send CC initial req., start Tx timer	PendingI
PendingI	Successful CC initial answer received	Stop Tx timer	Open
PendingI	Failure to send, or temporary error and CCFH equal to CONTINUE	Grant service to end user	Idle
PendingI	Failure to send, or temporary error and CCFH equal to TERMINATE or to RETRY_AND_TERMINATE	Terminate end user's service	Idle
PendingI	Tx timer expired and CCFH equal to TERMINATE	Terminate end user's service	Idle
PendingI	Tx timer expired and CCFH equal to CONTINUE or to RETRY_AND_TERMINATE	Grant service to end user	PendingI
PendingI	CC initial answer received with Result-Code equal to END_USER_SERVICE_DENIED or to USER_UNKNOWN	Terminate end user's service	Idle
PendingI	CC initial answer received with Result-Code equal to CREDIT_CONTROL_NOT_APPLICABLE	Grant service to end user	Idle
PendingI	Failed CC initial answer received and CCFH equal to CONTINUE	Grant service to end user	Idle
PendingI	Failed CC initial answer received and CCFH equal to TERMINATE or to RETRY_AND_TERMINATE	Terminate end user's service	Idle

PendingI	User service terminated	Queue termination event	PendingI
PendingI	Change in rating condition	Queue changed rating condition event	PendingI

Table 3: Session-Based Client State Machine for the First Interrogation with CCR

State	Event	Action	New State
Open	Granted unit elapses and no final-unit indication received	Send CC update req., start Tx timer	PendingU
Open	Granted unit elapses and final unit action equal to TERMINATE received	Terminate end user's service, send CC termination req.	PendingT
Open	Change in rating condition in queue	Send CC update req., start Tx timer	PendingU
Open	Service terminated in queue	Send CC termination req.	PendingT
Open	Change in rating condition or Validity-Time elapses	Send CC update req., start Tx timer	PendingU
Open	User service terminated	Send CC termination req.	PendingT

Open	RAR received	Send RAA followed by CC update req., start Tx timer	PendingU
PendingU	Successful CC update answer received	Stop Tx timer	Open
PendingU	Failure to send, or temporary error and CCFH equal to CONTINUE	Grant service to end user	Idle
PendingU	Failure to send, or temporary error and CCFH equal to TERMINATE or to RETRY_AND_TERMINATE	Terminate end user's service	Idle
PendingU	Tx timer expired and CCFH equal to TERMINATE	Terminate end user's service	Idle
PendingU	Tx timer expired and CCFH equal to CONTINUE or to RETRY_AND_TERMINATE	Grant service to end user	PendingU
PendingU	CC update answer received with Result-Code equal to END_USER_SERVICE_DENIED	Terminate end user's service	Idle
PendingU	CC update answer received with Result-Code equal to CREDIT_CONTROL_NOT_APPLICABLE	Grant service to end user	Idle
PendingU	Failed CC update answer received and CCFH equal to CONTINUE	Grant service to end user	Idle
PendingU	Failed CC update answer received and CCFH equal to TERMINATE or to RETRY_AND_TERMINATE	Terminate end user's service	Idle
PendingU	User service terminated	Queue termination event	PendingU

PendingU	Change in rating condition	Queue changed rating condition event	PendingU
PendingU	RAR received	Send RAA	PendingU
PendingT	Successful CC termination answer received		Idle
PendingT	Failure to send, temporary error, or failed answer		Idle
PendingT	Change in rating condition		PendingT

Table 4: Session-Based Client State Machine for Intermediate and Final Interrogations

State	Event	Action	New State
Idle	Client or device requests a one-time service	Send CC event req., start Tx timer	PendingE
Idle	Request in storage	Send stored request	PendingB
PendingE	Successful CC event answer received	Grant service to end user	Idle
PendingE	Failure to send, temporary error, failed CC event answer received, or Tx timer expired; requested action CHECK_BALANCE or PRICE_ENQUIRY	Indicate service error	Idle

PendingE	CC event answer received with Result-Code equal to END_USER_SERVICE_DENIED or to USER_UNKNOWN and Tx timer running	Terminate end user's service	Idle
PendingE	CC event answer received with Result-Code equal to CREDIT_CONTROL_NOT_APPLICABLE; requested action DIRECT_DEBITING	Grant service to end user	Idle
PendingE	Failure to send, temporary error, or failed CC event answer received; requested action DIRECT_DEBITING; DDFH equal to CONTINUE	Grant service to end user	Idle
PendingE	Failed CC event answer received or temporary error; requested action DIRECT_DEBITING; DDFH equal to TERMINATE_OR_BUFFER and Tx timer running	Terminate end user's service	Idle
PendingE	Tx timer expired; requested action DIRECT_DEBITING	Grant service to end user	PendingE
PendingE	Failure to send; requested action DIRECT_DEBITING; DDFH equal to TERMINATE_OR_BUFFER	Store request with T flag	Idle
PendingE	Temporary error; requested action DIRECT_DEBITING; DDFH equal to TERMINATE_OR_BUFFER; Tx timer expired	Store request	Idle
PendingE	Failed answer or answer received with Result-Code equal to END_USER_SERVICE DENIED or to USER_UNKNOWN; requested action DIRECT_DEBITING; Tx timer expired		Idle

PendingE	Failed CC event answer received; requested action REFUND_ACCOUNT	Indicate service error and delete request	Idle
PendingE	Failure to send or Tx timer expired; requested action REFUND_ACCOUNT	Store request with T flag	Idle
PendingE	Temporary error; requested action REFUND_ACCOUNT	Store request	Idle
PendingB	Successful CC answer received	Delete request	Idle
PendingB	Failed CC answer received	Delete request	Idle
PendingB	Failure to send or temporary error		Idle

Table 5: One-Time Event Client State Machine

State	Event	Action	New State
Idle	CC initial request received and successfully processed	Send CC initial answer, reserve units, start Tcc	Open
Idle	CC initial request received but not successfully processed	Send CC initial answer with Result-Code != SUCCESS	Idle
Idle	CC event request received and successfully processed	Send CC event answer	Idle
Idle	CC event request received but not successfully processed	Send CC event answer with Result-Code != SUCCESS	Idle

Open	CC update request received and successfully processed	Send CC update answer, debit used units, reserve new units, restart Tcc	Open
Open	CC update request received but not successfully processed	Send CC update answer with Result-Code != SUCCESS, debit used units	Idle
Open	CC termination request received and successfully processed	Send CC termin. answer, stop Tcc, debit used units	Idle
Open	CC termination request received but not successfully processed	Send CC termin. answer with Result-Code != SUCCESS, debit used units	Idle
Open	Session supervision timer Tcc expired	Release reserved units	Idle

Table 6: Session-Based and Event-Based Server State Machine

8. Credit-Control AVPs

This section defines the Credit-Control AVPs that are specific to the Diameter Credit-Control application and that MAY be included in the Diameter Credit-Control messages.

The AVPs defined in this section MAY also be included in authorization commands defined in authorization-specific applications, such as [RFC7155] and [RFC4004], if the first interrogation is performed as part of the authorization/ authentication process, as described in Section 5.2.

The Diameter AVP rules are defined in [RFC6733], Section 4. These AVP rules are observed in AVPs defined in this section.

The following table describes the Diameter AVPs defined in the credit-control application, their AVP Code values, types, and possible flag values. The AVP Flag rules ('M', 'V') are explained in [RFC6733], Section 4.1.

Attribute Name	AVP Code	Defined in Section	Data Type	AVP Flag Rules		
				MUST	MAY	MUST NOT
CC-Correlation-Id	411	8.1	OctetString		M	V
CC-Input-Octets	412	8.24	Unsigned64	M		V
CC-Money	413	8.22	Grouped	M		V
CC-Output-Octets	414	8.25	Unsigned64	M		V
CC-Request-Number	415	8.2	Unsigned32	M		V
CC-Request-Type	416	8.3	Enumerated	M		V
CC-Service-Specific-Units	417	8.26	Unsigned64	M		V
CC-Session-Failover	418	8.4	Enumerated	M		V
CC-Sub-Session-Id	419	8.5	Unsigned64	M		V
CC-Time	420	8.21	Unsigned32	M		V
CC-Total-Octets	421	8.23	Unsigned64	M		V
CC-Unit-Type	454	8.32	Enumerated	M		V
Check-Balance-Result	422	8.6	Enumerated	M		V
Cost-Information	423	8.7	Grouped	M		V
Cost-Unit	424	8.12	UTF8String	M		V
Credit-Control	426	8.13	Enumerated	M		V
Credit-Control-Failure-Handling	427	8.14	Enumerated	M		V
Currency-Code	425	8.11	Unsigned32	M		V
Direct-Debiting-Failure-Handling	428	8.15	Enumerated	M		V
Exponent	429	8.9	Integer32	M		V
Final-Unit-Action	449	8.35	Enumerated	M		V
Final-Unit-Indication	430	8.34	Grouped	M		V
QoS-Final-Unit-Indication	669	8.68	Grouped		M	V
Granted-Service-Unit	431	8.17	Grouped	M		V
G-S-U-Pool-Identifier	453	8.31	Unsigned32	M		V
G-S-U-Pool-Reference	457	8.30	Grouped	M		V
Multiple-Services-Credit-Control	456	8.16	Grouped	M		V
Multiple-Services-Indicator	455	8.40	Enumerated	M		V
Rating-Group	432	8.29	Unsigned32	M		V
Redirect-Address-Type	433	8.38	Enumerated	M		V
Redirect-Server	434	8.37	Grouped	M		V
Redirect-Server-Address	435	8.39	UTF8String	M		V
Redirect-Server-Extension	665	8.64	Grouped		M	V
Redirect-Address-IPAddress	666	8.65	Address		M	V
Redirect-Address-URL	667	8.66	UTF8String		M	V
Redirect-Address-SIP-URI	668	8.67	UTF8String		M	V

Requested-Action	436	8.41	Enumerated	M		V
Requested-Service-Unit	437	8.18	Grouped	M		V
Restriction-Filter-Rule	438	8.36	IPFilterRule	M		V
Service-Context-Id	461	8.42	UTF8String	M		V
Service-Identifier	439	8.28	Unsigned32	M		V
Service-Parameter-Info	440	8.43	Grouped		M	V
Service-Parameter-Type	441	8.44	Unsigned32		M	V
Service-Parameter-Value	442	8.45	OctetString		M	V
Subscription-Id	443	8.46	Grouped	M		V
Subscription-Id-Data	444	8.48	UTF8String	M		V
Subscription-Id-Type	450	8.47	Enumerated	M		V
Subscription-Id-Extension	659	8.58	Grouped		M	V
Subscription-Id-E164	660	8.59	UTF8String		M	V
Subscription-Id-IMSI	661	8.60	UTF8String		M	V
Subscription-Id-SIP-URI	662	8.61	UTF8String		M	V
Subscription-Id-NAI	663	8.62	UTF8String		M	V
Subscription-Id-Private	664	8.63	UTF8String		M	V
Tariff-Change-Usage	452	8.27	Enumerated	M		V
Tariff-Time-Change	451	8.20	Time	M		V
Unit-Value	445	8.8	Grouped	M		V
Used-Service-Unit	446	8.19	Grouped	M		V
User-Equipment-Info	458	8.49	Grouped		M	V
User-Equipment-Info-Type	459	8.50	Enumerated		M	V
User-Equipment-Info-Value	460	8.51	OctetString		M	V
User-Equipment-Info-Extension	653	8.52	Grouped		M	V
User-Equipment-Info-IMEISV	654	8.53	OctetString		M	V
User-Equipment-Info-MAC	655	8.54	OctetString		M	V
User-Equipment-Info-EUI64	656	8.55	OctetString		M	V
User-Equipment-Info-ModifiedEUI64	657	8.56	OctetString		M	V
User-Equipment-Info-IMEI	658	8.57	OctetString		M	V
Value-Digits	447	8.10	Integer64	M		V
Validity-Time	448	8.33	Unsigned32	M		V

8.1. CC-Correlation-Id AVP

The CC-Correlation-Id AVP (AVP Code 411) is of type OctetString and contains information to correlate credit-control requests generated for different components of the service, e.g., transport and service level. Whoever allocates the Service-Context-Id (i.e., a unique identifier of a service-specific document) is also responsible for defining the content and encoding of the CC-Correlation-Id AVP.

8.2. CC-Request-Number AVP

The CC-Request-Number AVP (AVP Code 415) is of type Unsigned32 and identifies this request within one session. As Session-Id AVPs are globally unique, the combination of the Session-Id AVP and the CC-Request-Number AVP is also globally unique and can be used in matching credit-control messages with confirmations. An easy way to produce unique numbers is to set the value of the CC-Request-Number AVP to 0 for a credit-control request with a CC-Request-Type AVP of INITIAL_REQUEST (the initial request in a session). The value of the CC-Request-Number AVP should be set to 1 for the first UPDATE_REQUEST, to 2 for the second, and so on until the value for TERMINATION_REQUEST is one more than the value for the last UPDATE_REQUEST. In the case of event charging (when the CC-Request-Type AVP has the value EVENT_REQUEST), the CC-Request-Number AVP should be set to 0 for a credit-control request.

8.3. CC-Request-Type AVP

The CC-Request-Type AVP (AVP Code 416) is of type Enumerated and contains the reason for sending the Credit-Control-Request message. It MUST be present in all Credit-Control-Request messages. The following values are defined for the CC-Request-Type AVP (the value of 0 (zero) is reserved):

INITIAL_REQUEST 1

This request is used to initiate a credit-control session. It contains credit-control information that is relevant to the initiation.

UPDATE_REQUEST 2

This request contains credit-control information for an existing credit-control session. Credit-control requests of this type SHOULD be sent every time a credit-control re-authorization is needed at the expiry of the allocated quota or validity time. Further, additional service-specific events MAY trigger a spontaneous UPDATE_REQUEST.

TERMINATION_REQUEST 3

This request is sent to terminate a credit-control session. It contains credit-control information relevant to the existing session.

EVENT_REQUEST 4

This request is used when there is no need to maintain any credit-control session state in the credit-control server. It contains all information relevant to the service and is the only request of the service. The reason for this request is further detailed in the Requested-Action AVP. The Requested-Action AVP MUST be included in the Credit-Control-Request message when CC-Request-Type is set to EVENT_REQUEST.

8.4. CC-Session-Failover AVP

The CC-Session-Failover AVP (AVP Code 418) is of type Enumerated and contains information as to whether moving the credit-control message stream to a backup server during an ongoing credit-control session is supported. In the case of communication failures, the credit-control message streams can be moved to an alternative destination if the credit-control server supports failover to an alternative server. The secondary credit-control server name, if received from the home Diameter AAA server, can be used as an address of the backup server. An implementation is not required to support moving a credit-control message stream to an alternative server, as this also requires moving information related to the credit-control session to the backup server.

The following values are defined for the CC-Session-Failover AVP:

FAILOVER_NOT_SUPPORTED 0

When the CC-Session-Failover AVP is set to FAILOVER_NOT_SUPPORTED, the credit-control message stream MUST NOT be moved to an alternative destination in the case of a communication failure. This is the default behavior if the AVP isn't included in the reply from the authorization or credit-control server.

FAILOVER_SUPPORTED 1

When the CC-Session-Failover AVP is set to FAILOVER_SUPPORTED, the credit-control message stream SHOULD be moved to an alternative destination in the case of a communication failure. Moving the credit-control message stream to a backup server MAY require that information related to the credit-control session should also be forwarded to an alternative server.

8.5. CC-Sub-Session-Id AVP

The CC-Sub-Session-Id AVP (AVP Code 419) is of type Unsigned64 and contains the credit-control sub-session identifier. The combination of the Session-Id AVP and this AVP MUST be unique per sub-session, and the value of this AVP MUST be monotonically increased by one for all new sub-sessions. The absence of this AVP implies that no sub-sessions are in use.

8.6. Check-Balance-Result AVP

The Check-Balance-Result AVP (AVP Code 422) is of type Enumerated and contains the result of the balance check. This AVP is applicable only when the Requested-Action AVP indicates CHECK_BALANCE in the Credit-Control-Request command. The following values are defined for the Check-Balance-Result AVP:

ENOUGH_CREDIT 0

There is enough credit in the account to cover the requested service.

NO_CREDIT 1

There isn't enough credit in the account to cover the requested service.

8.7. Cost-Information AVP

The Cost-Information AVP (AVP Code 423) is of type Grouped, and it is used to return the cost information of a service, which the credit-control client can transfer transparently to the end user. The included Unit-Value AVP contains the cost estimate (always of type "money") of the service in the case of price inquiries, or the accumulated cost estimation in the case of a credit-control session.

The Currency-Code AVP specifies in which currency the cost was given. The Cost-Unit AVP specifies the unit when the service cost is a cost per unit (e.g., cost for the service is $1 per minute).

When the Requested-Action AVP with the value PRICE_ENQUIRY is included in the Credit-Control-Request command, the Cost-Information AVP sent in the succeeding Credit-Control-Answer command contains the cost estimation for the requested service, without any reservations being made.

The Cost-Information AVP included in the Credit-Control-Answer command with the CC-Request-Type set to UPDATE_REQUEST contains the accumulated cost estimation for the session, without taking any credit reservations into account.

The Cost-Information AVP included in the Credit-Control-Answer command with the CC-Request-Type set to EVENT_REQUEST or TERMINATION_REQUEST contains the estimated total cost for the requested service.

The Cost-Information AVP is defined as follows (per grouped-avp-def as defined in [RFC6733]):

```
Cost-Information ::= < AVP Header: 423 >
                     { Unit-Value }
                     { Currency-Code }
                     [ Cost-Unit ]
```

8.8. Unit-Value AVP

The Unit-Value AVP is of type Grouped (AVP Code 445) and specifies the cost as a floating-point value. The Unit-Value is a significand with an exponent; i.e., Unit-Value = Value-Digits AVP * 10^Exponent. This representation avoids unwanted rounding off. For example, the value of 2,3 is represented as Value-Digits = 23 and Exponent = -1. The absence of the exponent part MUST be interpreted as an exponent equal to zero.

The Unit-Value AVP is defined as follows (per grouped-avp-def as defined in [RFC6733]):

```
Unit-Value ::= < AVP Header: 445 >
               { Value-Digits }
               [ Exponent ]
```

8.9. Exponent AVP

The Exponent AVP is of type Integer32 (AVP Code 429) and contains the exponent value to be applied for the Value-Digits AVP within the Unit-Value AVP.

8.10. Value-Digits AVP

The Value-Digits AVP is of type Integer64 (AVP Code 447) and contains the significant digits of the number. If decimal values are needed to present the units, the scaling MUST be indicated with the related Exponent AVP. For example, for the monetary amount $0.05, the value of the Value-Digits AVP MUST be set to 5, and the scaling MUST be indicated with the Exponent AVP set to -2.

8.11. Currency-Code AVP

The Currency-Code AVP (AVP Code 425) is of type Unsigned32 and contains a currency code that specifies in which currency the values of AVPs containing monetary units were given. It is specified by using the numeric values defined in the ISO 4217 standard [ISO4217].

8.12. Cost-Unit AVP

The Cost-Unit AVP (AVP Code 424) is of type UTF8String, and it is used to display a human-readable string to the end user. It specifies the applicable unit to the Cost-Information AVP when the service cost is a cost per unit (e.g., cost of the service is $1 per minute). The Cost-Unit setting can be minutes, hours, days, kilobytes, megabytes, etc.

8.13. Credit-Control AVP

The Credit-Control AVP (AVP Code 426) is of type Enumerated and MUST be included in AA-Request messages when the Service Element has credit-control capabilities. The following values are defined for the Credit-Control AVP:

CREDIT_AUTHORIZATION 0

If the home Diameter AAA server determines that the user has a prepaid subscription, this value indicates that the credit-control server MUST be contacted to perform the first interrogation. The value of the Credit-Control AVP MUST always be set to 0 in an AA-Request sent to perform the first interrogation and to initiate a new credit-control session.

RE_AUTHORIZATION 1

This value indicates to the Diameter AAA server that a credit-control session is ongoing for the subscriber and that the credit-control server MUST NOT be contacted. The Credit-Control AVP set to the value of 1 is to be used only when the first interrogation has been successfully performed and the credit-control session is ongoing

(i.e., re-authorization triggered by authorization lifetime). This value MUST NOT be used in an AA-Request sent to perform the first interrogation.

8.14. Credit-Control-Failure-Handling AVP (CCFH)

The CCFH (AVP Code 427) is of type Enumerated. The credit-control client uses information in this AVP to decide what to do if sending credit-control messages to the credit-control server has been, for instance, temporarily prevented due to a network problem. Depending on the service logic, the credit-control server can order the client to terminate the service immediately when there is a reason to believe that the service cannot be charged, or to try failover to an alternative server, if possible. The server could then either terminate or grant the service, should the alternative connection also fail.

The following values are defined for the CCFH:

TERMINATE 0

When the CCFH is set to TERMINATE, the service MUST only be granted for as long as there is a connection to the credit-control server. If the credit-control client does not receive any Credit-Control-Answer messages before the Tx timer (as defined in Section 13) expires, the credit-control request is regarded as failed, and the end user's service session is terminated.

This is the default behavior if the AVP isn't included in the reply from the authorization or credit-control server.

CONTINUE 1

When the CCFH is set to CONTINUE, the credit-control client SHOULD resend the request to an alternative server in the case of transport or temporary failures, provided that (1) a failover procedure is supported in the credit-control server and the credit-control client and (2) an alternative server is available. Otherwise, the service SHOULD be granted, even if credit-control messages can't be delivered.

RETRY_AND_TERMINATE 2

When the CCFH is set to RETRY_AND_TERMINATE, the credit-control client SHOULD resend the request to an alternative server in the case of transport or temporary failures, provided that (1) a failover procedure is supported in the credit-control server and the credit-control client and (2) an alternative server is available.

Otherwise, the service SHOULD NOT be granted when the credit-control messages can't be delivered.

8.15. Direct-Debiting-Failure-Handling AVP (DDFH)

The DDFH (AVP Code 428) is of type Enumerated. The credit-control client uses information in this AVP to decide what to do if sending credit-control messages (Requested-Action AVP set to DIRECT_DEBITING) to the credit-control server has been, for instance, temporarily prevented due to a network problem.

The following values are defined for the DDFH:

TERMINATE_OR_BUFFER 0

When the DDFH is set to TERMINATE_OR_BUFFER, the service MUST be granted for as long as there is a connection to the credit-control server. If the credit-control client does not receive any Credit-Control-Answer messages before the Tx timer (as defined in Section 13) expires, the credit-control request is regarded as failed. The client SHOULD terminate the service if it can determine from the failed answer that units have not been debited. Otherwise, the credit-control client SHOULD grant the service, store the request in application-level non-volatile storage, and try to resend the request. These requests MUST be marked as possible duplicates by setting the T flag in the command header as described in [RFC6733], Section 3. This is the default behavior if the AVP isn't included in the reply from the authorization server.

CONTINUE 1

When the DDFH is set to CONTINUE, the service SHOULD be granted, even if credit-control messages can't be delivered, and the request should be deleted.

8.16. Multiple-Services-Credit-Control AVP

The Multiple-Services-Credit-Control AVP (AVP Code 456) is of type Grouped and contains the AVPs related to the independent credit-control of multiple services. Note that each instance of this AVP carries units related to one or more services or related to a single rating-group.

The Service-Identifier AVP and the Rating-Group AVP are used to associate the granted units to a given service or rating-group. If both the Service-Identifier AVP and the Rating-Group AVP are included, the target of the service units is always the service(s) indicated by the value of the Service-Identifier AVP(s). If only the

Rating-Group AVP is present, the Multiple-Services-Credit-Control AVP relates to all the services that belong to the specified rating-group.

The G-S-U-Pool-Reference AVP allows the server to specify a G-S-U-Pool-Identifier identifying a credit pool within which the units of the specified type are considered pooled. If a G-S-U-Pool-Reference AVP is present, then actual service units of the specified type MUST also be present. For example, if the G-S-U-Pool-Reference AVP specifies a CC-Unit-Type value of TIME (Section 8.32), then the CC-Time AVP MUST be present.

The Requested-Service-Unit AVP MAY contain the amount of requested service units or the requested monetary value. It MUST be present in the initial interrogation and within the intermediate interrogations in which a new quota is requested. If the credit-control client does not include the Requested-Service-Unit AVP in a request command -- because, for instance, it has determined that the end user terminated the service -- the server MUST debit the used amount from the user's account but MUST NOT return a new quota in the corresponding answer. The Validity-Time, Result-Code, and Final-Unit-Indication or QoS-Final-Unit-Indication AVPs MAY be present in a Credit-Control-Answer command as defined in Sections 5.1.2 and 5.6 for graceful service termination.

When both the Tariff-Time-Change AVP and the Tariff-Change-Usage AVP are present, the server MUST include two separate instances of the Multiple-Services-Credit-Control AVP with the Granted-Service-Unit AVP associated to the same service-identifier and/or rating-group. Where the two quotas are associated to the same pool or to different pools, the credit-pooling mechanism defined in Section 5.1.2 applies. When the client is reporting used units before and after the tariff time change, it MUST use the Tariff-Change-Usage AVP inside the Used-Service-Unit AVP.

A server not implementing the independent credit-control of multiple services MUST treat the Multiple-Services-Credit-Control AVP as an invalid AVP.

The Multiple-Services-Credit-Control AVP is defined as follows (per grouped-avp-def as defined in [RFC6733]):

```
 Multiple-Services-Credit-Control ::= < AVP Header: 456 >
                                       [ Granted-Service-Unit ]
                                       [ Requested-Service-Unit ]
                                      *[ Used-Service-Unit ]
                                       [ Tariff-Change-Usage ]
                                      *[ Service-Identifier ]
                                       [ Rating-Group ]
                                      *[ G-S-U-Pool-Reference ]
                                       [ Validity-Time ]
                                       [ Result-Code ]
                                       [ Final-Unit-Indication ]
                                       [ QoS-Final-Unit-Indication ]
                                      *[ AVP ]
```

8.17. Granted-Service-Unit AVP

The Granted-Service-Unit AVP (AVP Code 431) is of type Grouped and contains the amount of units that the Diameter Credit-Control client can provide to the end user until the service must be released or the new Credit-Control-Request must be sent. A client is not required to implement all the unit types, and it must treat unknown or unsupported unit types in the Answer message as an incorrect CCA. In this case, the client MUST terminate the credit-control session and indicate the reason as DIAMETER_BAD_ANSWER in the Termination-Cause AVP.

The Granted-Service-Unit AVP is defined as follows (per grouped-avp-def as defined in [RFC6733]):

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

8.18. Requested-Service-Unit AVP

The Requested-Service-Unit AVP (AVP Code 437) is of type Grouped and contains the amount of requested units specified by the Diameter Credit-Control client. A server is not required to implement all the unit types, and it must treat unknown or unsupported unit types as invalid AVPs.

The Requested-Service-Unit AVP is defined as follows (per grouped-avp-def as defined in [RFC6733]):

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

8.19. Used-Service-Unit AVP

The Used-Service-Unit AVP is of type Grouped (AVP Code 446) and contains the amount of used units measured from the point when the service became active or, if interim interrogations are used during the session, from the point when the previous measurement ended. Note: The value reported in a Used-Service-Unit AVP is not necessarily related to the grant provided in a Granted-Service-Unit AVP, e.g., the value in this AVP may exceed the value in the grant.

The Used-Service-Unit AVP is defined as follows (per grouped-avp-def as defined in [RFC6733]):

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

8.20. Tariff-Time-Change AVP

The Tariff-Time-Change AVP (AVP Code 451) is of type Time. It is sent from the server to the client and includes the time in seconds since January 1, 1900, 00:00 UTC, when the tariff of the service will be changed.

The tariff change mechanism is optional for the client and server, and it is not used for time-based services (Section 5). If a client does not support the tariff time change mechanism, it MUST treat the Tariff-Time-Change AVP in the Answer message as an incorrect CCA. In this case, the client terminates the credit-control session and indicates the reason as DIAMETER_BAD_ANSWER in the Termination-Cause AVP.

Omission of this AVP means that no tariff change is to be reported.

8.21. CC-Time AVP

The CC-Time AVP (AVP Code 420) is of type Unsigned32 and indicates the length of the requested, granted, or used time in seconds.

8.22. CC-Money AVP

The CC-Money AVP (AVP Code 413) is of type Grouped and specifies the monetary amount in the given currency. The Currency-Code AVP SHOULD be included. The CC-Money AVP is defined as follows (per grouped-avp-def as defined in [RFC6733]):

```
CC-Money ::= < AVP Header: 413 >
             { Unit-Value }
             [ Currency-Code ]
```

8.23. CC-Total-Octets AVP

The CC-Total-Octets AVP (AVP Code 421) is of type Unsigned64 and contains the total number of requested, granted, or used octets regardless of the direction (sent or received).

8.24. CC-Input-Octets AVP

The CC-Input-Octets AVP (AVP Code 412) is of type Unsigned64 and contains the number of requested, granted, or used octets that can be / have been received from the end user.

8.25. CC-Output-Octets AVP

The CC-Output-Octets AVP (AVP Code 414) is of type Unsigned64 and contains the number of requested, granted, or used octets that can be / have been sent to the end user.

8.26. CC-Service-Specific-Units AVP

The CC-Service-Specific-Units AVP (AVP Code 417) is of type Unsigned64 and specifies the number of service-specific units (e.g., number of events, points) given in a selected service. The service-specific units always refer to the service identified in the Service-Identifier AVP (or Rating-Group AVP when the Multiple-Services-Credit-Control AVP is used).

8.27. Tariff-Change-Usage AVP

The Tariff-Change-Usage AVP (AVP Code 452) is of type Enumerated and defines whether units are used before or after a tariff change, or whether the units straddled a tariff change during the reporting period. Omission of this AVP means that no tariff change has occurred.

In addition, when present in Answer messages as part of the Multiple-Services-Credit-Control AVP, this AVP defines whether units are allocated to be used before or after a tariff change event.

When the Tariff-Time-Change AVP is present, omission of this AVP in Answer messages means that the single-quota mechanism applies.

Tariff-Change-Usage can be set to one of the following values:

UNIT_BEFORE_TARIFF_CHANGE 0

When present in the Multiple-Services-Credit-Control AVP, this value indicates the amount of units allocated for use before a tariff change occurs.

When present in the Used-Service-Unit AVP, this value indicates the amount of resource units used before a tariff change had occurred.

UNIT_AFTER_TARIFF_CHANGE 1

When present in the Multiple-Services-Credit-Control AVP, this value indicates the amount of units allocated for use after a tariff change occurs.

When present in the Used-Service-Unit AVP, this value indicates the amount of resource units used after a tariff change had occurred.

UNIT_INDETERMINATE 2

This value is to be used only in the Used-Service-Unit AVP and indicates the amount of resource units that straddle the tariff change (e.g., the metering process reports to the credit-control client in blocks of n octets, and one block straddled the tariff change).

8.28. Service-Identifier AVP

The Service-Identifier AVP is of type Unsigned32 (AVP Code 439) and contains the identifier of a service. The specific service the request relates to is uniquely identified by the combination of the Service-Context-Id AVP and the Service-Identifier AVP.

A usage example of this AVP is illustrated in Appendix A.9.

8.29. Rating-Group AVP

The Rating-Group AVP is of type Unsigned32 (AVP Code 432) and contains the identifier of a rating-group. All the services subject to the same rating type are part of the same rating-group. The specific rating-group the request relates to is uniquely identified by the combination of the Service-Context-Id AVP and the Rating-Group AVP.

A usage example of this AVP is illustrated in Appendix A.9.

8.30. G-S-U-Pool-Reference AVP

The G-S-U-Pool-Reference AVP (AVP Code 457) is of type Grouped. It is used in the Credit-Control-Answer message and associates the Granted-Service-Unit AVP within which it appears with a credit pool within the session.

The G-S-U-Pool-Identifier AVP specifies the credit pool from which credit is drawn for this unit type.

The CC-Unit-Type AVP specifies the type of units for which credit is pooled.

The Unit-Value AVP specifies the multiplier, which converts between service units of type CC-Unit-Type and abstract service units within the credit pool (and thus to service units of any other services or rating-groups associated with the same pool).

The G-S-U-Pool-Reference AVP is defined as follows (per grouped-avp-def as defined in [RFC6733]):

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

8.31. G-S-U-Pool-Identifier AVP

The G-S-U-Pool-Identifier AVP (AVP Code 453) is of type Unsigned32 and identifies a credit pool within the session.

8.32. CC-Unit-Type AVP

The CC-Unit-Type AVP (AVP Code 454) is of type Enumerated and specifies the type of units considered to be pooled into a credit pool.

The following values are defined for the CC-Unit-Type AVP:

TIME	0
MONEY	1
TOTAL-OCTETS	2
INPUT-OCTETS	3
OUTPUT-OCTETS	4
SERVICE-SPECIFIC-UNITS	5

8.33. Validity-Time AVP

The Validity-Time AVP is of type Unsigned32 (AVP Code 448). It is sent from the credit-control server to the credit-control client. The Validity-Time AVP contains the validity time of the granted service units. The measurement of the Validity-Time is started upon receipt of the Credit-Control-Answer message containing this AVP. If the granted service units have not been consumed within the validity time specified in this AVP, the credit-control client MUST send a Credit-Control-Request message to the server, with CC-Request-Type set to UPDATE_REQUEST. The value field of the Validity-Time AVP is given in seconds.

The Validity-Time AVP is also used for graceful service termination (see Section 5.6) to indicate to the credit-control client how long the subscriber is allowed to use network resources after the specified action (i.e., REDIRECT or RESTRICT_ACCESS) started. When the Validity-Time elapses, a new intermediate interrogation is sent to the server.

8.34. Final-Unit-Indication AVP

The Final-Unit-Indication AVP (AVP Code 430) is of type Grouped and indicates that the Granted-Service-Unit AVP in the Credit-Control-Answer or in the AA-Answer contains the final units for the service. After these units have expired, the Diameter Credit-Control client is responsible for executing the action indicated in the Final-Unit-Action AVP (see Section 5.6).

If more than one unit type is received in the Credit-Control-Answer, the unit type that first expired SHOULD cause the credit-control client to execute the specified action.

In the first interrogation, the Final-Unit-Indication AVP with Final-Unit-Action set to REDIRECT or RESTRICT_ACCESS can also be present with no Granted-Service-Unit AVP in the Credit-Control-Answer or in the AA-Answer. This indicates to the Diameter Credit-Control client that the client is to execute the specified action immediately. If the home service provider policy is to terminate the service, naturally, the server SHOULD return the appropriate transient failure (see Section 9.1) in order to implement the policy-defined action.

The Final-Unit-Action AVP defines the behavior of the Service Element when the user's account cannot cover the cost of the service and MUST always be present if the Final-Unit-Indication AVP is included in a command.

If the Final-Unit-Action AVP is set to TERMINATE, the Final-Unit-Indication group AVP MUST NOT contain any other AVPs.

If the Final-Unit-Action AVP is set to REDIRECT, the Redirect-Server AVP or the Redirect-Server-Extension AVP (at least one) MUST be present. The Restriction-Filter-Rule AVP or the Filter-Id AVP MAY be present in the Credit-Control-Answer message if the user is also allowed to access other services that are not accessible through the address given in the Redirect-Server AVP.

If the Final-Unit-Action AVP is set to RESTRICT_ACCESS, either the Restriction-Filter-Rule AVP or the Filter-Id AVP SHOULD be present.

The Filter-Id AVP is defined in [RFC7155]. The Filter-Id AVP can be used to reference an IP filter list installed in the access device by means other than the Diameter Credit-Control application, e.g., locally configured or configured by another entity.

If the Final-Unit-Action AVP is set to REDIRECT and the type of server is not one of the enumerations in the Redirect-Address-Type AVP, then the QoS-Final-Unit-Indication AVP SHOULD be used together with the Redirect-Server-Extension AVP instead of the Final-Unit-Indication AVP.

If the Final-Unit-Action AVP is set to RESTRICT_ACCESS or REDIRECT and the classification of the restricted traffic cannot be expressed using an IPFilterRule, or if actions (e.g., QoS) other than just allowing traffic need to be enforced, then the QoS-Final-Unit-Indication AVP SHOULD be used instead of the Final-Unit-Indication AVP. However, if the credit-control server wants to preserve backward compatibility with credit-control clients that support only [RFC4006], the Final-Unit-Indication AVP SHOULD be used together with the Filter-Id AVP.

The Final-Unit-Indication AVP is defined as follows (per grouped-avp-def as defined in [RFC6733]):

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

8.35. Final-Unit-Action AVP

The Final-Unit-Action AVP (AVP Code 449) is of type Enumerated and indicates to the credit-control client the action to be taken when the user's account cannot cover the service cost.

Final-Unit-Action can be set to one of the following values:

TERMINATE 0

The credit-control client MUST terminate the service session. This is the default handling, applicable whenever the credit-control client receives an unsupported Final-Unit-Action value, and it MUST be supported by all the Diameter Credit-Control client implementations conforming to this specification.

REDIRECT 1

The Service Element MUST redirect the user to the address specified in the Redirect-Server-Address AVP or one of the AVPs included in the Redirect-Server-Extension AVP. The redirect action is defined in Section 5.6.2.

RESTRICT_ACCESS 2

The access device MUST restrict the user's access according to the filter AVPs contained in the applied Grouped AVP: according to IP packet filters defined in the Restriction-Filter-Rule AVP, according to the packet classifier filters defined in the Filter-Rule AVP, or according to the packet filters identified by the Filter-Id AVP. All of the packets not matching any restriction filters (see Section 5.6.3) MUST be dropped.

8.36. Restriction-Filter-Rule AVP

The Restriction-Filter-Rule AVP (AVP Code 438) is of type IPFilterRule and provides filter rules corresponding to services that are to remain accessible even if there are no more service units granted. The access device has to configure the specified filter rules for the subscriber and MUST drop all the packets not matching these filters. Zero, one, or more such AVPs MAY be present in a Credit-Control-Answer message or in an AA-Answer message.

8.37. Redirect-Server AVP

The Redirect-Server AVP (AVP Code 434) is of type Grouped and contains the address information of the redirect server (e.g., HTTP redirect server, SIP Server) with which the end user is to be connected when the account cannot cover the service cost. It MUST be present when the Final-Unit-Action AVP is set to REDIRECT.

The Redirect-Server AVP is defined as follows (per grouped-avp-def as defined in [RFC6733]):

```
Redirect-Server ::= < AVP Header: 434 >
                    { Redirect-Address-Type }
                    { Redirect-Server-Address }
```

8.38. Redirect-Address-Type AVP

The Redirect-Address-Type AVP (AVP Code 433) is of type Enumerated and defines the address type of the address given in the Redirect-Server-Address AVP.

Redirect-Address-Type can be set to one of the following values:

IPv4 Address 0

The address type is in the form of a "dotted-decimal" IPv4 address, as defined in [RFC791].

IPv6 Address 1

The address type is in the form of an IPv6 address, as defined in [RFC4291]. The address MUST conform to the textual representation of the address according to [RFC5952].

Because [RFC5952] is more restrictive than the "RFC 3513" format required by [RFC4006], some legacy implementations may not be compliant with the new requirements. Accordingly, implementations receiving this AVP MAY be liberal in the textual IPv6 representations that are accepted, without raising an error.

URL 2

The address type is in the form of a Uniform Resource Locator, as defined in [RFC3986].

SIP URI 3

The address type is in the form of a SIP Uniform Resource Identifier, as defined in [RFC3261].

8.39. Redirect-Server-Address AVP

The Redirect-Server-Address AVP (AVP Code 435) is of type UTF8String and defines the address of the redirect server (e.g., HTTP redirect server, SIP Server) with which the end user is to be connected when the account cannot cover the service cost.

8.40. Multiple-Services-Indicator AVP

The Multiple-Services-Indicator AVP (AVP Code 455) is of type Enumerated and indicates whether the Diameter Credit-Control client is capable of handling multiple services independently within a (sub-)session. The absence of this AVP means that independent credit-control of multiple services is not supported.

A server not implementing the independent credit-control of multiple services MUST treat the Multiple-Services-Indicator AVP as an invalid AVP.

The following values are defined for the Multiple-Services-Indicator AVP:

MULTIPLE_SERVICES_NOT_SUPPORTED 0

The client does not support independent credit-control of multiple services within a (sub-)session.

MULTIPLE_SERVICES_SUPPORTED 1

The client supports independent credit-control of multiple services within a (sub-)session.

8.41. Requested-Action AVP

The Requested-Action AVP (AVP Code 436) is of type Enumerated and contains the requested action being sent in a Credit-Control-Request command where the CC-Request-Type is set to EVENT_REQUEST. The following values are defined for the Requested-Action AVP:

DIRECT_DEBITING 0

This indicates a request to decrease the end user's account according to information specified in the Requested-Service-Unit AVP and/or Service-Identifier AVP (additional rating information may be included in service-specific AVPs or in the Service-Parameter-Info AVP). The Granted-Service-Unit AVP in the Credit-Control-Answer command contains the debited units.

REFUND_ACCOUNT 1

This indicates a request to increase the end user's account according to information specified in the Requested-Service-Unit AVP and/or Service-Identifier AVP (additional rating information may be included in service-specific AVPs or in the Service-Parameter-Info AVP). The Granted-Service-Unit AVP in the Credit-Control-Answer command contains the refunded units.

CHECK_BALANCE 2

This indicates a balance-check request. In this case, the checking of the account balance is done without any credit reservations from the account. The Check-Balance-Result AVP in the Credit-Control-Answer command contains the result of the balance check.

PRICE_ENQUIRY 3

This indicates a price-inquiry request. In this case, neither checking of the account balance nor reservation from the account will be done; only the price of the service will be returned in the Cost-Information AVP in the Credit-Control-Answer command.

8.42. Service-Context-Id AVP

The Service-Context-Id AVP is of type UTF8String (AVP Code 461) and contains a unique identifier of the Diameter Credit-Control service-specific document (as defined in Section 4.1.2) that applies to the request. This is an identifier allocated by the service provider, the Service Element manufacturer, or a standardization body, and MUST uniquely identify a given Diameter Credit-Control service-specific document. The format of the Service-Context-Id is:

"service-context" "@" "domain"

service-context = Token

The Token is an arbitrary string of characters and digits.

"domain" represents the entity that allocated the Service-Context-Id. It can be ietf.org, 3gpp.org, etc. if the identifier is allocated by a standardization body, or it can be the Fully Qualified Domain Name (FQDN) of the service provider (e.g., provider.example.com) or the vendor (e.g., vendor.example.com) if the identifier is allocated by a private entity.

This AVP SHOULD be placed as close to the Diameter header as possible.

Service-specific documents that are for private use only (i.e., for one provider's own use, where no interoperability is deemed useful) may define private identifiers without a need for coordination. However, when interoperability is desired, coordination of the identifiers via, for example, publication of an informational RFC is RECOMMENDED in order to make the Service-Context-Id AVP globally available.

8.43. Service-Parameter-Info AVP

The Service-Parameter-Info AVP (AVP Code 440) is of type Grouped and contains service-specific information used for price calculation or rating. The Service-Parameter-Type AVP defines the service parameter type, and the Service-Parameter-Value AVP contains the parameter value. The actual contents of these AVPs are not within the scope of this document and SHOULD be defined in another Diameter application, in standards written by other standardization bodies, or in service-specific documentation.

In the case of an unknown service request (e.g., unknown Service-Parameter-Type), the corresponding Answer message MUST contain the error code DIAMETER_RATING_FAILED. A Credit-Control-Answer message with this error MUST contain one or more Failed-AVP AVPs containing the Service-Parameter-Info AVPs that caused the failure.

The Service-Parameter-Info AVP is defined as follows (per grouped-avp-def as defined in [RFC6733]):

```
Service-Parameter-Info ::= < AVP Header: 440 >
                           { Service-Parameter-Type }
                           { Service-Parameter-Value }
```

8.44. Service-Parameter-Type AVP

The Service-Parameter-Type AVP is of type Unsigned32 (AVP Code 441) and defines the type of the service-event-specific parameter (e.g., it can be the end-user location or service name). The different parameters and their types are service specific, and the meanings of these parameters are not defined in this document. Whoever allocates the Service-Context-Id (i.e., a unique identifier of a service-specific document) is also responsible for assigning Service-Parameter-Type values for the service and ensuring their uniqueness within the given service. The Service-Parameter-Value AVP contains the value associated with the service parameter type.

8.45. Service-Parameter-Value AVP

The Service-Parameter-Value AVP is of type OctetString (AVP Code 442) and contains the value of the service parameter type.

8.46. Subscription-Id AVP

The Subscription-Id AVP (AVP Code 443) is used to identify the end user's subscription and is of type Grouped. The Subscription-Id AVP includes a Subscription-Id-Data AVP that holds the identifier and a Subscription-Id-Type AVP that defines the identifier type.

The Subscription-Id AVP is defined as follows (per grouped-avp-def as defined in [RFC6733]):

```
Subscription-Id ::= < AVP Header: 443 >
                    { Subscription-Id-Type }
                    { Subscription-Id-Data }
```

8.47. Subscription-Id-Type AVP

The Subscription-Id-Type AVP (AVP Code 450) is of type Enumerated, and it is used to determine which type of identifier is carried by the Subscription-Id AVP.

This specification defines the following subscription identifiers. However, new Subscription-Id-Type values can be assigned by IANA as defined in Section 12. A server MUST implement all the Subscription-Id-Type values required to perform credit authorization for the services it supports, including possible future values. Unknown or unsupported Subscription-Id-Type values MUST be treated according to the 'M' flag rule, as defined in [RFC6733].

END_USER_E164 0

The identifier is in international E.164 format (e.g., MSISDN), according to the ITU-T E.164 numbering plan defined in [E164] and [CE164].

END_USER_IMSI 1

The identifier is in IMSI format, according to the ITU-T E.212 identification plan as defined in [E212] and [CE212].

END_USER_SIP_URI 2

The identifier is in the form of a SIP URI, as defined in [RFC3261].

END_USER_NAI 3

The identifier is in the form of a Network Access Identifier, as defined in [RFC7542].

END_USER_PRIVATE 4

The identifier is a credit-control server private identifier.

8.48. Subscription-Id-Data AVP

The Subscription-Id-Data AVP (AVP Code 444) is used to identify the end user and is of type UTF8String. The Subscription-Id-Type AVP defines which type of identifier is used.

8.49. User-Equipment-Info AVP

The User-Equipment-Info AVP (AVP Code 458) is of type Grouped and allows the credit-control client to indicate the identity and capability of the terminal the subscriber is using for the connection to the network.

The User-Equipment-Info AVP is defined as follows (per grouped-avp-def as defined in [RFC6733]):

```
User-Equipment-Info ::= < AVP Header: 458 >
                        { User-Equipment-Info-Type }
                        { User-Equipment-Info-Value }
```

8.50. User-Equipment-Info-Type AVP

The User-Equipment-Info-Type AVP is of type Enumerated (AVP Code 459) and defines the type of user equipment information contained in the User-Equipment-Info-Value AVP.

This specification defines the following user equipment types. However, new User-Equipment-Info-Type values can be assigned by IANA as defined in Section 12.

IMEISV 0

The identifier contains the International Mobile Equipment Identifier and Software Version (IMEISV) in the IMEISV format according to 3GPP TS 23.003 [TGPPIMEI].

MAC 1

The 48-bit Media Access Control (MAC) address is formatted as described in Section 3.21 of [RFC3580].

EUI64 2

The 64-bit identifier used to identify the hardware instance of the product, as defined in [EUI64].

MODIFIED_EUI64 3

There are a number of types of terminals that have identifiers other than the International Mobile Equipment Identifier (IMEI), IEEE 802 MACs, or EUI-64. These identifiers can be converted to modified EUI-64 format as described in [RFC4291] or by using some other methods referred to in the service-specific documentation.

8.51. User-Equipment-Info-Value AVP

The User-Equipment-Info-Value AVP (AVP Code 460) is of type OctetString. The User-Equipment-Info-Type AVP defines which type of identifier is used.

8.52. User-Equipment-Info-Extension AVP

The User-Equipment-Info-Extension AVP (AVP Code 653) is of type Grouped and allows the credit-control client to indicate the identity and capability of the terminal the subscriber is using for the connection to the network. If the type of the equipment is one of the enumerated User-Equipment-Info-Type AVP values, then the credit-control client SHOULD send the information in the User-Equipment-Info AVP, in addition to or instead of the User-Equipment-Info-Extension AVP. This is done in order to preserve backward compatibility with credit-control servers that support only [RFC4006]. Exactly one AVP MUST be included inside the User-Equipment-Info-Extension AVP.

The User-Equipment-Info-Extension AVP is defined as follows (per grouped-avp-def as defined in [RFC6733]):

```
 User-Equipment-Info-Extension ::= < AVP Header: 653 >
                                 [ User-Equipment-Info-IMEISV ]
                                 [ User-Equipment-Info-MAC ]
                                 [ User-Equipment-Info-EUI64 ]
                                 [ User-Equipment-Info-ModifiedEUI64 ]
                                 [ User-Equipment-Info-IMEI ]
                                 [ AVP ]
```

8.53. User-Equipment-Info-IMEISV AVP

The User-Equipment-Info-IMEISV AVP (AVP Code 654) is of type OctetString. The User-Equipment-Info-IMEISV AVP contains the International Mobile Equipment Identifier and Software Version in the IMEISV format according to 3GPP TS 23.003 [TGPPIMEI].

8.54. User-Equipment-Info-MAC AVP

The User-Equipment-Info-MAC AVP (AVP Code 655) is of type OctetString. The User-Equipment-Info-MAC AVP contains the 48-bit MAC address; the MAC address is formatted as described in Section 4.1.7.8 of [RFC5777].

8.55. User-Equipment-Info-EUI64 AVP

The User-Equipment-Info-EUI64 AVP (AVP Code 656) is of type OctetString. The User-Equipment-Info-EUI64 AVP contains the 64-bit identifier used to identify the hardware instance of the product, as defined in [EUI64].

8.56. User-Equipment-Info-ModifiedEUI64 AVP

The User-Equipment-Info-ModifiedEUI64 AVP (AVP Code 657) is of type OctetString. There are a number of types of terminals that have identifiers other than IMEI, IEEE 802 MACs, or EUI-64. These identifiers can be converted to modified EUI-64 format as described in [RFC4291] or by using some other methods referred to in the service-specific documentation. The User-Equipment-Info-ModifiedEUI64 AVP contains such identifiers.

8.57. User-Equipment-Info-IMEI AVP

The User-Equipment-Info-IMEI AVP (AVP Code 658) is of type OctetString. The User-Equipment-Info-IMEI AVP contains the International Mobile Equipment Identifier in the IMEI format according to 3GPP TS 23.003 [TGPPIMEI].

8.58. Subscription-Id-Extension AVP

The Subscription-Id-Extension AVP (AVP Code 659) is used to identify the end user's subscription and is of type Grouped. The Subscription-Id-Extension group AVP MUST include an AVP holding the subscription identifier. The type of this included AVP indicates the type of the subscription identifier. For each of the enumerated values of the Subscription-Id-Type AVP, there is a corresponding sub-AVP for use within the Subscription-Id-Extension group AVP. If a new identifier type is required, a corresponding new sub-AVP SHOULD be defined for use within the Subscription-Id-Extension group AVP.

If full backward compatibility with [RFC4006] is required, then the Subscription-Id AVP MUST be used to indicate identifier types enumerated in the Subscription-Id-Type AVP, whereas the Subscription-Id-Extension AVP MUST be used only for newly defined identifier types. If full backward compatibility with [RFC4006] is not required, then the Subscription-Id-Extension AVP MAY be used to carry the existing identifier types. In this case, the Subscription-Id-Extension AVP MAY be sent together with the Subscription-Id AVP.

Exactly one sub-AVP MUST be included inside the Subscription-Id-Extension AVP.

The Subscription-Id-Extension AVP is defined as follows (per grouped-avp-def as defined in [RFC6733]):

```
Subscription-Id-Extension ::= < AVP Header: 659 >
                              [ Subscription-Id-E164 ]
                              [ Subscription-Id-IMSI ]
                              [ Subscription-Id-SIP-URI ]
                              [ Subscription-Id-NAI ]
                              [ Subscription-Id-Private ]
                              [ AVP ]
```

8.59. Subscription-Id-E164 AVP

The Subscription-Id-E164 AVP (AVP Code 660) is of type UTF8String. The Subscription-Id-E164 AVP contains the international E.164 format (e.g., MSISDN), according to the ITU-T E.164 numbering plan defined in [E164] and [CE164].

8.60. Subscription-Id-IMSI AVP

The Subscription-Id-IMSI AVP (AVP Code 661) is of type UTF8String. The Subscription-Id-IMSI AVP contains the IMSI format, according to the ITU-T E.212 identification plan as defined in [E212] and [CE212].

8.61. Subscription-Id-SIP-URI AVP

The Subscription-Id-SIP-URI AVP (AVP Code 662) is of type UTF8String. The Subscription-Id-SIP-URI AVP contains the identifier in the form of a SIP URI, as defined in [RFC3261].

8.62. Subscription-Id-NAI AVP

The Subscription-Id-NAI AVP (AVP Code 663) is of type UTF8String. The Subscription-Id-NAI AVP contains the identifier in the form of a Network Access Identifier, as defined in [RFC7542].

8.63. Subscription-Id-Private AVP

The Subscription-Id-Private AVP (AVP Code 664) is of type UTF8String. The Subscription-Id-Private AVP contains a credit-control server private identifier.

8.64. Redirect-Server-Extension AVP

The Redirect-Server-Extension AVP (AVP Code 665) is of type Grouped and contains the address information of the redirect server (e.g., HTTP redirect server, SIP Server) with which the end user is to be connected when the account cannot cover the service cost. It MUST be present inside the QoS-Final-Unit-Indication AVP when the Final-Unit-Action AVP is set to REDIRECT. If the type of the redirect server is one of the enumerated values of the Redirect-Address-Type AVP, then the credit-control server SHOULD send the information in the Redirect-Server AVP, in addition to or instead of the Redirect-Server-Extension AVP. This is done in order to preserve backward compatibility with credit-control clients that support only [RFC4006]. Exactly one AVP MUST be included inside the Redirect-Server-Extension AVP.

The Redirect-Server-Extension AVP is defined as follows (per grouped-avp-def as defined in [RFC6733]):

```
Redirect-Server-Extension ::= < AVP Header: 665 >
                              [ Redirect-Address-IPAddress ]
                              [ Redirect-Address-URL ]
                              [ Redirect-Address-SIP-URI ]
                              [ AVP ]
```

8.65. Redirect-Address-IPAddress AVP

The Redirect-Address-IPAddress AVP (AVP Code 666) is of type Address and defines the IPv4 or IPv6 address of the redirect server with which the end user is to be connected when the account cannot cover the service cost.

When encoded as an IPv6 address in 16 bytes, the IPv4-mapped IPv6 format [RFC4291] MAY be used to indicate an IPv4 address.

The interpretation of Redirect-Address-IPAddress by the Diameter Credit-Control client is a matter of local policy.

8.66. Redirect-Address-URL AVP

The Redirect-Address-URL AVP (AVP Code 667) is of type UTF8String and defines the address of the redirect server with which the end user is to be connected when the account cannot cover the service cost. The address type is in the form of a Uniform Resource Locator, as defined in [RFC3986]. Note that individual URL schemes may restrict the contents of the UTF8String.

8.67. Redirect-Address-SIP-URI AVP

The Redirect-Address-SIP-URI AVP (AVP Code 668) is of type UTF8String and defines the address of the redirect server with which the end user is to be connected when the account cannot cover the service cost. The address type is in the form of a SIP Uniform Resource Identifier, as defined in [RFC3261].

8.68. QoS-Final-Unit-Indication AVP

The QoS-Final-Unit-Indication AVP (AVP Code 669) is of type Grouped and indicates that the Granted-Service-Unit AVP in the Credit-Control-Answer or in the AA-Answer contains the final units for the service. After these units have expired, the Diameter Credit-Control client is responsible for executing the action indicated in the Final-Unit-Action AVP (see Section 5.6).

If more than one unit type is received in the Credit-Control-Answer, the unit type that first expired SHOULD cause the credit-control client to execute the specified action.

In the first interrogation, the QoS-Final-Unit-Indication AVP with Final-Unit-Action set to REDIRECT or RESTRICT_ACCESS can also be present with no Granted-Service-Unit AVP in the Credit-Control-Answer or in the AA-Answer. This indicates to the Diameter Credit-Control client that the client is to execute the specified action

immediately. If the home service provider policy is to terminate the service, naturally, the server SHOULD return the appropriate transient failure (see Section 9.1) in order to implement the policy-defined action.

The Final-Unit-Action AVP defines the behavior of the Service Element when the user's account cannot cover the cost of the service and MUST always be present if the QoS-Final-Unit-Indication AVP is included in a command.

If the Final-Unit-Action AVP is set to TERMINATE, the QoS-Final-Unit-Indication group AVP MUST NOT contain any other AVPs.

If the Final-Unit-Action AVP is set to REDIRECT, then the Redirect-Server-Extension AVP MUST be present. The Filter-Rule AVP or the Filter-Id AVP MAY be present in the Credit-Control-Answer message if the user is also allowed to access other services that are not accessible through the address given in the Redirect-Server-Extension AVP or if access to these services needs to be limited in some way (e.g., QoS).

If the Final-Unit-Action AVP is set to RESTRICT_ACCESS, either the Filter-Rule AVP or the Filter-Id AVP SHOULD be present.

The Filter-Rule AVP is defined in [RFC5777]. The Filter-Rule AVP can be used to define a specific combination of a condition and an action. If used only with traffic conditions, it should define which traffic should be allowed when no more service units are granted. However, if QoS or treatment information exists in the AVP, these actions should be executed, e.g., limiting the allowed traffic with certain QoS information. When multiple Filter-Rule AVPs exist, precedence should be determined as defined in [RFC5777].

The Filter-Id AVP is defined in [RFC7155]. The Filter-Id AVP can be used to reference an IP filter list installed in the access device by means other than the Diameter Credit-Control application, e.g., locally configured or configured by another entity.

If the Final-Unit-Action AVP is (1) set to TERMINATE, (2) set to RESTRICT_ACCESS and the action required is to allow only traffic that could be classified using an IPFilterRule, or (3) set to REDIRECT using a type that is one of the types in the Redirect-Address-Type AVP, then the credit-control server SHOULD send the information in the Final-Unit-Indication AVP, in addition to or instead of the QoS-Final-Unit-Indication AVP. This is done in order to preserve backward compatibility with credit-control clients that support only [RFC4006].

The QoS-Final-Unit-Indication AVP is defined as follows (per grouped-avp-def as defined in [RFC6733]):

```
      QoS-Final-Unit-Indication ::= < AVP Header: 669 >
                                    { Final-Unit-Action }
                                   *[ Filter-Rule ]
                                   *[ Filter-Id ]
                                    [ Redirect-Server-Extension ]
                                   *[ AVP ]
```

9. Result-Code AVP Values

This section defines new Result-Code AVP [RFC6733] values that must be supported by all Diameter implementations that conform to this specification.

The Credit-Control-Answer message includes the Result-Code AVP, which may indicate that an error was present in the Credit-Control-Request message. A rejected Credit-Control-Request message SHOULD cause the user's session to be terminated.

9.1. Transient Failures

Errors that fall within the category of transient failures are used to inform the peer that the request could not be satisfied at the time it was received but that the request MAY be able to be satisfied in the future.

DIAMETER_END_USER_SERVICE_DENIED 4010

The credit-control server denies the service request due to service restrictions. If the CCR contained used service units, they are deducted, if possible.

DIAMETER_CREDIT_CONTROL_NOT_APPLICABLE 4011

The credit-control server determines that the service can be granted to the end user but that no further credit-control is needed for the service (e.g., the service is free of charge).

DIAMETER_CREDIT_LIMIT_REACHED 4012

The credit-control server denies the service request because the end user's account could not cover the requested service. If the CCR contained used service units, they are deducted, if possible.

9.2. Permanent Failures

Errors that fall within the category of permanent failures are used to inform the peer that the request failed and should not be attempted again.

DIAMETER_USER_UNKNOWN 5030

The specified end user is unknown in the credit-control server.

DIAMETER_RATING_FAILED 5031

This error code is used to inform the credit-control client that the credit-control server cannot rate the service request due to insufficient rating input, an incorrect AVP combination, or an AVP or AVP value that is not recognized or supported in the rating. The Failed-AVP AVP MUST be included and contain (1) a copy of the entire AVP or AVPs that could not be processed successfully or (2) an example of the missing AVP, complete with the Vendor-Id if applicable. The value field of the missing AVP should be of correct minimum length and contain zeros.

10. AVP Occurrence Table

The table in Section 10.1 presents the AVPs defined in this document and specifies in which Diameter messages they MAY or MUST NOT be present. Note that AVPs that can only be present within a Grouped AVP are not represented in the table.

The table uses the following symbols:

0	The AVP MUST NOT be present in the message.
0+	Zero or more instances of the AVP MAY be present in the message.
0-1	Zero or one instance of the AVP MAY be present in the message. It is considered an error if there is more than one instance of the AVP.
1	One instance of the AVP MUST be present in the message.

10.1. Credit-Control AVP Table

The table in this section is used to represent which credit-control application-specific AVPs defined in this document are to be present in the credit-control messages.

Attribute Name	Command Code	
	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
QoS-Final-Unit-Indication	0	0-1
Granted-Service-Unit	0	0-1
Multiple-Services-Credit-Control	0+	0+
Multiple-Services-Indicator	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

Subscription-Id-Extension	0+	0
Termination-Cause	0-1	0
User-Equipment-Info	0-1	0
User-Equipment-Info-Extension	0-1	0
Used-Service-Unit	0+	0
User-Name	0-1	0-1
Validity-Time	0	0-1

10.2. Re-Auth-Request/Re-Auth-Answer AVP Table

This section defines AVPs that are specific to the Diameter Credit-Control application and that MAY be included in the Diameter Re-Auth-Request/Re-Auth-Answer (RAR/RAA) message [RFC6733].

The RAR/RAA command MAY include the following additional AVPs:

	Command Code	
Attribute Name	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. RADIUS/Diameter Credit-Control Interworking Model

This section defines the basic principles for the Diameter Credit-Control / RADIUS prepaid interworking model -- that is, a message translation between a RADIUS-based prepaid solution and a Diameter Credit-Control application. A complete description of the protocol translations between RADIUS and the Diameter Credit-Control application is beyond the scope of this specification and SHOULD be addressed in another appropriate document.

The Diameter Credit-Control architecture may have a Translation Agent capable of translation between RADIUS prepaid and Diameter Credit-Control protocols. A AAA server (usually the home AAA server) may act as a Translation Agent and as a Diameter Credit-Control client for Service Elements that use credit-control mechanisms other than Diameter Credit-Control -- for instance, RADIUS prepaid. In this case, the home AAA server contacts the Diameter Credit-Control server as part of the authorization process. The interworking architecture is illustrated in Figure 9, and an interworking flow is illustrated in Figure 10. In a roaming situation, the Service

Element (e.g., the NAS) may be located in the visited network, and a visited AAA server is usually contacted. The visited AAA server then connects to the home AAA server.

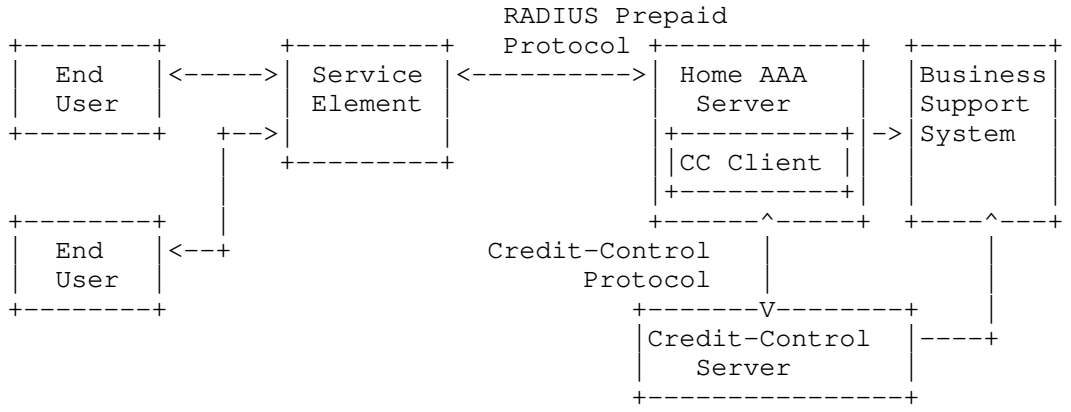


Figure 9: Credit-Control Architecture with Service Element Containing Translation Agent, Translating RADIUS Prepaid to Diameter Credit-Control Protocol

When the AAA server acting as a Translation Agent receives an initial RADIUS Access-Request message from a Service Element (e.g., NAS access), it performs regular authentication and authorization. If the RADIUS Access-Request message indicates that the Service Element is capable of credit-control and if the home AAA server finds that the subscriber is a prepaid subscriber, then a Diameter Credit-Control-Request SHOULD be sent toward the credit-control server to perform credit authorization and to establish a credit-control session. After the Diameter Credit-Control server checks the end user's account balance, rates the service, and reserves credit from the end user's account, the reserved quota is returned to the home AAA server in the Diameter Credit-Control-Answer. The home AAA server then sends the reserved quota to the Service Element in the RADIUS Access-Accept.

At the expiry of the allocated quota, the Service Element sends a new RADIUS Access-Request containing the units used thus far to the home AAA server. The home AAA server shall map a RADIUS Access-Request containing the reported units to the Diameter Credit-Control server in a Diameter Credit-Control-Request (UPDATE_REQUEST). The Diameter Credit-Control server debits the used units from the end user's account and allocates a new quota that is returned to the home AAA server in the Diameter Credit-Control-Answer. The quota is transferred to the Service Element in the RADIUS Access-Accept. When the end user terminates the service or when the entire quota has been

used, the Service Element sends a RADIUS Access-Request. To debit the used units from the end user's account and to stop the credit-control session, the home AAA server sends a Diameter Credit-Control-Request (TERMINATION_REQUEST) to the credit-control server. The Diameter Credit-Control server acknowledges the session termination by sending a Diameter Credit-Control-Answer to the home AAA server. The RADIUS Access-Accept is sent to the NAS.

Figure 10 illustrates a Diameter Credit-Control / RADIUS prepaid interworking sequence.

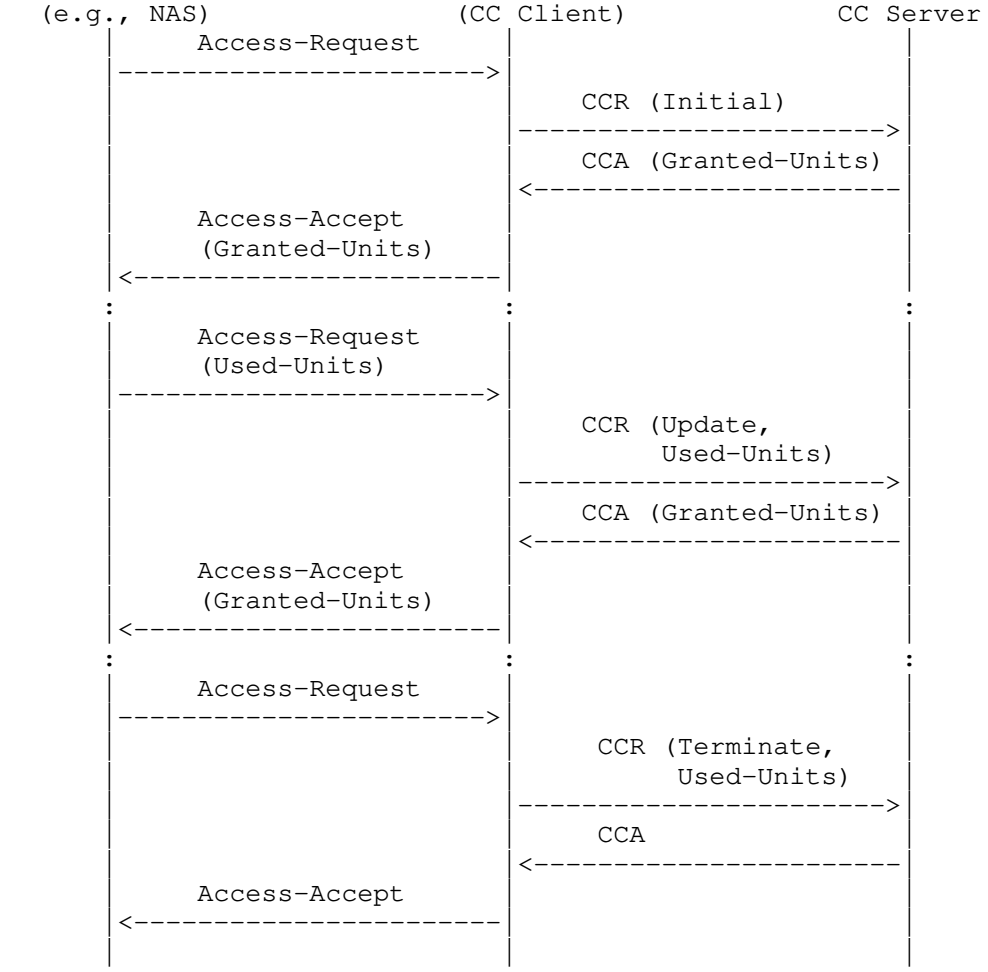


Figure 10: Message Flow Example with Diameter Credit-Control / RADIUS Prepaid Interworking

12. IANA Considerations

This document uses several registries that were originally created in [RFC4006] or the values assigned to existing namespaces managed by IANA. IANA has updated these registries to reference this document. The registries and their allocation policies are specified below.

12.1. Application Identifier

This specification assigns the value 4, "Diameter Credit Control", to the "Application IDs" namespace defined in [RFC6733]. See Section 1.3 for more information.

12.2. Command Codes

This specification uses the value 272 from the "Command Codes" namespace defined in [RFC6733] for the Credit-Control-Request (CCR) and Credit-Control-Answer (CCA) commands.

12.3. AVP Codes

See Section 8 for the assignments in this specification.

This document describes new AVP codes beyond those described in [RFC4006]. IANA has allocated codes for the AVPs listed in Table 7.

Attribute Name	Code	Defined in
User-Equipment-Info-Extension	653	Section 8.52
User-Equipment-Info-IMEISV	654	Section 8.53
User-Equipment-Info-MAC	655	Section 8.54
User-Equipment-Info-EUI64	656	Section 8.55
User-Equipment-Info-ModifiedEUI64	657	Section 8.56
User-Equipment-Info-IMEI	658	Section 8.57
Subscription-Id-Extension	659	Section 8.58
Subscription-Id-E164	660	Section 8.59
Subscription-Id-IMSI	661	Section 8.60
Subscription-Id-SIP-URI	662	Section 8.61
Subscription-Id-NAI	663	Section 8.62
Subscription-Id-Private	664	Section 8.63
Redirect-Server-Extension	665	Section 8.64
Redirect-Address-IPAddress	666	Section 8.65
Redirect-Address-URL	667	Section 8.66
Redirect-Address-SIP-URI	668	Section 8.67
QoS-Final-Unit-Indication	669	Section 8.68

Table 7: Requested AVP Assignments

12.4. Result-Code AVP Values

This specification assigns the values 4010, 4011, and 4012 in the "Result-Code AVP Values (code 268) - Transient Failures" namespace and values 5030 and 5031 in the "Result-Code AVP Values (code 268) - Permanent Failure" namespace, both of which were defined by [RFC6733]. See Section 9 for the assignments in this specification.

12.5. CC-Request-Type AVP

As defined in Section 8.3, the CC-Request-Type AVP includes Enumerated type values 1-4. IANA has created and is maintaining a namespace for this AVP. The definition of new values is subject to the Specification Required policy [RFC8126] and conditions for enumerated values described in [RFC7423], Section 5.6.

12.6. CC-Session-Failover AVP

As defined in Section 8.4, the CC-Session-Failover AVP includes Enumerated type values 0-1. IANA has created and is maintaining a namespace for this AVP. The definition of new values is subject to the Specification Required policy [RFC8126] and conditions for enumerated values described in [RFC7423], Section 5.6.

12.7. CC-Unit-Type AVP

As defined in Section 8.32, the CC-Unit-Type AVP includes Enumerated type values 0-5. IANA has created and is maintaining a namespace for this AVP. The definition of new values is subject to the Specification Required policy [RFC8126] and conditions for enumerated values described in [RFC7423], Section 5.6.

12.8. Check-Balance-Result AVP

As defined in Section 8.6, the Check-Balance-Result AVP includes Enumerated type values 0-1. IANA has created and is maintaining a namespace for this AVP. The definition of new values is subject to the Specification Required policy [RFC8126] and conditions for enumerated values described in [RFC7423], Section 5.6.

12.9. Credit-Control AVP

As defined in Section 8.13, the Credit-Control AVP includes Enumerated type values 0-1. IANA has created and is maintaining a namespace for this AVP. The definition of new values is subject to the Specification Required policy [RFC8126] and conditions for enumerated values described in [RFC7423], Section 5.6.

12.10. Credit-Control-Failure-Handling AVP

As defined in Section 8.14, the Credit-Control-Failure-Handling AVP includes Enumerated type values 0-2. IANA has created and is maintaining a namespace for this AVP. The definition of new values is subject to the Specification Required policy [RFC8126] and conditions for enumerated values described in [RFC7423], Section 5.6.

12.11. Direct-Debiting-Failure-Handling AVP

As defined in Section 8.15, the Direct-Debiting-Failure-Handling AVP includes Enumerated type values 0-1. IANA has created and is maintaining a namespace for this AVP. The definition of new values is subject to the Specification Required policy [RFC8126] and conditions for enumerated values described in [RFC7423], Section 5.6.

12.12. Final-Unit-Action AVP

As defined in Section 8.35, the Final-Unit-Action AVP includes Enumerated type values 0-2. IANA has created and is maintaining a namespace for this AVP. The definition of new values is subject to the Specification Required policy [RFC8126] and conditions for enumerated values described in [RFC7423], Section 5.6.

12.13. Multiple-Services-Indicator AVP

As defined in Section 8.40, the Multiple-Services-Indicator AVP includes Enumerated type values 0-1. IANA has created and is maintaining a namespace for this AVP. The definition of new values is subject to the Specification Required policy [RFC8126] and conditions for enumerated values described in [RFC7423], Section 5.6.

12.14. Redirect-Address-Type AVP

As defined in Section 8.38, the Redirect-Address-Type AVP includes Enumerated type values 0-3. IANA has created and is maintaining a namespace for this AVP. The definition of new values is subject to the Specification Required policy [RFC8126] and conditions for enumerated values described in [RFC7423], Section 5.6.

12.15. Requested-Action AVP

As defined in Section 8.41, the Requested-Action AVP includes Enumerated type values 0-3. IANA has created and is maintaining a namespace for this AVP. The definition of new values is subject to the Specification Required policy [RFC8126] and conditions for enumerated values described in [RFC7423], Section 5.6.

12.16. Subscription-Id-Type AVP

As defined in Section 8.47, the Subscription-Id-Type AVP includes Enumerated type values 0-4. IANA has created and is maintaining a namespace for this AVP. The definition of new values is subject to the Specification Required policy [RFC8126] and conditions for enumerated values described in [RFC7423], Section 5.6.

12.17. Tariff-Change-Usage AVP

As defined in Section 8.27, the Tariff-Change-Usage AVP includes Enumerated type values 0-2. IANA has created and is maintaining a namespace for this AVP. The definition of new values is subject to the Specification Required policy [RFC8126] and conditions for enumerated values described in [RFC7423], Section 5.6.

12.18. User-Equipment-Info-Type AVP

As defined in Section 8.50, the User-Equipment-Info-Type AVP includes Enumerated type values 0-3. IANA has created and is maintaining a namespace for this AVP. The definition of new values is subject to the Specification Required policy [RFC8126] and conditions for enumerated values described in [RFC7423], Section 5.6.

13. Parameters Related to the Credit-Control Application

Tx timer

When real-time credit-control is required, the credit-control client contacts the credit-control server before and while the service is provided to an end user. Due to the real-time nature of the application, communication delays SHOULD be minimized, e.g., to avoid an overly long service setup time experienced by the end user. The Tx timer is introduced to control the waiting time in the client in the Pending state. When the Tx timer elapses, the credit-control client takes action for the end user according to the value of the CCFH or the DDFH. The recommended value is 10 seconds.

Tcc timer

The Tcc timer supervises an ongoing credit-control session in the credit-control server. It is RECOMMENDED to use the Validity-Time as input to set the Tcc timer value. In the case of transient failures in the network, the Diameter Credit-Control server might change to Idle state. To avoid this, the Tcc timer MAY be set so that Tcc is equal to 2 x Validity-Time.

Credit-Control-Failure-Handling and Direct-Debiting-Failure-Handling

Client implementations may offer the possibility of locally configuring these AVPs. In such a case, their values and behavior are defined in Sections 5.7 and 6.5, respectively.

14. Security Considerations

Security considerations regarding the Diameter protocol itself are discussed in [RFC6733]. The use of this application of Diameter MUST take into consideration the security issues and requirements of the base protocol.

This application includes a mechanism for application-layer replay protection by means of (1) the Session-Id AVP as specified in [RFC6733] and (2) the CC-Request-Number AVP, which is specified in this document. The Diameter Credit-Control application is often used within one domain, and there may be a single hop between the peers. In these environments, the use of TLS/TCP, DTLS/SCTP (Datagram Transport Layer Security / Stream Control Transmission Protocol), or IPsec is sufficient. The details of security considerations related to TLS/TCP, DTLS/SCTP, and IPsec are discussed in [RFC6733].

Because this application handles monetary transactions (directly or indirectly), it increases interest in various security attacks. Therefore, all parties communicating with each other MUST be authenticated, including, for instance, TLS client-side authentication. In addition, authorization of the client SHOULD be emphasized, i.e., that the client is allowed to perform credit-control for a certain user. The specific means of authorization are outside the scope of this specification but can be, for instance, manual configuration.

Another kind of threat is malicious modification, injection, or deletion of AVPs or complete credit-control messages. The credit-control messages contain sensitive billing-related information (such as subscription identifiers, granted units, used units, or cost information) whose malicious modification can have financial consequences. Sometimes simply delaying the credit-control messages can cause disturbances in the credit-control client or server.

Even without any modifications to the messages, an adversary that can eavesdrop on transactions can obtain privacy-sensitive information. Also, by monitoring the credit-control messages, one can collect information about the credit-control server's billing models and business relationships.

When third-party relays or proxies are involved, hop-by-hop security does not necessarily provide sufficient protection for Diameter user sessions. In some cases, it may be inappropriate to send Diameter messages, such as CCR messages and CCA messages, containing sensitive AVPs via untrusted Diameter proxy agents, as there are no assurances that third-party proxies will not modify the credit-control commands or AVP values.

14.1. Direct Connection with Redirects

A Diameter Credit-Control agent cannot always know whether agents between it and the end user's Diameter Credit-Control server are reliable. In this case, the Diameter Credit-Control agent doesn't have a routing entry in its Diameter routing table (defined in [RFC6733], Section 2.7) for the realm of the credit-control server in the end user's home realm. The Diameter Credit-Control agent can have a default route configured to a local redirect agent, and it redirects the CCR message to the redirect agent. The local redirect agent then returns a redirect notification (Result-Code 3006, DIAMETER_REDIRECT_INDICATION) to the credit-control agent, as well as information about the Diameter Credit-Control server(s) (Redirect-Host AVP) and information about how the routing entry resulting from the Redirect-Host is to be used (Redirect-Host-Usage AVP). The Diameter Credit-Control agent then forwards the CCR message directly

to one of the hosts identified by the CCA message from the redirect agent. If the value of the Redirect-Host-Usage AVP does not equal zero, all subsequent messages are sent to the host specified in the Redirect-Host AVP until the time specified by the Redirect-Max-Cache-Time AVP has expired.

Even with redirects, there are some authorization issues. There may be attacks toward nodes that have been properly authorized but that abuse their authorization or have been compromised. These issues are discussed more widely in [RFC4072], Section 8.

14.2. Application-Level Redirects

This document includes a redirection feature (Section 5.6.2) whereby the service provider can redirect (in an application-specific way) the end user to an alternate location when their credits have expired. This technique is useful in that it allows the user to return to normal service quickly, but it also exposes additional risks and attack surface. In particular, this redirection can potentially occur at an arbitrary point in a user's session, potentially without any additional contextual confirmation available to the user that the redirection is driven by the network. This lack of confirmation matters because, in many application protocols, the communication peer is also capable of inducing redirection. When the peer is an attacker, the redirection can be to an attacker-controlled site. In particular, such sites may be "phishing" sites designed to appear similar to legitimate payment sites in an attempt to obtain users' payment information for fraudulent purposes. When users become accustomed to such redirections, they may have difficulty distinguishing such attacks from legitimate redirections.

Because of the potentially harmful consequences of arbitrary redirection by an attacker (such as to phishing sites), it is important for service providers to be aware of that risk and ensure that their users are aware of it as well. Service providers should follow industry best practices for the specific application-layer protocol to reduce the chances that such attacks could be mistaken for legitimate redirections. The details of such a practice are out of scope for this document.

15. Privacy Considerations

As the Diameter protocol, and especially the credit-control application, deal with subscribers and their actions, extra care should be taken regarding the privacy of the subscribers. Per terminology used in [RFC6973], both the credit-control client and the credit-control server are intermediary entities, wherein the subscribers' privacy may be compromised even if no security issues exist, and only authorized entities have access to the privacy-sensitive information.

15.1. Privacy-Sensitive AVPs

The privacy-sensitive AVPs listed in this section MUST NOT be sent across non-trusted networks or Diameter agents without end-to-end authentication and confidentiality protection, as described in [RFC6733], Section 13.3.

The following AVPs contain privacy-sensitive information at different levels:

1. CC-Correlation-Id AVP: may contain privacy-sensitive information, as the service provider may encode personal information that helps it correlate different subscriptions and access technologies.

2. Check-Balance-Result AVP: contains information on the balance status of the subscriber.

3. Currency-Code AVP: contains information on the subscriber's locale.

4. Cost-Unit AVP: contains privacy-sensitive information for the Cost-Information AVP, in human-readable format.

5. Service-Identifier AVP: may contain privacy-sensitive information about the subscriber's Internet activity.

6. Rating-Group AVP: may contain privacy-sensitive information about the subscriber's Internet activity.

7. Restriction-Filter-Rule AVP: the information inside IPFilterRule may be used to infer services used by the subscriber.

8. Redirect-Server-Address AVP: the service provider might embed personal information on the subscriber in the URL/URI (e.g., to create a personalized message). However, the service provider may instead anonymize the subscriber's identity in the URL/URI and let the redirect server query the information directly. Such anonymized information must not allow personal information or the subscriber's identity to be easily guessed. Furthermore, the service provider should treat the URL/URI schema itself as confidential and make sure it cannot be inferred (1) from observation of the traffic or (2) due to its trivial structure. A trivial structure could allow an adversary to query/modify personal information even without knowing the subscriber's identity. Similar AVPs are Redirect-Address-URL and Redirect-Address-SIP-URI.

9. Service-Context-Id AVP: depending on how the service provider uses it, it may contain privacy-sensitive information about the service (e.g., in a 3GPP network Service-Context-Id AVP, it has a different value for packet switching, SMS, Multimedia Messages (MMSs), etc.).

10. Service-Parameter-Info AVP: depending on how the service provider uses it, it may contain privacy-sensitive information about the subscriber (e.g., location).

11. Subscription-Id-Data AVP: contains the identity of the subscriber. Similar AVPs are Subscription-Id-E164, Subscription-Id-IMSI, Subscription-Id-SIP-URI, Subscription-Id-NAI, and Subscription-Id-Private.

12. User-Equipment-Info-Value AVP: contains the identity of the device of the subscriber. Similar AVPs are User-Equipment-Info-IMEISV, User-Equipment-Info-MAC, User-Equipment-Info-EUI64, User-Equipment-Info-ModifiedEUI64, and User-Equipment-Info-IMEI.

13. QoS-Final-Unit-Indication AVP: Grouped AVP that may contain privacy-sensitive information in its sub-AVPs (e.g., IPFilterRule, redirect address).

Note that some AVPs that are used in this document are defined in [RFC6733] and may contain privacy-sensitive information. These AVPs are not listed above.

15.2. Data Minimization

Due to the nature of the credit-control application, some personal data and identity information must be stored in both the credit-control client and the credit-control server. However, this could be minimized by following these guidelines:

1. Data stored in the credit-control client does not need to persist across sessions. All data could be deleted once the session ends and could be reconstructed once a new session is initialized. Note that while the credit-control server is usually owned by the service provider with which the subscriber already has some direct legal or business relationship (where the privacy level could be agreed upon), this is not always true for a credit-control client that may be owned by a third party.

2. Some information about the subscriber has to be stored in persistent storage in the credit-control server (e.g., identity, balance); however, per-transaction information does not have to be stored in persistent storage, and per-session information may be deleted from persistent storage once the session ends.

3. In some cases, per-transaction information has to be stored on the credit-control server, client, or both, for regulatory, auditability, or debugging reasons. However, this could be minimized by following these guidelines:

   A. Data retention does not need to exceed the required duration.

   B. Transaction information could be aggregated in some cases (e.g., prefer information per session over information per rating-group; prefer hourly byte summary over per-transaction byte counts).

   C. If not strictly needed, information that is more sensitive (e.g., location, equipment type) could be filtered out of such logs. This information is often used to make rating decisions, and in this case, the rating decisions should be logged instead of the data used to make them.

   D. Due to the reasons explained in the first guideline, the credit-control server, rather than the credit-control client, would be the preferred location for storing such transaction information.

15.3. Diameter Agents

Diameter agents, as described in [RFC6733], may be owned by third parties. If end-to-end security is supported between the credit-control client and the credit-control server, the operator can use it to encrypt privacy-sensitive AVPs (as listed in Section 15.1) and prevent such information from leaking into the agent.

In some cases, the Diameter agent needs access to privacy-sensitive AVPs, in order to make correct routing decisions or even to modify the content of these AVPs. For example, a proxy agent may need to look at the Subscription-Id-IMSI AVP, in order to extract the mobile country and network codes of the user and use them to look up the destination to which the request should be routed (see Section 2.8.2 in [RFC6733]). In such a case, the credit-control client and credit-control server may use a mechanism that anonymizes the identity of the subscriber, as well as a mechanism to encrypt other AVPs not used by the agent.

16. References

16.1. Normative References

[CE164] International Telecommunication Union, "COMPLEMENT TO ITU-T RECOMMENDATION E.164 (11/2010): LIST OF ITU-T RECOMMENDATION E.164 ASSIGNED COUNTRY CODES", November 2011, <https://www.itu.int/dms_pub/itu-t/opb/sp/T-SP-E.164D-11-2011-PDF-E.pdf>.

[CE212] International Telecommunication Union, "COMPLEMENT TO RECOMMENDATION ITU-T E.212 (09/2016): LIST OF MOBILE COUNTRY OR GEOGRAPHICAL AREA CODES", February 2017, <https://www.itu.int/dms_pub/itu-t/opb/sp/T-SP-E.212A-2017-PDF-E.pdf>.

[E164] International Telecommunication Union, "The international public telecommunication numbering plan", ITU-T Recommendation E.164, November 2010, <https://www.itu.int/rec/T-REC-E.164/>.

[E212] International Telecommunication Union, "The international identification plan for public networks and subscriptions", ITU-T Recommendation E.212, September 2016, <https://www.itu.int/rec/T-REC-E.212/en>.

[EUI64] IEEE, "Guidelines for Use of Extended Unique Identifier (EUI), Organizationally Unique Identifier (OUI), and Company ID (CID)", August 2017, <https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/tutorials/eui.pdf>.

[ISO4217] ISO, "Codes for the representation of currencies", ISO 4217:2015, 2015, <https://www.iso.org/iso-4217-currency-codes.html>.

[RFC791] Postel, J., "Internet Protocol", STD 5, RFC 791, DOI 10.17487/RFC0791, September 1981, <https://www.rfc-editor.org/info/rfc791>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, DOI 10.17487/RFC3261, June 2002, <https://www.rfc-editor.org/info/rfc3261>.

[RFC3539] Aboba, B. and J. Wood, "Authentication, Authorization and Accounting (AAA) Transport Profile", RFC 3539, DOI 10.17487/RFC3539, June 2003, <https://www.rfc-editor.org/info/rfc3539>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <https://www.rfc-editor.org/info/rfc3986>.

[RFC4006] Hakala, H., Mattila, L., Koskinen, J-P., Stura, M., and J. Loughney, "Diameter Credit-Control Application", RFC 4006, DOI 10.17487/RFC4006, August 2005, <https://www.rfc-editor.org/info/rfc4006>.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <https://www.rfc-editor.org/info/rfc4291>.

[RFC5777] Korhonen, J., Tschofenig, H., Arumaithurai, M., Jones, M., Ed., and A. Lior, "Traffic Classification and Quality of Service (QoS) Attributes for Diameter", RFC 5777, DOI 10.17487/RFC5777, February 2010, <https://www.rfc-editor.org/info/rfc5777>.

[RFC5952] Kawamura, S. and M. Kawashima, "A Recommendation for IPv6 Address Text Representation", RFC 5952, DOI 10.17487/RFC5952, August 2010, <https://www.rfc-editor.org/info/rfc5952>.

[RFC6733] Fajardo, V., Ed., Arkko, J., Loughney, J., and G. Zorn, Ed., "Diameter Base Protocol", RFC 6733, DOI 10.17487/RFC6733, October 2012, <https://www.rfc-editor.org/info/rfc6733>.

[RFC7155] Zorn, G., Ed., "Diameter Network Access Server Application", RFC 7155, DOI 10.17487/RFC7155, April 2014, <https://www.rfc-editor.org/info/rfc7155>.

[RFC7423] Morand, L., Ed., Fajardo, V., and H. Tschofenig, "Diameter Applications Design Guidelines", BCP 193, RFC 7423, DOI 10.17487/RFC7423, November 2014, <https://www.rfc-editor.org/info/rfc7423>.

[RFC7542] DeKok, A., "The Network Access Identifier", RFC 7542, DOI 10.17487/RFC7542, May 2015, <https://www.rfc-editor.org/info/rfc7542>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[TGPPIMEI] 3rd Generation Partnership Project, Technical Specification Group Core Network, "Numbering, addressing and identification (release 15)", 3GPP TS 23.003 version 15.6.0, December 2018.

16.2. Informative References

[RFC2866] Rigney, C., "RADIUS Accounting", RFC 2866, DOI 10.17487/RFC2866, June 2000, <https://www.rfc-editor.org/info/rfc2866>.

[RFC3580] Congdon, P., Aboba, B., Smith, A., Zorn, G., and J. Roese, "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines", RFC 3580, DOI 10.17487/RFC3580, September 2003, <https://www.rfc-editor.org/info/rfc3580>.

[RFC3725] Rosenberg, J., Peterson, J., Schulzrinne, H., and G. Camarillo, "Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)", BCP 85, RFC 3725, DOI 10.17487/RFC3725, April 2004, <https://www.rfc-editor.org/info/rfc3725>.

[RFC4004] Calhoun, P., Johansson, T., Perkins, C., Hiller, T., Ed., and P. McCann, "Diameter Mobile IPv4 Application", RFC 4004, DOI 10.17487/RFC4004, August 2005, <https://www.rfc-editor.org/info/rfc4004>.

[RFC4072] Eronen, P., Ed., Hiller, T., and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application", RFC 4072, DOI 10.17487/RFC4072, August 2005, <https://www.rfc-editor.org/info/rfc4072>.

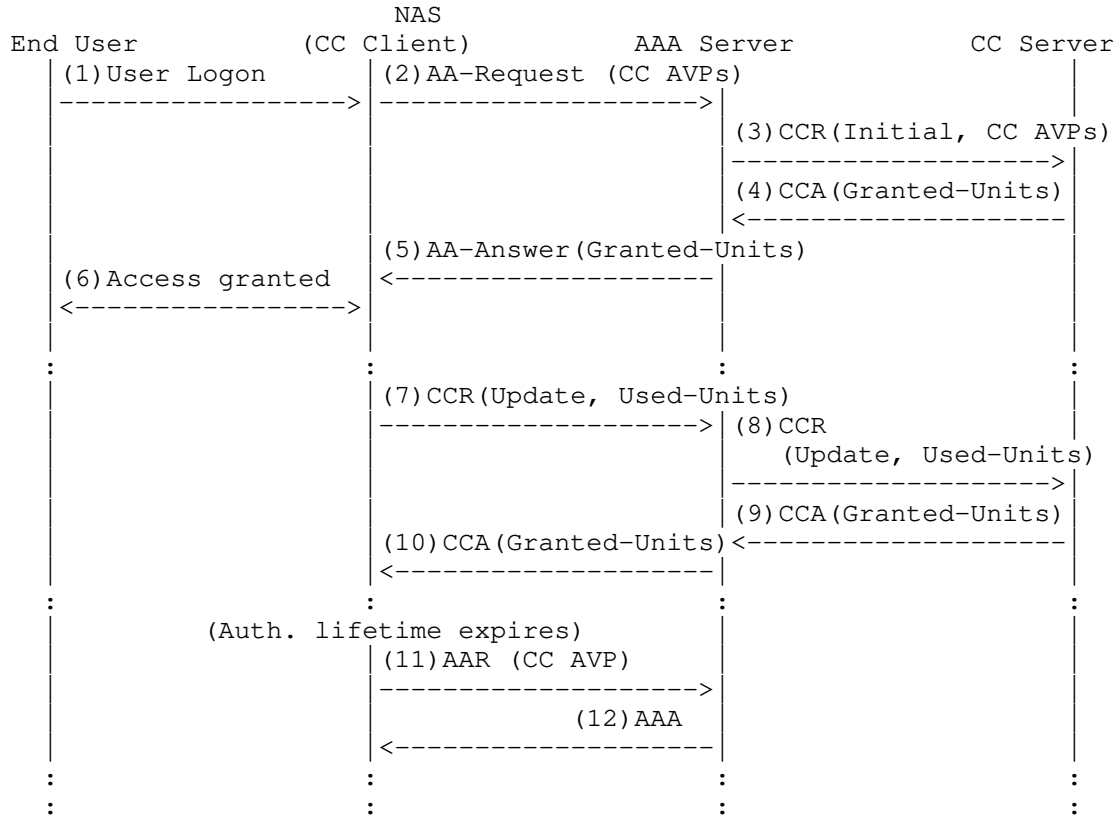
[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, DOI 10.17487/RFC6973, July 2013, <https://www.rfc-editor.org/info/rfc6973>.

[TGPPCHARG] 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, "Service aspects; Charging and Billing", 3GPP TS 22.115 version 15.5.0, September 2018.

Appendix A. Credit-Control Sequences

A.1. Flow I

A credit-control flow for Network Access Services prepaid is shown in Figure 11. The Diameter protocol application is implemented in the Network Access Server (NAS) per [RFC7155]. The focus of this flow is on credit authorization.



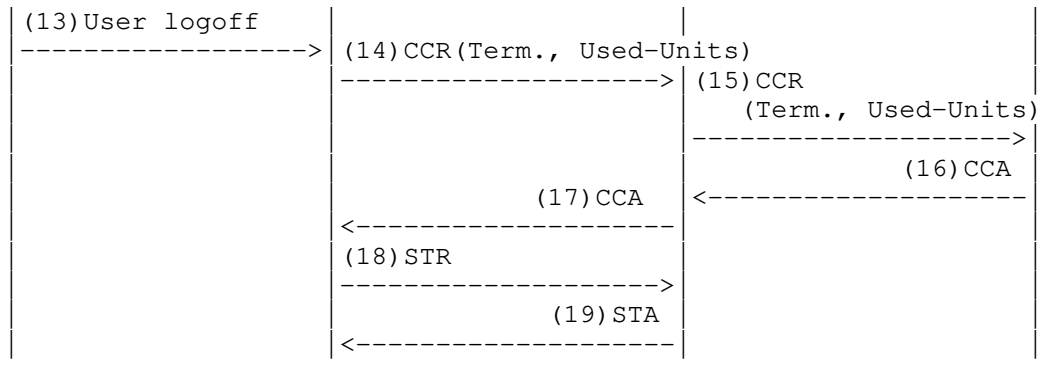


Figure 11: Flow I

The user logs on to the network (1). The Diameter NAS sends a Diameter AA-Request (AAR) to the home Diameter AAA server (2). The credit-control client populates the AAR with the Credit-Control AVP set to CREDIT_AUTHORIZATION, and service-specific AVPs are included, as usual [RFC7155]. The home Diameter AAA server performs service-specific authentication and authorization, as usual. The home Diameter AAA server determines that the user is a prepaid user and notices from the Credit-Control AVP that the NAS has credit-control capabilities. It sends a Diameter Credit-Control-Request with CC-Request-Type set to INITIAL_REQUEST to the Diameter Credit-Control server to perform credit authorization (3) and to establish a credit-control session. (The home Diameter AAA server may forward service-specific AVPs received from the NAS as input for the rating process.) The Diameter Credit-Control server checks the end user's account balance, rates the service, and reserves credit from the end user's account. The reserved quota is returned to the home Diameter AAA server in the Diameter Credit-Control-Answer (4). The home Diameter AAA server sends the reserved quota to the NAS in the Diameter AA-Answer (AAA). Upon receiving the AA-Answer, the NAS starts the credit-control session and starts monitoring the granted units (5). The NAS grants access to the end user (6). At the expiry of the allocated quota, the NAS sends a Diameter Credit-Control-Request with CC-Request-Type set to UPDATE_REQUEST to the home Diameter AAA server (7). This message contains the units used thus far. The home Diameter AAA server forwards the CCR to the Diameter Credit-Control server (8). The Diameter Credit-Control server debits the used units from the end user's account and allocates a new quota that is returned to the home Diameter AAA server in the Diameter Credit-Control-Answer (9). The message is forwarded to the NAS (10). During the ongoing credit-control session, the authorization lifetime expires, and the authorization/authentication client in the NAS performs service-specific re-authorization to the home Diameter AAA server, as usual. The credit-control client populates the AAR with

the Credit-Control AVP set to RE_AUTHORIZATION, indicating that the credit-control server shall not be contacted, as the credit authorization is controlled by the burning rate of the granted units (11). The home Diameter AAA server performs service-specific re-authorization as usual and returns the AA-Answer to the NAS (12). The end user logs off from the network (13). To debit the used units from the end user's account and to stop the credit-control session, the NAS sends a Diameter Credit-Control-Request with CC-Request-Type set to TERMINATION_REQUEST to the home Diameter AAA server (14). The home Diameter AAA server forwards the CCR to the credit-control server (15). The Diameter Credit-Control server acknowledges the session termination by sending a Diameter Credit-Control-Answer to the home Diameter AAA server (16). The home Diameter AAA server forwards the answer to the NAS (17). The STR/STA takes place between the NAS and home Diameter AAA server, as usual (18), (19).

A.2. Flow II

Figure 12 provides an example of Diameter Credit-Control for SIP sessions. Although the flow focuses on illustrating the usage of credit-control messages, the SIP signaling is inaccurate, and the diagram is not by any means an attempt to define a service provider's SIP network. However, for the sake of this example, some assumptions are made below.

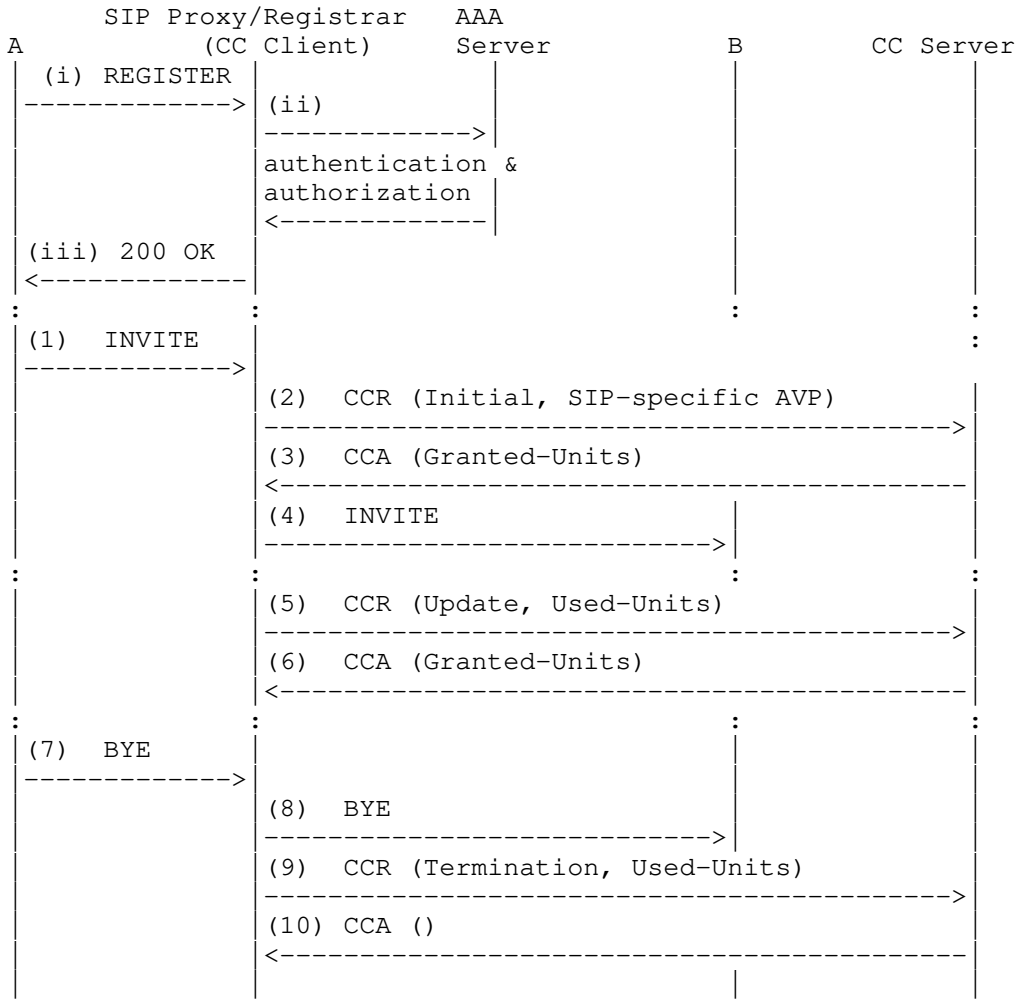


Figure 12: Flow II

Typically, prepaid services based, for example, on time usage for SIP sessions require an entity in the service provider network to intercept all the requests within the SIP dialog in order to detect events, such as session establishment and session release, that are essential for performing credit-control operations with the credit-control server. Therefore, in this example, it is assumed that the SIP Proxy adds a Record-Route header in the initial SIP INVITE to make sure that all the future requests in the created dialog traverse through it (for the definitions of "Record-Route" and "dialog", please refer to [RFC3261]). Finally, the degree of

credit-control measuring of the media by the proxy depends on the business model design used in setting up the end system and proxies in the SIP network.

The end user (SIP User Agent A) sends a REGISTER with credentials (i). The SIP Proxy sends a request to the home AAA server to perform multimedia authentication and authorization by using, for instance, a Diameter multimedia application (ii). The home AAA server checks that the credentials are correct and checks the user profile. Eventually, a 200 OK response (iii) is sent to the User Agent. Note that the authentication and authorization are valid for the registration validity period duration (i.e., until re-registration is performed). Several SIP sessions may be established without re-authorization.

User Agent A sends an INVITE (1). The SIP Proxy sends a Diameter Credit-Control-Request (INITIAL_REQUEST) to the Diameter Credit-Control server (2). The Credit-Control-Request contains information obtained from the SIP signaling describing the requested service (e.g., calling party, called party, Session Description Protocol (SDP) attributes). The Diameter Credit-Control server checks the end user's account balance, rates the service, and reserves credit from the end user's account. The reserved quota is returned to the SIP Proxy in the Diameter Credit-Control-Answer (3). The SIP Proxy forwards the SIP INVITE to User Agent B (4). B's phone rings, and B answers. The media flows between them, and the SIP Proxy starts measuring the quota. At the expiry of the allocated quota, the SIP Proxy sends a Diameter Credit-Control-Request (UPDATE_REQUEST) to the Diameter Credit-Control server (5). This message contains the units used thus far. The Diameter Credit-Control server debits the used units from the end user's account and allocates new credit that is returned to the SIP Proxy in the Diameter Credit-Control-Answer (6). The end user terminates the service by sending a BYE message (7). The SIP Proxy forwards the BYE message to User Agent B (8) and sends a Diameter Credit-Control-Request (TERMINATION_REQUEST) to the credit-control server (9). The Diameter Credit-Control server acknowledges the session termination by sending a Diameter Credit-Control-Answer to the SIP Proxy (10).

A.3. Flow III

A credit-control flow for Multimedia Messaging Service is shown in Figure 13. The sender is charged as soon as the messaging server successfully stores the message.

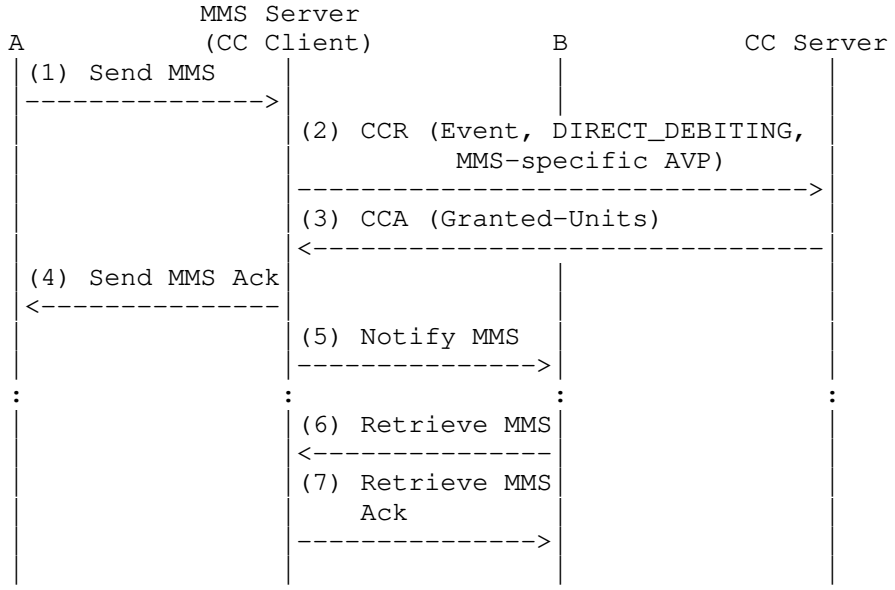


Figure 13: Flow III

This is an example of Diameter Credit-Control for direct debiting using the Multimedia Messaging Service environment. Although the flow focuses on illustrating the usage of credit-control messages, the MMS signaling is inaccurate, and the diagram is not by any means an attempt to define a service provider's MMS configuration or billing model.

End user A sends an MMS to the MMS server (1). The MMS server stores the message and sends a Diameter Credit-Control-Request (EVENT_REQUEST with Requested-Action set to DIRECT_DEBITING) to the Diameter Credit-Control server (2). The Credit-Control-Request contains information about the MMS message (e.g., size, recipient address, image coding type). The Diameter Credit-Control server checks the end user's account balance, rates the service, and debits the service from the end user's account. The granted quota is returned to the MMS server in the Diameter Credit-Control-Answer (3).

The MMS server acknowledges the successful reception of the MMS message (4). The MMS server notifies the recipient about the new MMS (5), and end user B retrieves the message from the MMS message store (6), (7).

Note that the transfer of the MMS message can take an extended period of time and can fail, in which case a recovery action is needed. The MMS server should return the already-debited units to the user's account by using the REFUND action described in Section 6.4.

A.4. Flow IV

Another credit-control flow for Multimedia Messaging Service is shown in Figure 14. The recipient is charged at the time of message delivery.

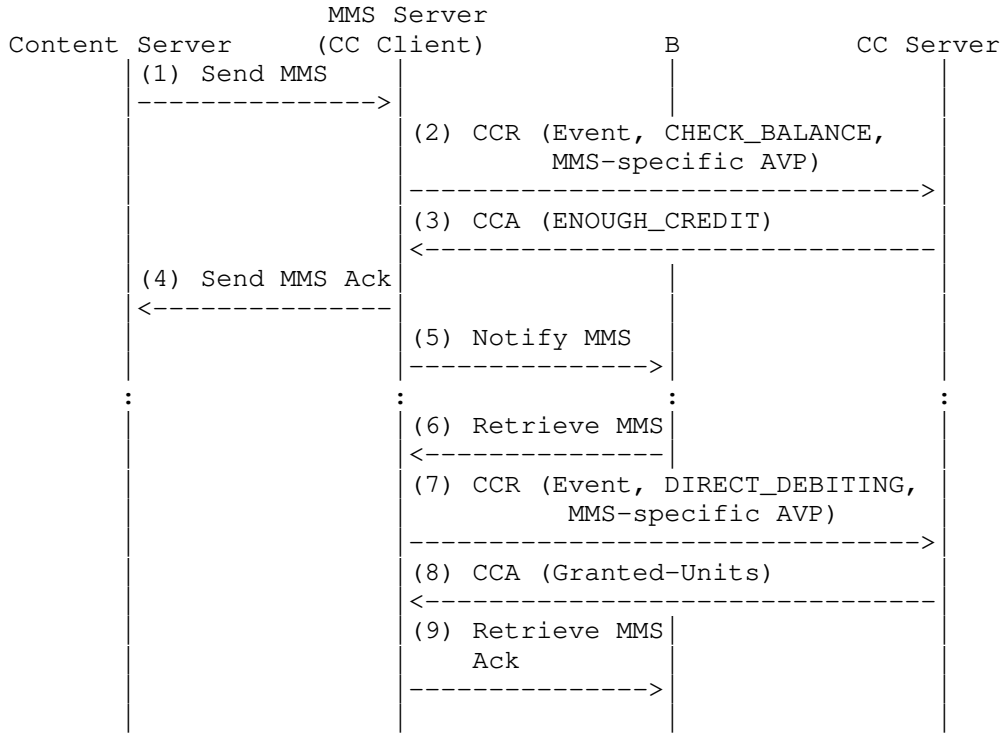


Figure 14: Flow IV

This is an example of Diameter Credit-Control for direct debiting using the Multimedia Messaging Service environment. Although the flow focuses on illustrating the usage of credit-control messages, the MMS signaling is inaccurate, and the diagram is not by any means an attempt to define a service provider's MMS configuration or billing model.

A content server sends an MMS to the MMS server (1), which stores the message. The message recipient will be charged for the MMS message in this case. As there can be a substantially long time between the receipt of the message at the MMS server and the actual retrieval of the message, the MMS server does not establish any credit-control sessions to the Diameter Credit-Control server; rather, it first performs only a balance check (without any credit reservations) by sending a Diameter Credit-Control-Request (EVENT_REQUEST with Requested-Action set to CHECK_BALANCE) to verify that end user B can cover the cost for the MMS (2). The Diameter Credit-Control server checks the end user's account balance and returns the answer to the MMS server in the Diameter Credit-Control-Answer (3). The MMS server acknowledges the successful reception of the MMS message (4). The MMS server notifies the recipient of the new MMS (5), and after some time end user B retrieves the message from the MMS message store (6). The MMS server sends a Diameter Credit-Control-Request (EVENT_REQUEST with Requested-Action set to DIRECT_DEBITING) to the Diameter Credit-Control server (7). The Credit-Control-Request contains information about the MMS message (e.g., size, recipient address, coding type). The Diameter Credit-Control server checks the end user's account balance, rates the service, and debits the service from the end user's account. The granted quota is returned to the MMS server in the Diameter Credit-Control-Answer (8). The MMS is transferred to end user B (9).

Note that the transfer of the MMS message can take an extended period of time and can fail, in which case a recovery action is needed. The MMS server should return the already-debited units to the user's account by using the REFUND action described in Section 6.4.

A.5. Flow V

Figure 15 provides an example of an Advice of Charge (AoC) service for a SIP call.

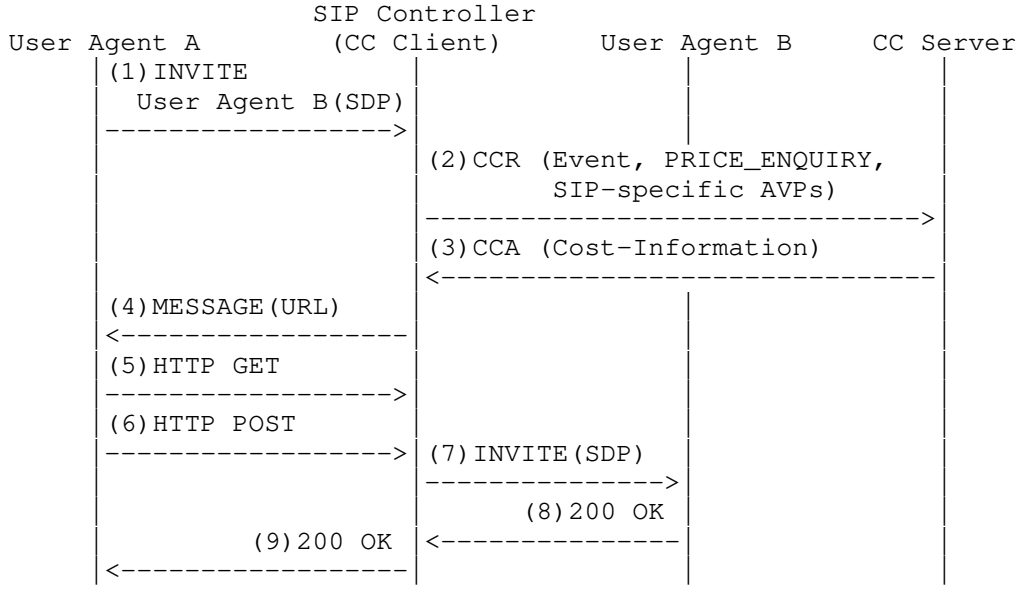


Figure 15: Flow V

This is an example of Diameter Credit-Control for SIP sessions. Although the flow focuses on illustrating the usage of credit-control messages, the SIP signaling is inaccurate, and the diagram is not by any means an attempt to define a service provider's SIP network.

User Agent A can be either a postpaid or prepaid subscriber using the AoC service. It is assumed that the SIP controller also has HTTP capabilities and delivers an interactive AoC web page with, for instance, the cost information, the details of the call derived from the SDP, and a button to accept/not accept the charges. (There may be many other ways to deliver AoC information; however, this flow focuses on the use of the credit-control messages.) The user has been authenticated and authorized prior to initiating the call and has been subscribed to the AoC service.

User Agent A sends an INVITE with the SDP to User Agent B via the SIP controller (1). The SIP controller determines that the user is subscribed to an AoC service and sends a Diameter Credit-Control-Request (EVENT_REQUEST with Requested-Action set to PRICE_ENQUIRY) to the Diameter Credit-Control server (2). The Credit-Control-Request

contains SIP-specific AVPs derived from the SIP signaling, describing the requested service (e.g., calling party, called party, SDP attributes). The Diameter Credit-Control server determines the cost of the service and returns the Credit-Control-Answer, including the Cost-Information AVP (3). The SIP controller manufactures the AoC web page with information received in SIP signaling and with the cost information received from the credit-control server. It then sends a SIP MESSAGE that contains a URL pointing to the AoC information web page (4). Upon receipt of the SIP MESSAGE, User Agent A automatically invokes the web browser that retrieves the AoC information (5). The user clicks on the appropriate button to accept the charges (6). The SIP controller continues the session and sends the INVITE to User Agent B, which accepts the call (7), (8), (9).

A.6. Flow VI

Figure 16 illustrates a credit-control flow for the REFUND case. It is assumed that there is a trusted relationship and secure connection between the gaming server and the Diameter Credit-Control server. The end user may be a prepaid subscriber or a postpaid subscriber.

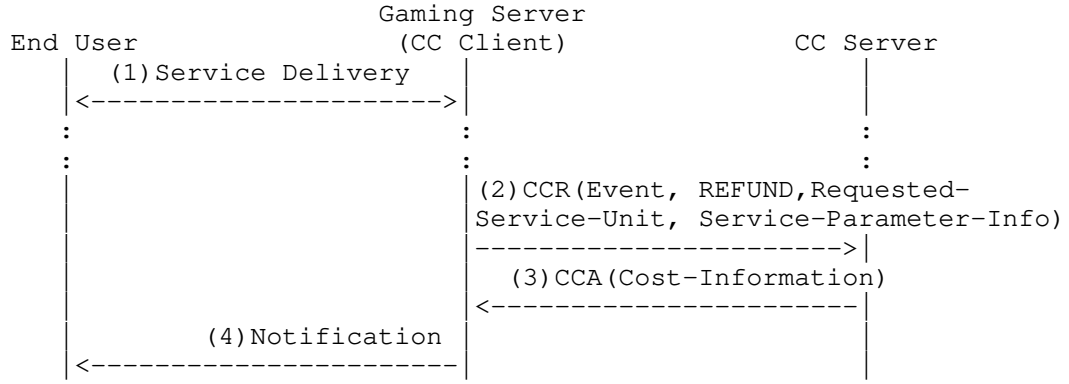


Figure 16: Flow VI

While the end user is playing the game (1), they enter a new level that entitles them to a bonus. The gaming server sends a Diameter Credit-Control-Request (EVENT_REQUEST with Requested-Action set to REFUND_ACCOUNT) to the Diameter Credit-Control server (2). The Credit-Control-Request contains the Requested-Service-Unit AVP with the CC-Service-Specific-Units containing the number of points the user just won. The Service-Parameter-Info AVP is also included in the request and specifies the service event to be rated (e.g., Tetris Bonus). From information received, the Diameter Credit-Control server determines the amount to be credited, refunds the user's account, and returns the Credit-Control-Answer, including the

Cost-Information AVP (3). The Cost-Information AVP indicates the credited amount. At the first opportunity, the gaming server notifies the end user of the credited amount (4).

A.7. Flow VII

Figure 17 provides an example of graceful service termination for a SIP call. It is assumed that the call is set up so that the controller is in the call as a B2BUA (Back-to-Back User Agent) performing third-party call control (3PCC). Note that the SIP signaling is inaccurate, as the focus of this flow is on graceful service termination and credit-control authorization. Best practices for 3PCC are defined in [RFC3725].

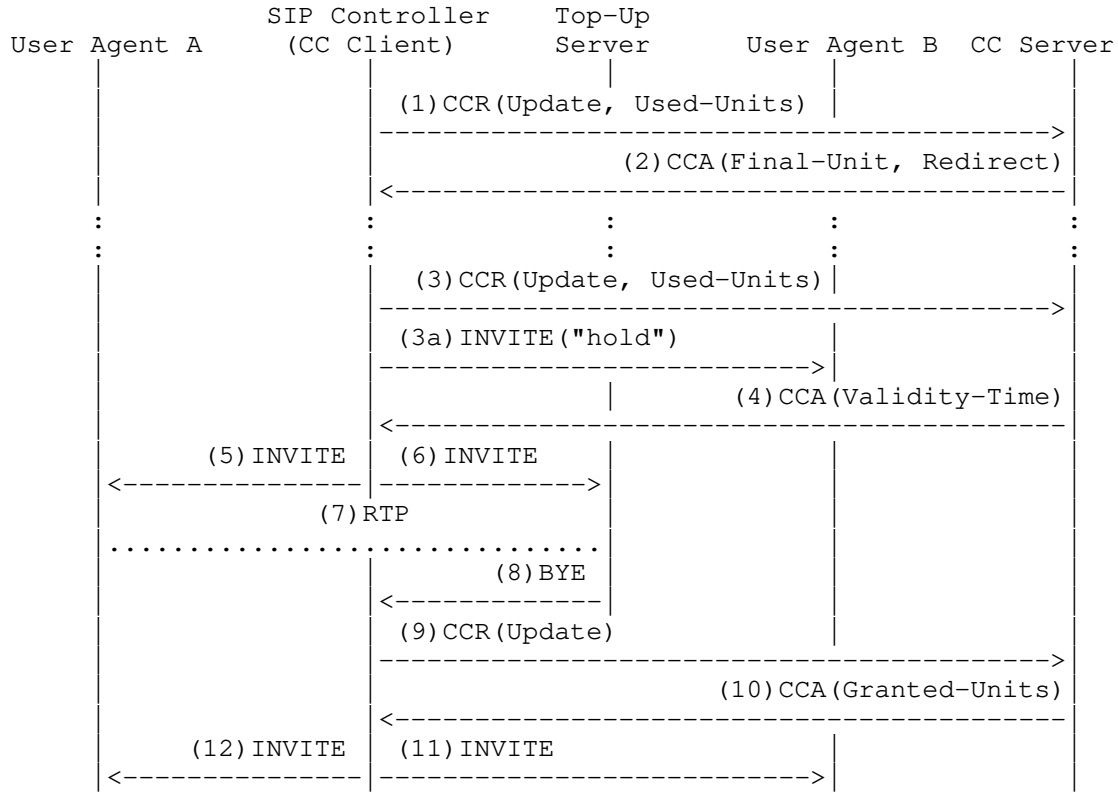


Figure 17: Flow VII

The call is ongoing between User Agents A and B; User Agent A has a prepaid subscription. At the expiry of the allocated quota, the SIP controller sends a Diameter Credit-Control-Request (UPDATE_REQUEST) to the Diameter Credit-Control server (1). This message contains the units used thus far. The Diameter Credit-Control server debits the used units from the end user's account and allocates the final quota returned to the SIP controller in the Diameter Credit-Control-Answer (2). This message contains the Final-Unit-Indication AVP with Final-Unit-Action set to REDIRECT, the Redirect-Address-Type set to SIP URI, and the Redirect-Server-Address set to the top-up server name (e.g., sip:sip-topup-server@domain.com). At the expiry of the final allocated quota, the SIP controller sends a Diameter Credit-Control-Request (UPDATE_REQUEST) to the Diameter Credit-Control server (3) and places the called party on "hold" by sending an INVITE with the appropriate connection address in the SDP (3a). The Credit-Control-Request message contains the units used thus far. The Diameter Credit-Control server debits the used units from the end user's account but does not make any credit reservations. The Credit-Control-Answer message, which contains the Validity-Time to supervise the graceful service termination process, is returned to the SIP controller (4). The SIP controller establishes a SIP session between the prepaid user and the top-up server (5), (6). The top-up server plays an announcement and prompts the user to enter a credit card number and the amount of money to be used to replenish the account (7). The top-up server validates the credit card number, replenishes the user's account (using some means outside the scope of this specification), and releases the SIP session (8). The SIP controller can now assume that communication between the prepaid user and the top-up server took place. It sends a spontaneous Credit-Control-Request (UPDATE_REQUEST) to the Diameter Credit-Control server to check whether the account has been replenished (9). The Diameter Credit-Control server reserves credit from the end user's account and returns the reserved quota to the SIP controller in the Credit-Control-Answer (10). At this point, the SIP controller reconnects the caller and the called party (11), (12).

A.8. Flow VIII

Figure 18 provides an example of graceful service termination initiated when the first interrogation takes place because the user's account is empty. In this example, the credit-control server supports the server-initiated credit re-authorization. The Diameter protocol application is implemented in the NAS per [RFC7155].

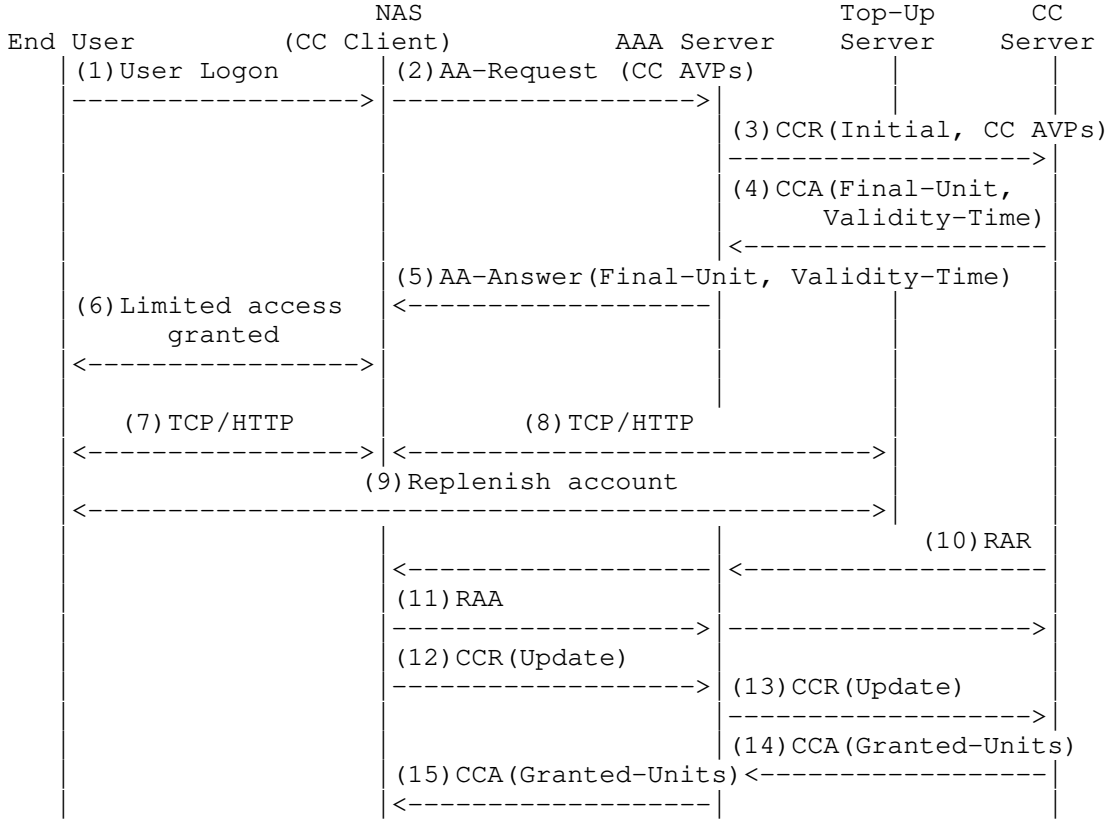


Figure 18: Flow VIII

The user logs on to the network (1). The Diameter NAS sends a Diameter AA-Request (AAR) to the home Diameter AAA server (2). The credit-control client populates the AAR with the Credit-Control AVP set to CREDIT_AUTHORIZATION, and service-specific AVPs are included, as usual [RFC7155]. The home Diameter AAA server performs service-specific authentication and authorization, as usual. The home Diameter AAA server determines that the user has a prepaid subscription and notices from the Credit-Control AVP that the NAS has credit-control capabilities. It sends a Diameter Credit-Control-

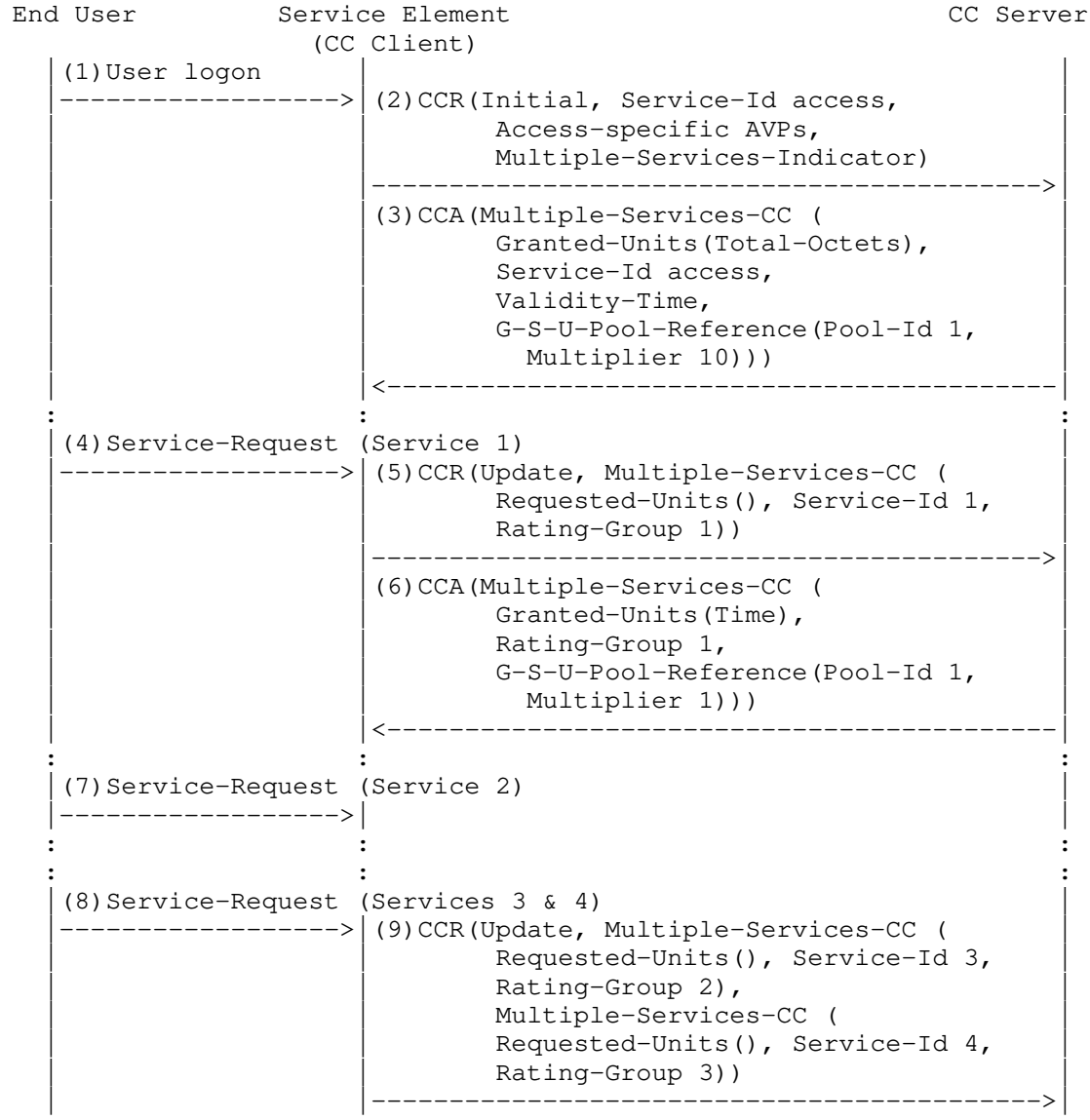
Request with CC-Request-Type set to INITIAL_REQUEST to the Diameter Credit-Control server to perform credit authorization (3) and to establish a credit-control session. (The home Diameter AAA server may forward service-specific AVPs received from the NAS as input for the rating process.) The Diameter Credit-Control server checks the end user's account balance, determines that the account cannot cover the cost of the service, and initiates graceful service termination. The Credit-Control-Answer is returned to the home Diameter AAA server (4). This message contains the Final-Unit-Indication AVP and the Validity-Time AVP set to a reasonable amount of time, to give the user a chance to replenish their account (e.g., 10 minutes). The Final-Unit-Indication AVP includes the Final-Unit-Action set to REDIRECT, the Redirect-Address-Type set to URL, and the Redirect-Server-Address set to the HTTP top-up server name. The home Diameter AAA server sends the received Credit-Control AVPs to the NAS in the Diameter AA-Answer (5). Upon successful AAA, the NAS starts the credit-control session and immediately starts graceful service termination, as instructed by the server. The NAS grants limited access to the user (6). The HTTP client software running in the user's device opens the transport connection redirected by the NAS to the top-up server (7), (8). An appropriate web page is provided for the user where the user can enter the credit card number and the amount of money to be used to replenish the account, along with a notification message that they are granted unlimited access if the replenishment operation will be successfully executed within, for example, the next 10 minutes. The top-up server validates the credit card number and replenishes the user's account (using some means outside the scope of this specification) (9). After successful account top-up, the credit-control server sends a Re-Auth-Request message to the NAS (10). The NAS acknowledges the request by returning the Re-Auth-Answer message (11) and initiates the credit re-authorization by sending a Credit-Control-Request (UPDATE_REQUEST) to the Diameter Credit-Control server (12), (13).

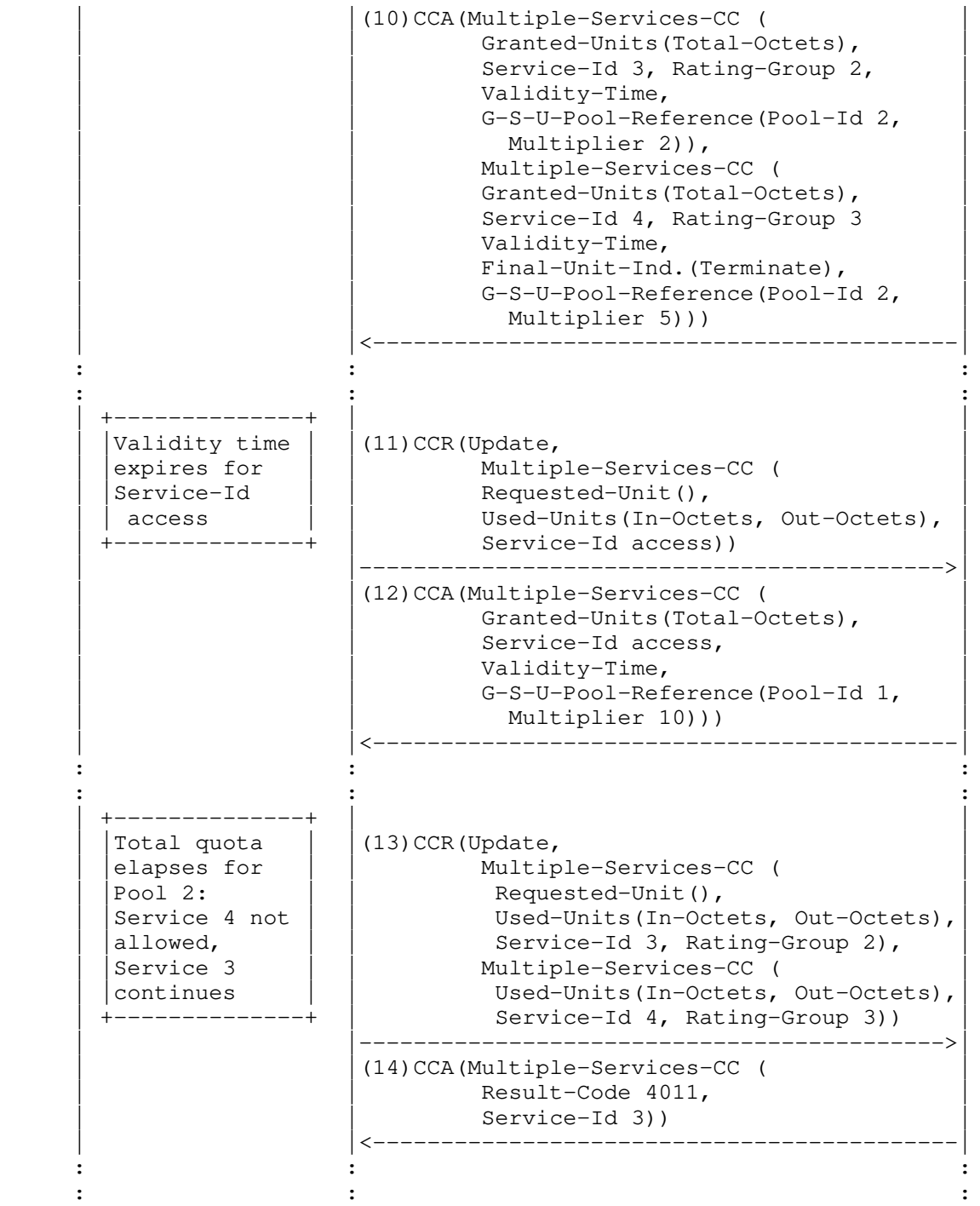
The Diameter Credit-Control server reserves credit from the end user's account and returns the reserved quota to the NAS via the home Diameter AAA server in the Credit-Control-Answer (14), (15). The NAS removes the restriction applied by graceful service termination and starts monitoring the granted units.

A.9. Flow IX

The Diameter Credit-Control application defines the Multiple-Services-Credit-Control AVP, which can be used to support independent credit-control of multiple services in a single credit-control (sub-)session for Service Elements that have such capabilities. It is possible to request and allocate resources as a credit pool that is shared between services or rating-groups.

Figure 19 illustrates a usage scenario where the credit-control client and server support independent credit-control of multiple services, as defined in Section 5.1.2. It is assumed that service-identifiers, rating-groups, and their associated parameters (e.g., IP 5-tuples) are locally configured in the Service Element or provisioned by an entity other than the credit-control server.




(10)CCA(Multiple-Services-CC (
Granted-Units(Total-Octets),
Service-Id 3, Rating-Group 2,
Validity-Time,
G-S-U-Pool-Reference(Pool-Id 2,
Multiplier 2)),
Multiple-Services-CC (
Granted-Units(Total-Octets),
Service-Id 4, Rating-Group 3
Validity-Time,
Final-Unit-Ind.(Terminate),
G-S-U-Pool-Reference(Pool-Id 2,
Multiplier 5)))
Validity time expires for Service-Id access
(11)CCR(Update,
Multiple-Services-CC (
Requested-Unit(),
Used-Units(In-Octets, Out-Octets),
Service-Id access))
(12)CCA(Multiple-Services-CC (
Granted-Units(Total-Octets),
Service-Id access,
Validity-Time,
G-S-U-Pool-Reference(Pool-Id 1,
Multiplier 10)))
Total quota elapses for Pool 2: Service 4 not allowed, Service 3 continues
(13)CCR(Update,
Multiple-Services-CC (
Requested-Unit(),
Used-Units(In-Octets, Out-Octets),
Service-Id 3, Rating-Group 2),
Multiple-Services-CC (
Used-Units(In-Octets, Out-Octets),
Service-Id 4, Rating-Group 3))
(14)CCA(Multiple-Services-CC (
Result-Code 4011,
Service-Id 3))

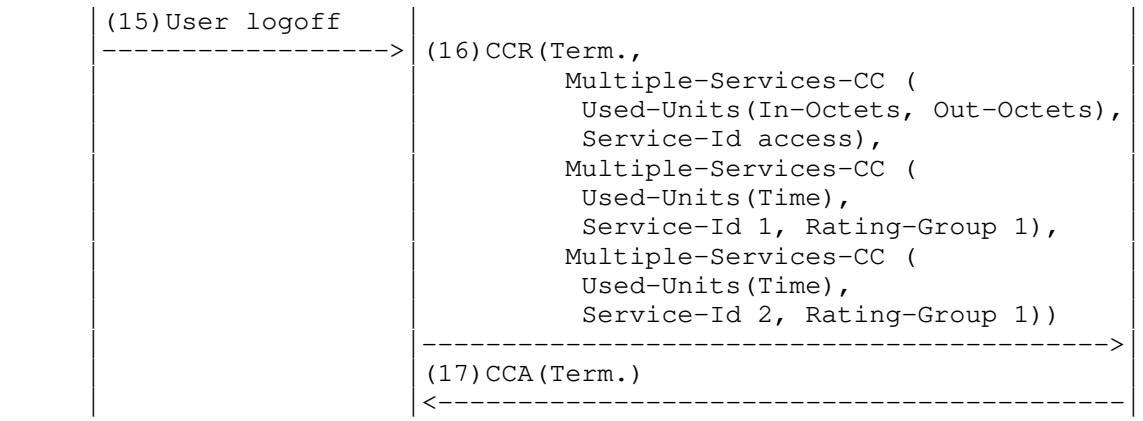


Figure 19: Flow IX: Example of Independent Credit-Control of Multiple Services in a Credit-Control (Sub-)Session

The user logs on to the network (1). The Service Element sends a Diameter Credit-Control-Request with CC-Request-Type set to INITIAL_REQUEST to the Diameter Credit-Control server to perform credit authorization for the bearer service (e.g., Internet access service) and to establish a credit-control session (2). In this message, the credit-control client indicates support for independent credit-control of multiple services within the session by including the Multiple-Services-Indicator AVP. The Diameter Credit-Control server checks the end user's account balance, with rating information received from the client (i.e., Service-Id and access-specific AVPs); rates the request; and reserves credit from the end user's account. Suppose that the server reserves $5 and determines that the cost is $1/MB. It then returns to the Service Element a Credit-Control-Answer message that includes the Multiple-Services-Credit-Control AVP with a quota of 5 MB associated to the Service-Id (access), to a multiplier value of 10, and to Pool-Id 1 (3).

The user uses service 1 (4). The Service Element sends a Diameter Credit-Control-Request with CC-Request-Type set to UPDATE_REQUEST to the credit-control server to perform credit authorization for service 1 (5). This message includes the Multiple-Services-Credit-Control AVP to request service units for service 1 that belong to Rating-Group 1. The Diameter Credit-Control server determines that service 1 draws credit resources from the same account as the access service (i.e., pool 1). It rates the request according to Service-Id/rating-group and updates the existing reservation by requesting more credit. Suppose that the server reserves $5 more (now the reservation is $10) and determines that the cost is $0.1/minute. The server authorizes the whole rating-group. It then returns to the Service Element a Credit-Control-Answer message that

includes the Multiple-Services-Credit-Control AVP with a quota of 50 minutes associated to Rating-Group 1, to a multiplier value of 1, and to Pool-Id 1 (6). The client adjusts the total amount of resources for pool 1 according to the received quota, which gives S for pool 1 = 100.

The user uses service 2, which belongs to the authorized rating-group (Rating-Group 1) (7). Resources are then consumed from pool 1.

The user now requests services 3 and 4 as well, which are not authorized (8). The Service Element sends a Diameter Credit-Control-Request with CC-Request-Type set to UPDATE_REQUEST to the credit-control server in order to perform credit authorization for services 3 and 4 (9). This message includes two instances of the Multiple-Services-Credit-Control AVP to request service units for service 3 that belong to Rating-Group 2 and service units for service 4 that belong to Rating-Group 3. The Diameter Credit-Control server determines that services 3 and 4 draw credit resources from another account (i.e., pool 2). It checks the end user's account balance and, according to Service-Id/rating-group information, rates the request. It then reserves credit from pool 2.

For example, the server reserves $5 and determines that service 3 costs $0.2/MB and service 4 costs $0.5/MB. The server authorizes only services 3 and 4. It returns to the Service Element a Credit-Control-Answer message that includes two instances of the Multiple-Services-Credit-Control AVP (10). One instance grants a quota of 12.5 MB associated to Service-Id 3 to a multiplier value of 2 and to Pool-Id 2. The other instance grants a quota of 5 MB associated to Service-Id 4 to a multiplier value of 5 and to Pool-Id 2.

The server also determines that pool 2 is exhausted and service 4 is not allowed to continue after these units will be consumed. Therefore, the Final-Unit-Indication AVP with action TERMINATE is associated to Service-Id 4. The client calculates the total amount of resources that can be used for pool 2 according to the received quotas and multipliers, which gives S for pool 2 = 50.

The Validity-Time for the access service expires. The Service Element sends a Credit-Control-Request message to the server in order to perform credit re-authorization for the Service-Id (access) (11). This message carries one instance of the Multiple-Services-Credit-Control AVP that includes the units used by this service. Suppose that the total amount of used units is 4 MB. The client adjusts the total amount of resources for pool 1 accordingly, which gives S for pool 1 = 60.

The server deducts $4 from the user's account and updates the reservation by requesting more credit. Suppose that the server reserves $5 more (now the reservation is $11) and already knows the cost of the Service-Id (access), which is $1/MB. It then returns to the Service Element a Credit-Control-Answer message that includes the Multiple-Services-Credit-Control AVP with a quota of 5 MB associated to the Service-Id (access), to a multiplier value of 10, and to Pool-Id 1 (12). The client adjusts the total amount of resources for pool 1 according to the received quota, which gives S for pool 1 = 110.

Services 3 and 4 consume the total amount of pool 2's credit resources (i.e., C1*2 + C2*5 >= S). The Service Element immediately starts the TERMINATE action for service 4 and sends a Credit-Control-Request message with CC-Request-Type set to UPDATE_REQUEST to the credit-control server in order to perform credit re-authorization for service 3 (13). This message contains two instances of the Multiple-Services-Credit-Control AVP to report the units used by services 3 and 4. The server deducts the last $5 from the user's account (pool 2) and returns the answer with Result-Code 4011 in the Multiple-Services-Credit-Control AVP to indicate that service 3 can continue without credit-control (14).

The end user logs off from the network (15). To debit the used units from the end user's account and to stop the credit-control session, the Service Element sends a Diameter Credit-Control-Request with CC-Request-Type set to TERMINATION_REQUEST to the credit-control server (16). This message contains the units used by each service in multiple instances of the Multiple-Services-Credit-Control AVP. The used units are associated with the relevant Service-Identifier and rating-group. The Diameter Credit-Control server debits the used units to the user's account (pool 1) and acknowledges the session termination by sending a Diameter Credit-Control-Answer to the Service Element (17).

Acknowledgements

The original authors of RFC 4006 are Harri Hakala, Leena Mattila, Juha-Pekka Koskinen, Marco Stura, and John Loughney.

The authors would like to thank Bernard Aboba, Jari Arkko, Robert Ekblad, Pasi Eronen, Benny Gustafsson, Robert Karlsson, Avi Lior, Jussi Maki, Paco Marin, Jeff Meyer, Anne Narhi, John Prudhoe, Christopher Richards, Juha Vallinen, and Mark Watson for their comments and suggestions.

Authors' Addresses

Lyle Bertz (editor)
Sprint
6220 Sprint Parkway
Overland Park, KS 66251
United States of America

Email: lyleb551144@gmail.com

David Dolson (editor)
Sandvine
408 Albert Street
Waterloo, ON N2L 3V3
Canada

Email: ddolson@acm.org

Yuval Lifshitz (editor)
Sandvine
408 Albert Street
Waterloo, ON N2L 3V3
Canada

Email: yuvalif@yahoo.com