Network Working Group
INTERNET-DRAFT
Category: Informational
draft-lior-radius-prepaid-extensions-08.txt
Expires: 18 January, 2006

A. Lior
Bridgewater Systems
P. Yegani
Cisco
K. Chowdhury
Starent Networks
H. Tschofenig
C. Guenther
Siemens

July 17, 2005

PrePaid Extensions to Remote Authentication Dial-In User Service (RADIUS)

Status of this Memo

Copyright Notice

Abstract

This draft presents an extension to the Remote Authentication Dial-In User Service (RADIUS) protocol to support charging for prepaid services. The charging models supported are namely: volume-based charging, duration-based charging and one-time-based charging.

Table of Contents

1. Introduction

This draft describes extensions for the RADIUS protocol. These extensions are meant to enable service providers to charge and bill their customers using prepaid accounts.

A prepaid service subscriber is a user who has purchased a contract according to which he will receive a particular data service for either a period of time or a quantity of data. In the typical prepaid scenario, the service provider verifies that the subscriber has sufficient funds in his account before delivering the service. Only if sufficient funds are available is the service provided to the user.

Note that the means by which the subscriber obtains funds is outside the scope of this document. Also note that, in some scenarios, the subscriber's account may be used to fund multiple services, some of which may use the extensions defined in this documents, and some may use other mechanisms. While the interworking of the mechanisms described in this document with other mechanisms should be possible and straightforward, how this could be done depends on the external mechanisms and is, as such, outside the scope of this document.

The business driver behind the protocol extensions defined in this document is to increase participation (i.e. a service provider's subscriber base) and thus to increase revenues. In particular, the extensions were designed with the following goals in mind.

- Make use of existing infrastructure as much as possible, and thereby limit the amount of necessary capital expenditures,
- provide the ability to rate service requests in real-time,</t>
- provide the ability to charge the user's account - charge prior to service provision,
- protect against revenue loss, i.e. prevent an end user from obtaining service when the available funds are not sufficient,
- protect against fraud, and
- be as widely deployable over dialup, wireless and WLAN networks.

The architecture between the entities that execute the RADIUS protocols with the extensions defined in this document assumes that rating of chargeable events does not occur in the element that provides the service. Instead, the rating may be performed at a dedicated server, termed the ôprepaid enabled AAA serverö or simply ôprepaid serverö. Alternatively, the actual rating may occur in an entity behind this prepaid server. Furthermore, business logic may dictate a time-dependent tariff model, for example that the price for a service may switch at 8pm from a high to a low tariff. The extensions defined in this document support such scenarios.

Furthermore, this documents assumes an architecture where a `quota server' is available which, through co-ordination with the rating entity and a centralized account balance manager, is able to provide a quota indication for a particular user when requested. This quota server may or may not coexist in the prepaid server.

1.1 Terminology

Network Access Server (NAS)	As in RADIUS.
Prepaid Client(PPC)	The entity which triggers the RADIUS message exchange including prepaid extensions defined in this document. The PPC typically resides in the NAS.
Prepaid Server(PPS)	The entity that interacts with the Prepaid Client using the RADIUS prepaid extensions defined in this document.
Home network	The entity which maintains the userÆs profile and prepaid account.
WLAN	Wireless Local Area Network
Service Event	
Access Service	The service that is provided to the user when the user is authenticated and authorized.

Furthermore, the following terms are used in this document. Mobile IP and AAA terminology: Home agent (HA), Home network, Home AAA (HAAA), Broker AAA (BAAA), Visited AAA (VAAA) and Foreign Agent (FA)

1.2 Requirements language

In this document, several words are used to signify the requirements of the specification. These words are often capitalized. The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Overview

This section provides an overview of the prepaid charging models, and their associated architectures, that are supported by the extensions proposed in this document.

2.1 Prepaid Charging Models

A number of models of how to charge customers for data services in a prepaid manner are supported, as follows.

- Volume-based charging (VBC): (e.g. 2 Cents/KiloByte)
- Duration-based charging (DBC): (e.g. 3 Cents/minute)
- Subscription-based charging (SBC): (e.g. Dollars/month)
- Event-based charging (EBC): (e.g. 7 Cents/URL or email)

Whether the user account is a dedicated prepaid account or a general account (such as a current bank account) is outside the scope of this document.

2.2 Architectural Model

The architectural model assumed in this document encompasses the following entities.

(1) Service Access Device (SAD): This entity provides a data service to the users, and typically coincides with the NAS. The SAD executes the RADIUS client which, for the purposes of this document, is termed the PPC. When prepaid service is used the SAD collects service event information and reports it while or after services are provided to the user. This event information is sent to the PPS using the extensions defined in this document.

(2) The PPS: The RADUIS server. If real-time credit control is

required, the PPC (SAD) contacts the PPS with service event information included before the service is provided. The PPS

performs a credit check and allocates a portion of available credit to the service event.

(3) The rating entity: This entity converts the credit that is allocated by the PPS into a time or volume amount, called the ôquotaö. This quota is then returned to the requesting PPC (SAD) (via the PPS). The rating entity may also determine that during service provision a tariff switch will occur. In this case the rating entity will include details of when exactly tariff switch will occur.

The requesting SAD (PPC) monitors the provision of the service according to the instructions returned by the PPS. After service completion or on a subsequent request for service, the PPS deducts the corresponding amount of credit from the user account. When a user terminates an on-going service, the PPC informs the PPS with a suitable indication about the unused portion of the allocated quota. The PPS is then able to refund the user account appropriately.

Multiple PPSs MAY be deployed for reasons of redundancy and load balancing. The system MAY also employ multiple rating servers. Prepaid accounts MAY be located in a centralized database. The detailed architecture of the system and its interfaces are outside the scope of this specification.

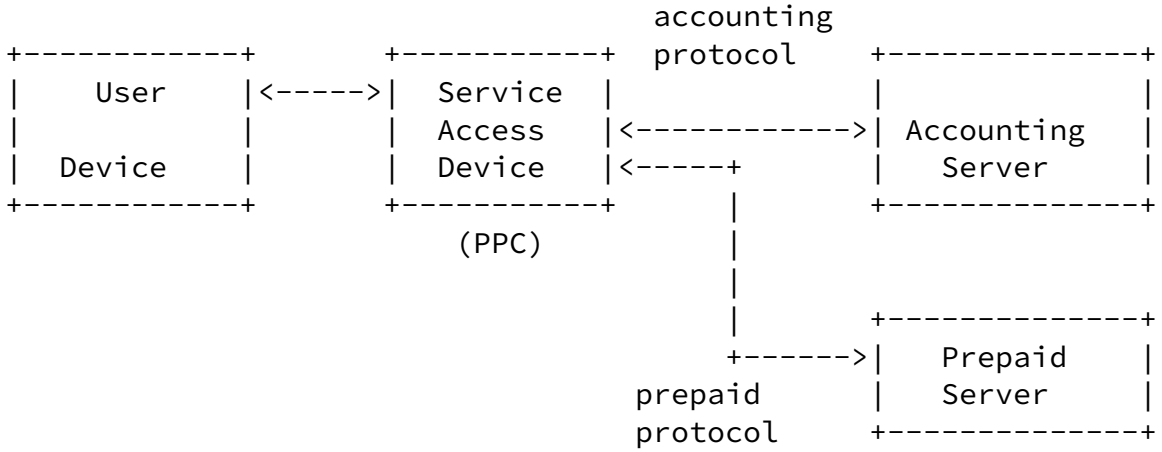


Figure 1 Basic Prepaid Architecture

The PPS and the accounting server in this architecture are logical entities. The real configuration MAY combine them into a single host.

The SAD MUST have the ability to meter the usage for a prepaid data session. This usage includes time or volume (e.g. number of bytes).

In roaming scenarios using mobile IP the PPC may run on the Home Agent. Furthermore, the device running the PPC may also have ôDynamic Session Capabilitiesö such as the ability to terminate a data session or change the filters associated with a specific data session by processing ôDisconnectö messages and ôChange of Authorizationö messages as per [RFC3576].

This document assumes that the PPS is used as the AAA server. There are three types of AAA server, as follows. (i) The AAA server in the home network (HAAA), which is responsible for authentication of the subscriber. In addition, the HAAA communicates with the PPS using the RADIUS protocol in order to authorize subscribers. (ii) The AAA server in the visited network (VAAA) which exists only in roaming scenarios and is responsible for forwarding the RADIUS messages to the HAAA. The VAAA may also modify the messages. Note that, in certain roaming deployments, the visited network may be connected to the home network via one or more broker networks. (iii) The AAA server in one of the aforementioned broker networks (BAAA), which is responsible for forwarding messages and does not play an active role in the prepaid data service delivery. A BAAA obviously exists only in those roaming deployments where the VAAA and the HAAA are connected via the BAAA of a broker network.

This document assumes that the PPS communicates with the HAAA for the purposes of authorisation. Additionally, the PPS interfaces to entities which

- Keep the subscriberÆs account balance (balance manager),
- Rate access service requests in real-time (Rating Engine), and
- Manage quota for a particular prepaid service (Quota Server).

Three deployment scenarios are presented in the remainder of this section. The first scenario is depicted in Figure 2. In this scenario, the SAD, which runs the PPC, the HAAA, and the PPS are located in the same provider network.

The Subscriber Device establishes a connection with one of possibly multiple SADs in the network. The selected SAD communicates with a HAAA server. However, in order to provide redundancy, multiple HAAA may be available.

The network has one or more PPSs. The interface between the HAAA and the PPS is implemented using the RADIUS protocol together with the extensions described in this document. However, in cases where the PPS does not implement the RADIUS protocol, the implementation would have to map the requirements defined in this document to a functionally equivalent protocol.

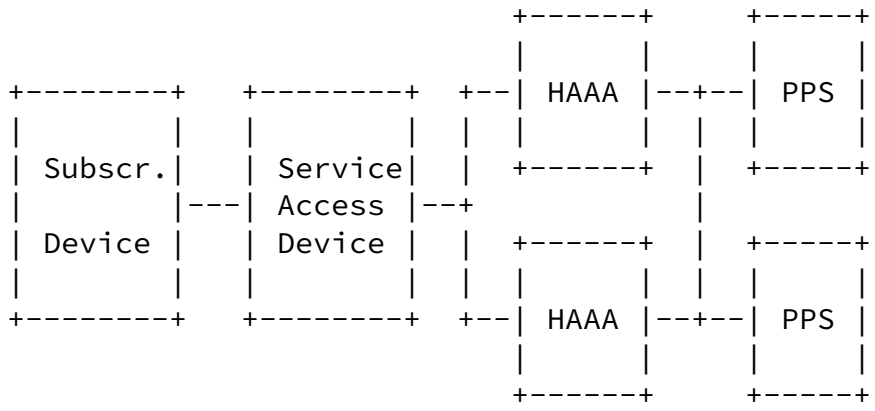
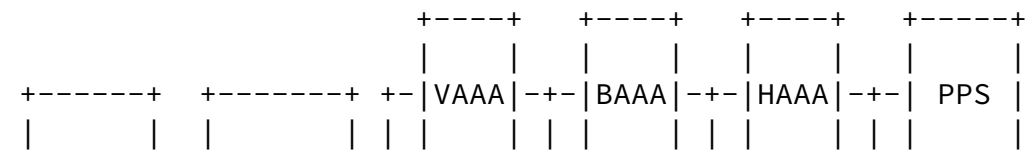
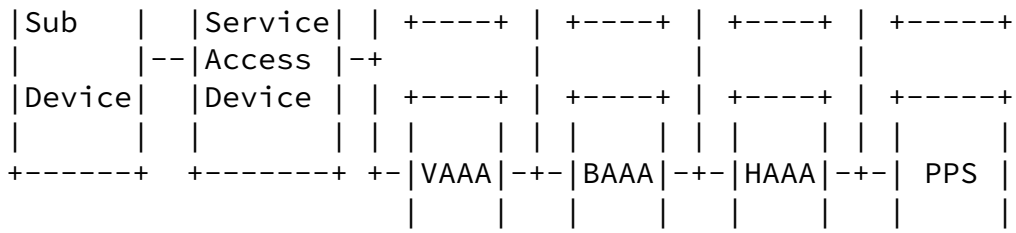


Figure 2 Basic Prepaid Access Architecture

The second scenario, depicted in Figure 3, is based on a static roaming architecture that is typical of a wholesale scenario for Dial-Up users or a broker scenario used in Dial-Up or WLAN roaming scenarios.





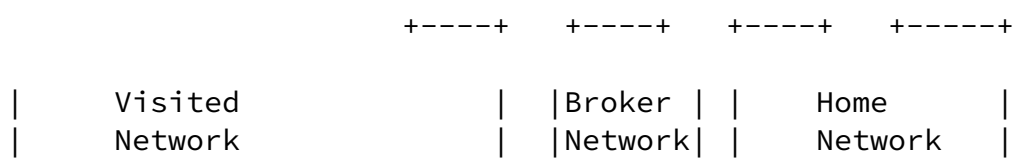
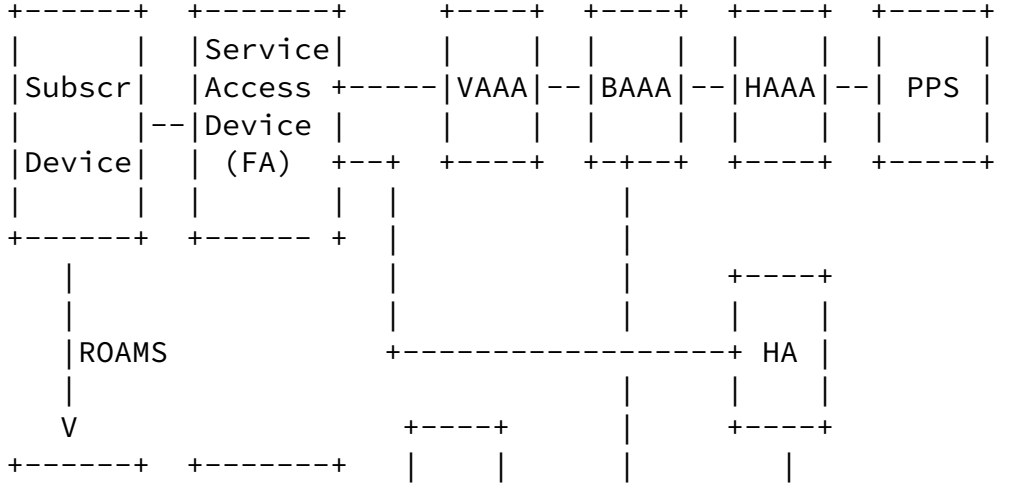


Figure 3 Static Roaming Prepaid Architecture

As in the basic prepaid architecture the subscriberÆs device establishes a connection with the SAD. The SAD communicates with the VAAA using the RADIUS protocol. The VAAA, in turn, communicates using the RADIUS protocol with BAAA servers in the broker network. There maybe more then one Broker Network between the Visited Network and the Home Network. The Home Network is the same as in the architecture depicted in Figure 2.

The third scenario is a roaming scenario where the network utilises Mobile-IP. It is depicted Figure 4. In this scenario the mobile device moves between networks that use different technologies such as between WLAN and Broadband. Mobile-IP addresses this type of mobility and therefore we need not be concerned with the underlying network technology.



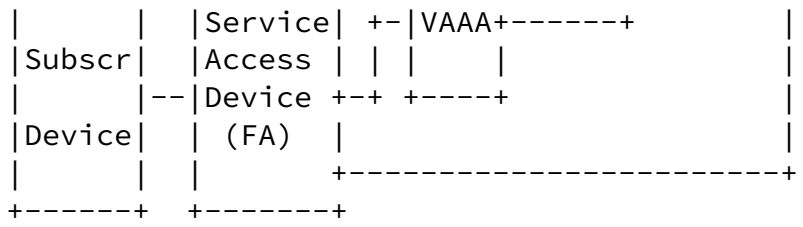


Figure 4 Roaming using Mobile-IP and pre-paid enabled SADs

In Figure 4, the Subscriber Device establishes a session with the SAD in the foreign network. The setup for this access service is identical to the cases covered above. Note that the SAD may be collocated with the Foreign Agent (FA) if Mobile-IPv4 is being used. As the subscriber device moves, it establishes a connection with another SAD possibly in another foreign network. The prepaid data service should continue to be available. When a device associates to another SAD it MUST re-authenticate at the new SAD and de-associate or log off from the old SAD. Furthermore, any unused quota at the old SAD MUST be credited into the subscriberÆs account immediately. This has to happen immediately because otherwise, if the subscriberÆs funds are low, he may be denied service at the new SAD.

Note that, if the SADs communicate directly with each other then there could be a way to accelerate the handoff procedure. In particular, the subscriber could be refunded more quickly. Unfortunately, handoff procedures are specific to the underlying network technologies and vary significantly in terms of delay.

2.3 Motivation

It has been asked ôWhy not use existing RADIUS attributes to construct a protocol for prepaid scenarios? This will allow us to have a solution with existing devices without code modification.ö

It is indeed possible to construct a solution for prepaid billing scenarios using existing RADIUS attributes. The RADIUS server would send an Access-Accept message containing a Session-Timeout(27) and include a Termination-Action(29) in the RADIUS-request. Upon receiving the Access-Accept message, the NAS would meter the duration of the session and upon termination of the session the NAS

would generate an Access-Request message again. The RADIUS server would then re-authenticate the session and reply with an Access-Accept message indicating the amount of additional time in a Session-Timeout(27). Alternatively, it would responds with an Access-Reject message if there were no more resources in the userÆs account.

Moreover, if the user terminates the session prematurely, the NAS would recover any unused time from the accounting stream.

There are several problems with such a solution:

- It only supports time-based accounting. The solution presented in this document supports both time and volume based prepaid.

- Using accounting messages to recoup unused time may be problematic because RADIUS accounting messages are not delivered in real-time. A RADIUS server may store-and-forward accounting messages in batches. The solution presented in this document does not rely on Accounting Packets at all. It uses Access-Request, messages which do flow through any network in real-time. Delaying accounting messages may cause revenue leakage.

- Session-Timeout(27) is not a mandatory attribute. If a prepaid subscriber is being serviced by a NAS that does not adhere to Session-Timeout then that subscriber may use the service for an undetermined period of time.

- Termination-Action(29) presents its own issues. Firstly the behaviour of Termination-Action(29) is not mandatory. Secondly, according to RFC2865, Termination-Action fires when the provision of the service has completed. However, service should not be terminated when negotiating additional quota, because this should happen in a manner transparent to the subscriber. Because Termination-Action occurs when the Service is completed it is unclear whether or not user experience would be affected. The RADIUS server might even allocate a new IP address to the subscriberÆs device. Furthermore, the RADIUS server has no way of telling why the Access-Request message was generated. The RADIUS server might have to wait for the corresponding accounting packet to determine the reason for this Access-Request message. Finally, re-authenticating the subscriber may take too long. The solution presented in this document allows

quota replenishing to occur in an undisruptive manner from the user perspective. No re-authentication is required and quotas can be negotiated prior to the available credit running out.

- Due to the fact that the standard RADIUS attributes are not mandatory, the correct prepaid operation is really an act of faith on the part of the RADIUS server. If Session-Timeout(27) and/or Termination-Action(29) are not supported, the prepaid subscriber might be able to obtain the service for free. The solution described in this document requires that a prepaid-aware SAD informs the

RADIUS server, regardless of whether or not the latter supports the prepaid extensions. The RADIUS server can then determine whether or not service should be granted. For example, if a prepaid subscriber is connected to a NAS that does not support prepaid, the RADIUS server can either instruct the NAS to tunnel the traffic to another entity in the home network (e.g. the Home Agent) that supports prepaid, or it provide only a restricted service.]

The solution presented in this document requires the support of two mandatory and one optional attribute. Furthermore, it does not require a great amount of additional code at a NAS that already supports time or volume metering. The solution requires that RADIUS entities advertise their prepaid capabilities in an Access-Request and that they generate an Access-Request Authorize-Only packet to obtain more quota when or before the current quota is used up. It also requires the NAS to send an Access-Request with Authorize-Only when the session terminates in order to refund the subscriberÆs account appropriately.

The solution provided in this document is extensible. For example, the protocol can be extended to support tariff switching and other prepaid business models.

The extensions described in this document were designed based on a number of use cases and scenarios. An overview of these can be found in Appendix A.

3. Operations

3.1 General Requirements

3.1.1 Broker AAA Requirements

Broker AAA (BAAA) servers MUST support the Message-Authenticator(80) attribute as defined in [RFC2869]. If they are used, they forward the RADIUS packets as usual to the appropriate RADIUS servers.

Accounting messages are not needed to deliver a prepaid service. However, accounting messages can be used to keep the PPS up to date as to what is happening with the prepaid data session. Therefore, a BAAA SHOULD deliver RADIUS Accounting messages using the pass through mode described in [RFC2866].

3.2 Authentication and Authorization for Prepaid Enabled SADs

The SAD initiates the authentication and authorization procedure by sending a RADIUS Access-Request to the HAAA.

If the SAD has PPC capabilities, it MUST include the PPAC(TBD) attribute in the RADIUS Access-Request. The PPAC(TBD) attribute indicates to the PPS which prepaid capabilities are possessed by the SAD. These are required in order to complete the prepaid authorization procedure.

If the SAD supports the Disconnect-Message or the Change-of-Authorization capabilities, then it SHOULD include the Dynamic-Capabilities attribute.

In certain deployments, there may be other ways to terminate a data session, or change authorization of an active session. For example, some SADs provide a session termination service via Telnet or SNMP. In these cases, the AAA server MAY add the Dynamic-Capabilities message to the Access-Request. Upon receiving the Change-of-Authorization message, the AAA server would then be responsible for terminating the session using the means that are supported by the device.

If the authentication procedure involves multiple message exchanges (as in EAP), the SAD MUST include the PPAC(TBD) attribute and the Dynamic-Capabilities attribute (if used) in at least the last

Access-Request of the authentication procedure.

The Access-Request is sent as usual to the HAAA. The packet may pass through one or more BAAA.

Once the Access-Request arrives at the HAAA, the HAAA authenticates the subscriber. If this fails, the HAAA sends an Access-Reject message to the client. If authentication succeeds, the HAAA determines whether or not the subscriber is a prepaid subscriber. (How this is done is beyond the scope of this document.) If the subscriber is not a prepaid subscriber, then the HAAA responds as usual with an Access-Accept or an Access-Reject message. If the subscriber is a prepaid subscriber then the HAAA SHALL forward the Access-Request to the PPS for further authorization.

The Access-Request contains the PPAC(TBD) attribute and the Dynamic-Capabilities attribute if one was included. The User-Name(1) attribute MAY be set to a value that represents the subscriberÆs identifier. This attribute is used by the PPS to locate his account. For added security, the HAAA MAY also set the User-Password(2) attribute to the password used between the HAAA and the PPS.

The PPS locates the subscriberÆs account and authorizes him. During this procedure, the PPS takes into consideration the SAD PPC Capabilities.

Upon successful authorization, the PPS generates an Access-Accept containing the PPAC(TBD) attribute and the PPAQ(TBD) attribute.

The PPAC attribute returned to the client indicates the type of prepaid service to be provided for the session. The PPAQ(TBD) attribute includes the following.

- The QUOTA-ID, which is set by the PPS to a unique value that is used to correlate subsequent quota requests;

- Volume and/or Time quotas, which are set to values representing a portion of the subscribers credit;

- It MAY contain a Time or Volume Threshold that controls when the

SAD should request additional quota;

- The IP address of the Serving PPS and one or more alternative PPSs. This is used by the HAAA to route subsequent quota replenishing messages to the appropriate PPS(s).

Note: Idle-Timeout(28) can be used to trigger the premature termination of a prepaid service, for example as a result of inactivity.

Depending on site policies, after failed authorization, the PPS may generate an Access-Reject to terminate the session immediately. Alternatively, the PPS may generate an Access-Accept blocking some or all of the traffic and/or redirect some or all of the traffic to a location to a fixed server. (This feature could be used, for example, to prompt the user to replenish their account.) Blocking of traffic is achieved by either Filter-ID(11) or NAS-Filter-Rule(see

Redirect I-d). Redirection is achieved by sending Redirect-Id or Redirect-Rule, HTTP Redirection defined in the Redirect I-d. The time period before the session is blocked/redirected is specified by the Session-Timeout(27) attribute.

Upon receiving an Access-Accept from the PPS, the HAAA appends the usual service attributes and forward the packet to the SAD. The HAAA SHOULD NOT overwrite any attributes already set by the PPS. If the HAAA, receives an Access-Reject message, it will simply forward the packet to its client. Depending on site policies, if the HAAA does not receive an Access-Accept or an Access-Reject message from the PPS it MAY do nothing or send an Access-Reject or an Access-Accept message back to the PPC.

3.3 Session Start Operation

The start of the session is indicated by the arrival of an Accounting-Request(Start) packet. The Accounting-Request (Start) MAY be routed to the PPS such that it can confirm the initial quota allocation.

Note that the role of the PPS is not to record accounting messages and therefore it SHOULD not respond with an Accounting Response

packet.

If the PPS does not receive the Accounting-Request(start) message it will only know that the session has started upon the first reception of a quota replenishment operation.

If the PPS does not receive indication directly (via Accounting-Request(start)) or indirectly, it SHOULD after some configurable time, deduce that the Session has not started. If the SAD supports termination capabilities, the PPS SHOULD send a Disconnect Message to the SAD to ensure that the session is indeed dead.

3.4 Mid-Session Operation

During the lifetime of a prepaid data session the SAD requests the replenishment of the quotas using Authorize-Only Access-Request messages.

Once either the allocated quota has been exhausted or the threshold has been reached, the SAD MUST send an Access-Request with Servicetype(6) set to a value of ôAuthorize Onlyö and the PPAQ(TBD) attribute.

The SAD MUST also include NAS identifiers, and Session identifier attributes in the Authorize Only Access-Request. The Session Identifier should be the same as the one used during the Access-Request. For example, if the User-Name(1) attribute was used in the Access-Request it MUST be included in the Authorize Only Access-Request, especially if the User-Name(1) attribute is used to route the Access-Request to the Home AAA server.

The Authorize Only Access-Request MUST NOT include a User Password and MUST NOT include a Chap Password. In order to authenticate the message, the SAD MUST include a Message-Authenticator(80) attribute. The SAD computes the value for the Message-Authenticator according to [RFC2869].

When the HAAA receives the Authorize-Only Access-Request that contains a PPAQ(TBD), it SHALL validate the message using the Message-Authenticator(80) as per [RFC2869]. If the HAAA receives an

Authorize Only Access-Request that contains a PPAQ(TBD) but not a Message-Authenticator(80) it SHALL silently discard the message. An Authorize Only Access-Request message that does not contain a PPAQ(TBD) is either erroneous or belongs to another application (for example, a Change of Authorization message [RFC3576]). In this case the Authorize Only Access-Request is either silently discarded or handled by another application.

Once the Authorize Only Access-Request message is validated, the HAAA SHALL forward the Authorize Only Access-Request to the appropriate PPS. The HAAA MUST forward the Authorize Only Access-Request to the PPS specified in the PPAQ(TBD). The HAAA MUST add an Message-Authenticator(80) to the message, according to [RFC2869]. As with the Access-Request message, the HAAA MAY modify the User-Name(1) attribute such that it represents the userÆs internal prepaid account in the PPS. Note the PPS may also use the Quota-ID sub-attribute contained within the PPAQ(TBD) to locate the user account.

Upon receiving the Authorize Only Access-Request containing a PPAQ(TBD) attribute, the PPS MUST validate the Message-

Authenticator(80) as described in [RFC2869]. If validation fails, the PPS MUST silently discard the message. If it receives an Authorize Only Access-Request message that does not contain a PPAQ(TBD) it MUST silently discard the message.

The PPS locates the prepaid session state using the Quota Id contained within the PPAQ(TBD). The PPS takes the most recently allocated quota and subtracts it from the userÆs balance. If sufficient balance remains, the PPS authorizes the PPS and allocates additional quota. The PPS may also calculate a new threshold value.

Upon successful re-authorization, the PPS generates an Access-Accept containing the PPAQ(TBD) attribute. The Access-Accept message MAY contain Servicetype(6) set to Authorize-Only and MAY contain the Message-Authenticator(80).

Depending on site policies, upon unsuccessful authorization, the PPS generates an Access-Reject or an Access-Accept with Filter-Id(11) or Ascend-Data-Filter (if supported) attribute and the Session-Timeout(27) attribute such that the subscriber can get access to a restricted set of locations for a short period of time. This feature

could be used to enable users to replenish their accounts, create new accounts, or to browse free content.

Upon receiving the Access-Accept from the PPS, the HAAA SHALL return the packet to its client. If the HAAA receives an Access-Reject message, it forwards the packet. Depending on site policies, if the HAAA does not receive an Access-Accept or an Access-Reject message from the PPS it MAY do nothing or it MAY send an Access-Reject message back to its client.

Upon receiving an Access-Accept, the SAD SHALL update its quotas and threshold parameters with the values contained in the PPAQ(TBD) attribute. Note that the PPS MAY update the PrePaidServer attribute(s) and these may have to be saved as well.

Upon receiving an Access-Accept message that contains an Filter-Id(11), an Ascend-Data-Filter attribute, or Session Timeout(27), the SAD SHALL restrict the subscriber session accordingly.

3.5 Dynamic Operations

The PPS may take advantage of the dynamic capabilities that are supported by the SAD as advertised in the Dynamic-Capabilities attribute during the initial Access-Request.

There are two types of action that the PPS may perform. Firstly, it may request the session to be terminated. Secondly, it may request the attributes associated with the session to be modified. More specifically, it may modify a previously sent PPAQ(TBD)

Both of these actions require that the session be uniquely identified at the SAD. As a minimum the PPS MUST

- provide either the NAS-IP-Address(4) or the NAS-Identifier(32)
- provide at least one session identifier such as User-Name(1), Framed-IP-Address(), the Accounting-Session-Id(44).

Other attributes could be used to uniquely identify a prepaid data session.

3.5.1 Unsolicited Session Termination Operation

At anytime during a session the PPS may send a Disconnect Message in order to terminate a session. This capability is described in detail in [RFC3576]. The PPS sends a Disconnect Message that MUST contain identifiers that uniquely identify the data session and the SAD servicing that session.

If the SAD receives a Disconnect-Message, it responds with either a Disconnect-ACK message (if it is able to terminate the session) or with a Disconnect-NAK packet (otherwise).

Upon successful termination of a session the SAD MUST return any unused quota to the PPS by issuing an Authorize Only Access-Request containing the PPAQ which contains any unused Quota and the Update-Reason set to ôRemote Forced Disconnectö.

3.5.2 Unsolicited Change of Authorization Operation

At any time during the session the PPC may receive a Change of Authorization (CoA) message. A PPS may send a new Quota to either add or to remove quota that is allocated to the service.

If the Change of Authorization contains a PPAQ then that PPAQ overrides a previously received PPAQ. The PPS MUST NOT change the units used in the PPAQ.

If the newly received PPAQ reduces the amount of allocated quota beyond what is already used then the SAD accepts the new PPAQ and act as it normally would when the quota is used up. For example, if the threshold is reached then is request a quota update.

3.6 Termination Operation

The termination phase is initiated when (i) the subscriber logs off, (ii) the subscriberÆs balances is exhausted, or (iii) when the SAD receives a Disconnect Message.

In the case where the user logged off, or the SAD receives a Disconnect Message, the SAD sends an Authorize-Only Access-Request message with a PPAQ(TBD) and Update-Reason attribute set to either ôClient Service terminationö or ôRemote Forced disconnectö. This message indicates the already consumed quota.

In the case where the currently allocated quota is exhausted, if the PPAQ(TBD) contained Termination-Action field, the SAD follows the specified action (which would be to immediately terminate the service), requests more quota, or redirects/filters the service.

3.7 Mobile IP Operations

In roaming scenarios with Mobile-IP, the prepaid data session should be maintained transparently if the HA is acting as the SAD.

As the subscriber device associates with the new SAD (AP or PDSN that supports PPC capability), the SAD sends a RADIUS Access-Request and the subscriber is re-authenticated and reauthorized. The SAD MUST include the PPAC(TBD) attribute in the RADIUS Access-Request. In this manner the procedure follows the Authentication and Authorization procedure described earlier.

If the HA was acting as the SAD before handoff, the userÆs prepaid session does not undergo any change after the handoff because the Mobile IP session is anchored at the HA and the userÆs Home IP address remains the same.

In the case of a wireless access point or PDSN acting as the SAD it is likely that the userÆs IP address will change (Care of Address). The prepaid session will be affected by this. In this scenario the SAD shall send an Access-Request message which is routed to the home network and MUST reach the prepaid system that is serving this session. The prepaid system correlates the new authorization request with the existing active session and assigns a quota to the new request. Any outstanding quota at the old SAD MUST be returned to the prepaid system if the Mobile-IP nodes (HA and FA) support registration revocation (Mobile IPv4 only). Specifically, the quota SHOULD be returned when the SAD sends the Authorize Only Access-Request with PPAQ(TBD) Update-Reason set to either ôRemote Forced

disconnectö or ôClient Service terminationö. In order to trigger the sending of this last Authorize Only Access-Request, the prepaid system may issue a Disconnect Message [3576] to the SAD.

Even if the subscriber moves to a SAD that does not have prepaid capabilities can the prepaid data service continue. This can be done by requesting the Home Agent (assuming that has such capabilities) to take over the responsibilities of the SAD (i.e. metering). This scenario will be discussed in a later version of this document.

3.8 Operation considerations for Multiple prepaid services

This section describes the support for multiple prepaid services on a single SAD. Message flows illustrating the various interactions are presented at the end of this document.

A SAD that supports prepaid operations for multi-services SHOULD set the ôMulti-Services Supportedö bit in the PPAC.

When working with multi-services, we need to differentiate between the services. A Service-Id attribute is used in the PPAQ(TBD) to uniquely differentiate between the services. The exact definition of the Service-Id attribute is outside the scope of this document.

A PPAQ that contains a Service-Id is associated with that Service. A PPAQ that contains a Rating-Group-Id is associated with that Rating-Group. A PPAQ MUST not contain both a Rating-Group-Id and a Service-Id. A PPAQ that contains neither a Rating-Group-Id or a Service-Id applies to the ôAccess Serviceö.

3.8.1 Initial Quota Request

When operations with multi-services is desired, the SAD requests the initial quota for the Service by sending a PPAQ containing the Service-Id for that Service in an Authorize-Only Access-Request packet. Similarly, if the SAD supports Rating-Groups then it may request a quota for the Rating-Group by sending a PPAQ containing the Rating-Group-Id. In both cases the Update-Reason is set to ôInitial-Requestö.

The Authorize-Only Access-Request message may contain more than one PPAQ. The Authorize-Only Access-Request MUST includes one or more attributes that serve to identify the session so that it can be linked to the original authentication. Which Session Identifiers are included is up to specific deployments. The Authorize-Only message must contain the Message-Authenticator(80) attribute for integrity protection of the Authorize-Only Access-Request message.

Upon receiving an Authorize-Only Access-Accept message containing one or more PPAQs, the prepaid system allocates resources to each PPAQ. Each PPAQ is assigned a unique QID that MUST appear in subsequent PPAQ updates for that service or rating-group. Additionally, the PPAQ MUST contain the Service-ID or Group-ID, unless the PPAQ is a generic ôAccess Serviceö.

3.8.2 Quota Update

Once the services start to utilize their allotted quota they will eventually need to replenish their quotas (either the threshold is reached or no more quota remains). To replenish the quota the PPC sends an Authorize-Only Access-Request message containing one or more PPAQs. Each PPAQ MUST contain the appropriate QID, Service-ID or Group-ID (or neither the Service-ID or Group-Id if the quota replenishment is for the ôAccess Serviceö). The Update-Reason filed indicates either ôThreshold reachedö(3), or ôQuota reachedö(4). The Authorize-Only message must contain session identifiers.

Upon receiving an Authorize-Only Access-Request packet with one or more PPAQs the PPS responds with a new PPAQ for that service. The PPAQ contains a new QID, the Service-Id or Rating-Group-Id, a new Quota. If the PPS does not grant additional quota to the service it

MUST include the Termination-Action subfield in the PPAQ that will instruct the SAD what to do with the service.

3.8.3 Termination

When the allotted quota for a service is exhausted the SAD shall act in accordance to the Termination-Action field set in the Quota. If

the Termination-Action field is absent then the service MUST be terminated.

If the service is to be terminated then the SAD shall send a PPAQ with the appropriate QID, the Service-Id, the used quota, and Update-Reason set to ôClient Service Terminationö.

If the ôAccess Serviceö has terminated, then all other services must be terminated as well. In this case the SAD MUST report on all issued quotas for the various services. The Update-Reason field should be set to ôAccess Service Terminatedö.

3.8.4 Dynamic Operations

Dynamic operations for multi-services are similar to dynamic operations described for single service operations. The prepaid system may send a COA message containing a PPAQ for an existing service instance. The SAD matches the PPAQ with the service using the Service-ID attribute. The new quota could differ from the previously allocated value. The SAD must react to the new value accordingly.

A disconnect message terminates the ôAccess Serviceö. As such the SAD MUST report all unused quotas by sending an Authorize Only Access Request message containing a PPAQ for each active service. The Update-Reason shall indicate that the reason for the update.

3.8.5 Support for Resource Pools

If the PPC supports pools as indicated by setting the ôPools supportedö bit in the PPAC(TBD) then the PPS may associate a Quota with a Pool by including the Pool-Id and the Pool-Multiplier in the PPAQ(TBD).

When Resource Pools are used, the PPAQ must not use the threshold field.

3.8.6

One-Time-Charging

To initiate a One-Time charge the PPC includes the PPAQ attribute in an Access-Request packet. The Access Request packet MUST include a Message-Authenticator(80) and an Event-Timestamp(55) attribute.

The Service Id field of the PPAQ identifies the prepaid service. The amount to be charged is specified using the Resource Quota and Resource Quota overflow subtypes. If the value specified is negative then the resources are credited to the userÆs account.

The QID field MUST be set to a unique value and is used by the PPS to detect duplicates. The Update Reason field MUST be set to One-Time Charging.

Upon receiving a One-Time charge PPAQ, the RADIUS server authenticates the user and, if successful, passes the PPAQ to the PPS. The PPS locates the account and debits or credits it accordingly. The PPS MUST respond to the PPS with an Access-Accept message if successful, or an Access-Reject message otherwise.

The RADIUS server shall respond to the SAD with an Access Accept message. Since this is a one-time charge the SAD must not allow the session to continue. Therefore, the RADIUS server should include in the Access-Accept a Session-Timeout set to 0. Upon receiving an Access-Accept response the SAD shall generate an Accounting Stop message.

A PPAQ used for One-Time charging may appear in an Authorize-Only Access Request. This is the case when the session already exists. The PPS responds with an Access-Accept to indicate that the userÆs account has been debited or an Access-Reject otherwise.

3.8.7 Error Handling

If the PPS receives a PPAQ with an invalid QID it MUST ignore that PPAQ.

If the PPS receives a PPAQ containing a Service-Id, or a Rating-

Group-Id that it does not recognize, then it MUST ignore that PPAQ.

If the PPC receives a PPAQ containing a Service-Id, or a Rating-Group-Id that it does not recognize, then it must ignore that PPAQ.

If the PPC receives a PPAQ that contains a Pool-Id without a Pool-Multiplier or a Pool-Multiplier without a Pool-Id it must ignore that PPAQ.

3.9 Accounting Considerations

Although typically generated, accounting messages are not required to deliver a prepaid data service. When generated, accounting messages are used for auditing purposes and for billing.

Accounting messages associated with prepaid data sessions should include the PPAQ(TBD) attribute.

3.10 SAD Operation

To be completed

3.11 Interoperability with Diameter Credit Control Application

The RADIUS prepaid extensions need to interoperate with the Diameter protocol. Two possibilities exist: The AAA infrastructure is Diameter based and the SAD are RADIUS based, or the SAD is Diameter based and the AAA infrastructure is RADIUS based.

The Diameter Credit Control Application [DIAMETERCC] describes how to implement a prepaid accounting system using an Diameter based infrastructure.

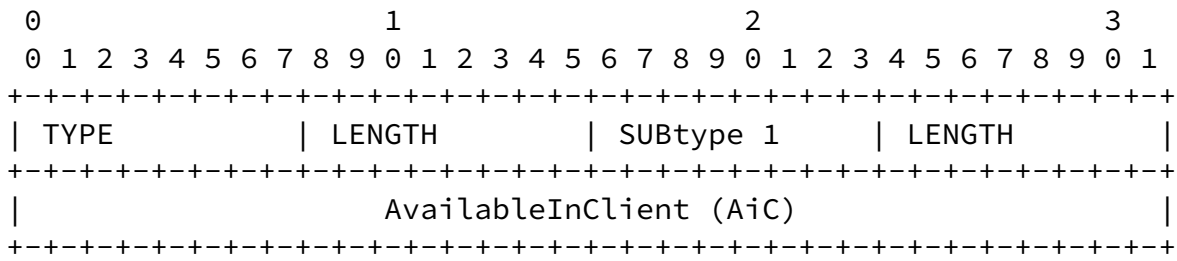
<This section to be completed.>

4. Attributes

This draft is using the RADIUS [RFC2865] namespace.

4.1
PPAC Attribute

The PrepaidAccountingCapability (PPAC) attribute is sent in the Access-Request message by a prepaid capable NAS and is used to describe the prepaid capabilities of the NAS. The PPAC is present in an Access-Accept message by the PPS to indicate the type of metering that is to be applied to this session.



TYPE : value of PPAC
LENGTH: 8
VALUE : String

The value MUST be encoded as follows:

Subtype (=1) : Subtype for AvailableInClient attribute
Length : Length of AvailableInClient attribute
(= 6 octets)
AvailableInClient (AiC):

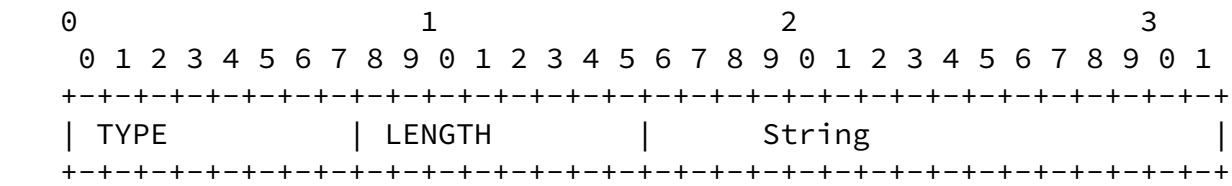
The optional AvailableInClient Subtype, generated by the PPC, indicates the metering capabilities of the NAS and shall be bitmap encoded. The possible values are:

0x00000001 Volume metering supported.
0x00000002 Duration metering supported.
0x00000004 Resource metering supported.
0x00000008 Pools supported
0x00000010 Rating groups supported
0x00000020 Multi-Services supported.
0x00000040 Tariff Switch supported.

Others Reserved

4.2
Session Termination Capability

The value shall be bitmap encoded rather than a raw integer. This attribute shall be included RADIUS Access-Request message to the RADIUS server and indicates whether or not the NAS supports Dynamic Authorization.



Type : value of Session Termination Capability
Length: = 4
String encoded as follows:

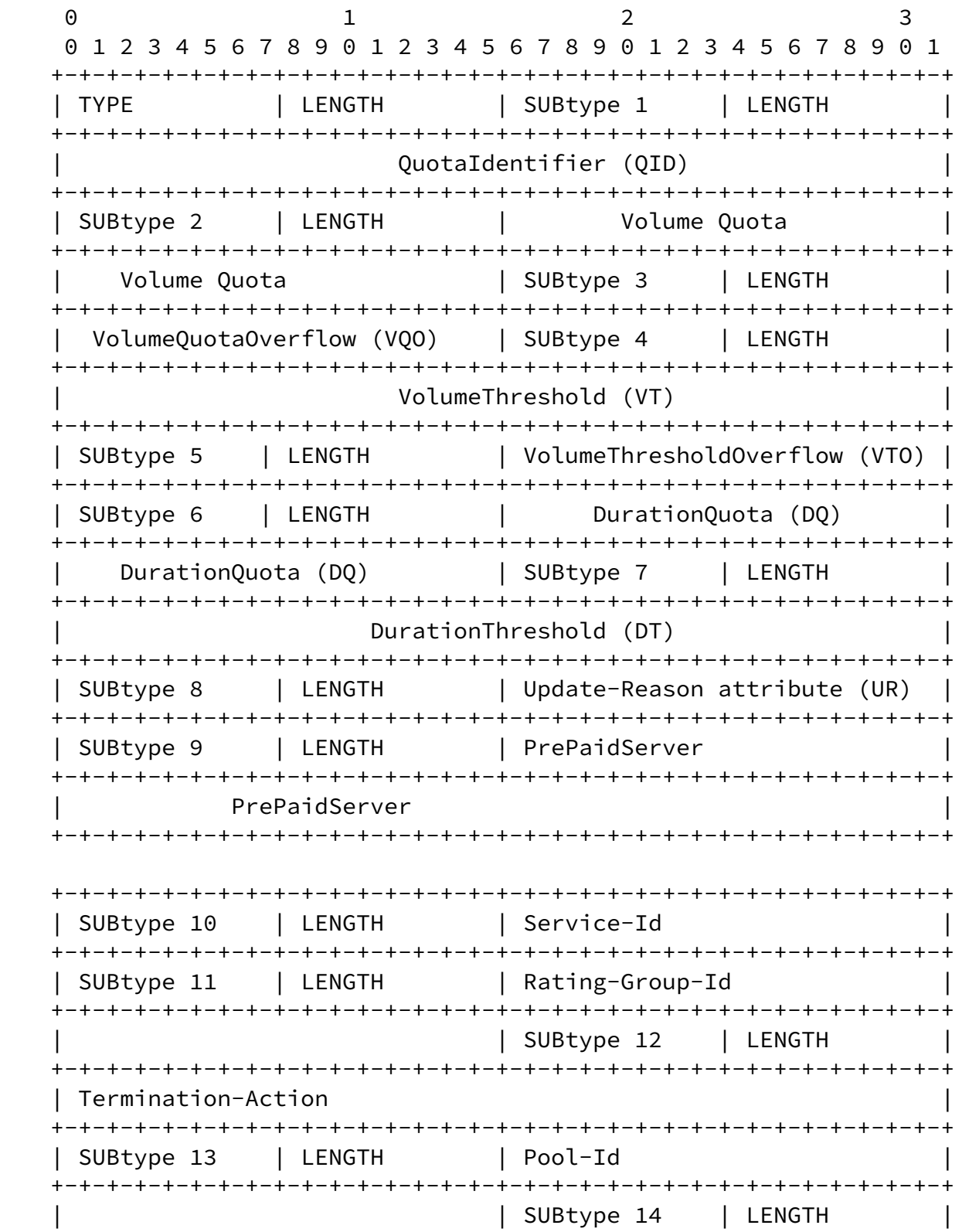
0x00000001 Dynamic Authorization Extensions (rfc3576) is supported.

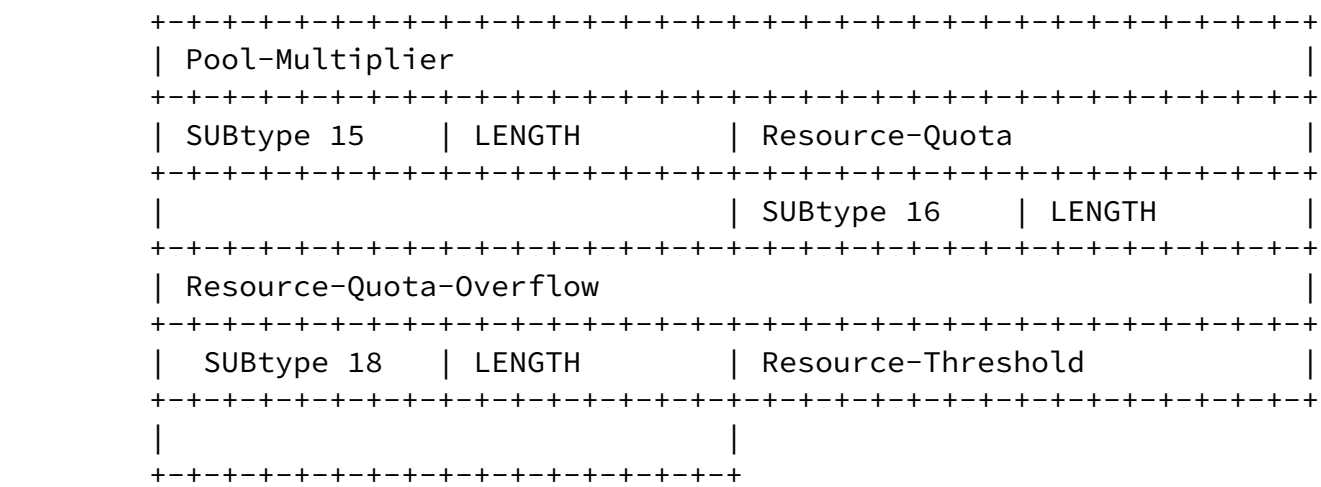
4.3
PPAQ Attribute

One or more PPAQ(TBD) attributes are sent in an Access Request, Authorize Only Access-Request and Access-Accept messages. In an Access Request message, the PPAQ attribute is used to facilitate One-Time charging transactions. In Authorize Only Access-Request messages it is used for One-Time charging, report usage and the request for further quota. It is also used to request prepaid quota for a new service instance. In an Access-Accept message it is used to allocate the (initial and subsequent) quotas.

When multiple services are supported, a PPAQ is associated with a specific service as indicated by the presence of a Service-Id, a Rating-Group-Id, or the ôAccess Serviceö (as indicated by the absence of a Service-Id and a Rating-Group-Id).

The attribute consists of a number of subtypes. Unused subtypes are omitted from the message.


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
TYPE
LENGTH
SUBtype 1
LENGTH
QuotaIdentifier (QID)
SUBtype 2
LENGTH
Volume Quota
Volume Quota
SUBtype 3
LENGTH
VolumeQuotaOverflow (VQO)
SUBtype 4
LENGTH
VolumeThreshold (VT)
SUBtype 5
LENGTH
VolumeThresholdOverflow (VTO)
SUBtype 6
LENGTH
DurationQuota (DQ)
DurationQuota (DQ)
SUBtype 7
LENGTH
DurationThreshold (DT)
SUBtype 8
LENGTH
Update-Reason attribute (UR)
SUBtype 9
LENGTH
PrePaidServer
PrePaidServer
SUBtype 10
LENGTH
Service-Id
SUBtype 11
LENGTH
Rating-Group-Id
SUBtype 12
LENGTH
Termination-Action
SUBtype 13
LENGTH
Pool-Id
SUBtype 14
LENGTH



Type : Value of PPAQ
Length: variable, greater than 8

String: The String value MUST be encoded as follows:

Subtype (=1): Subtype for QuotaIDentifier attribute
Length   : Length of QuotaIDentifier attribute (= 6 octets)

QuotaIDentifier (QID):

The QuotaIDentifier subtype is generated by the PPS together with the allocation of a Volume or Duration Quota. The on-line quota update RADIUS Access-Request message sent from the SAD to the PPS shall include a previously received QuotaIDentifier.

Subtype (=2): Subtype for VolumeQuota attribute
Length   : length of VolumeQuota attribute (= 6 octets)

VolumeQuota (VQ):

The optional VolumeQuota subtype is only present if Volume Based charging is used. In a RADIUS Access-Accept message (PPS to SAD direction), it indicates the Volume (in octets) allocated for the session by the PPS. In RADIUS Authorize Only Access-Request message (SAD to PPS direction), it indicates the total used volume (in octets) for both forward and reverse traffic.

Subtype (=3): Subtype for VolumeQuotaOverflow

Length : length of VolumeQuotaOverflow attribute (= 4 octets)

VolumeQuotaOverflow (VQO):

The optional VolumeQuotaOverflow subtype is used to indicate how many times the VolumeQuota counter has wrapped around 2^32 over the course of the service being provided.

Subtype (=4): Subtype for VolumeThreshold attribute
Length : length of VolumeThreshold attribute (= 6 octets)

VolumeThreshold (VT):

The VolumeThreshold Subtype shall always be present if VolumeQuota is present in a RADIUS Access-Accept message (PPS to SAD direction). It is generated by the PPS and indicates the volume (in octets) that shall be consumed before a new quota should be requested. This threshold should not be larger than the VolumeQuota.

Subtype (=5): Subtype for VolumeThresholdOverflow
Length : Length of VolumeThresholdOverflow attribute
(= 4 octets)

VolumeThresholdOverflow (VTO):

The optional VolumeThresholdOverflow subtype is used to indicate how many times the VolumeThreshold counter has wrapped around 2^32 over the course of the service being provided.

Subtype (=6): Subtype for DurationQuota attribute
Length : length of DurationQuota attribute (= 6 octets)

DurationQuota (DQ):

The optional DurationQuota Subtype is only present if Duration Based charging is used. In RADIUS Access-Accept message (PPS to SAD direction), it indicates the Duration (in seconds) allocated for the session by the PPS. In on-line RADIUS Access-Accept message (PPC to PPS direction), it indicates the total Duration in seconds) since the start of the accounting session related to

the QuotaID.

Subtype (=7): Subtype for DurationThreshold attribute
Length : length of DurationThreshold attribute (= 6 octets)

DurationThreshold (DT):

The DurationThreshold subtype shall always be present if DurationQuota is present in a RADIUS Access-Accept message (PPS to SAD direction). It represents the duration (in seconds) after which new quota should be requested. This threshold should not be larger than the DurationQuota.

Subtype (=8): Subtype for Update-Reason attribute
Length : length of Update-Reason attribute (= 4 octets)

Update-Reason attribute (UR):

The Update-Reason subtype shall be present in the on-line RADIUS Access-Request message (SAD to PPS direction). It indicates the reason for initiating the on-line quota update operation. Update reasons 4, 5, 6, 7 and 8 indicate that the associated resources are released at the client side, and therefore the PPS shall not allocate a new quota in the RADIUS Access_Accept message.

1. Pre-initialization
2. Initial Request
3. Threshold Reached
4. Quota Reached
5. Remote Forced Disconnect
6. Client Service Termination
7. ôAccess Serviceö Terminated
8. Service not established
9. One-Time Charging

Subtype (=9) : Subtype for PrePaidServer attribute
Length : Length of PrePaidServer
(IPv4 = 6 octets, IPv6= 18 octets

PrePaidServer:

The optional, multi-value PrePaidServer attribute indicates the

address of the serving prepaid system. If present, the Home RADIUS server uses this address to route the message to the serving PPS. The attribute may be sent by the Home RADIUS server.

If present in the incoming RADIUS Access-Accept message, the PDSN shall send this attribute back without modifying it in the subsequent RADIUS Access-Request message, except for the first one. If multiple values are present, the PDSN shall not change their order.

Subtype (=10) : Subtype for Service ID
Length : Length of Service ID

Service-Id:

Opaque string that uniquely describes a service instance to which prepaid metering should be applied. A Service-Id could be an IP 5-tuple (source address, source port, destination address, destination port, protocol). If Service-ID is present in the PPAQ the PPAQ refers to that service. If a PPAQ does not contain a Service-Id then the PPAQ refers to the Access Service.

Subtype (=11) : Subtype for Rating-Group-Id
Length : 6

Rating-Group-Id

Identifies that this PPAQ is associated with resources allocated to a Rating Group with the corresponding ID.

Subtype (=12) : Subtype for Termination-Action
Length : 6

This field is an enumeration of the action to take when the PPS does not grant additional quota. Valid actions are as follows:

0 Reserved
1 Terminate
2 Request More Quota
3 Redirect/Filter

Subtype (=13) : Pool-Id

Length : 6

Identifies the Pool that this quota is to be associated with.

Subtype (=14) : Pool-Multiplier
Length : 6

The pool-multiplier determines the weight that resources are inserted into the pool and the rate at which resources are taken out of the pool by this service or Rating-Group.

Subtype (=15) : Subtype for Resource-Quota
Length : 6

The optional Resource-Quota subtype is only present if Resource Based or one-time charging is used. In the RADIUS Access-Accept message (PPS to SAD direction) it indicates the Resources allocated for the session by the PPS. In RADIUS Authorize Only Access-Request message (SAD to PPS direction), it indicates the resources used in total, including both incoming and outgoing chargeable traffic. In one-time charging scenarios, the subtype represents the number of units to charge or credit the user.

Subtype (=16) : Subtype for Resource Quota Overflow
Length : 6

Subtype (=18) : Subtype for ResourceThreshold
Length : 6

NOTES:

Volume-Quota, Time-Quota, or Resource-Quota MUST appear in the attribute. If Volume Quota appears, Volume Threshold may also appear.

A PPAQ MUST NOT contain both a Service-Id and a Rating-Group-Id.

A PPAQ that does not contain a Service-ID or a Rating-Group-Id applies to the ôAccess Serviceö.

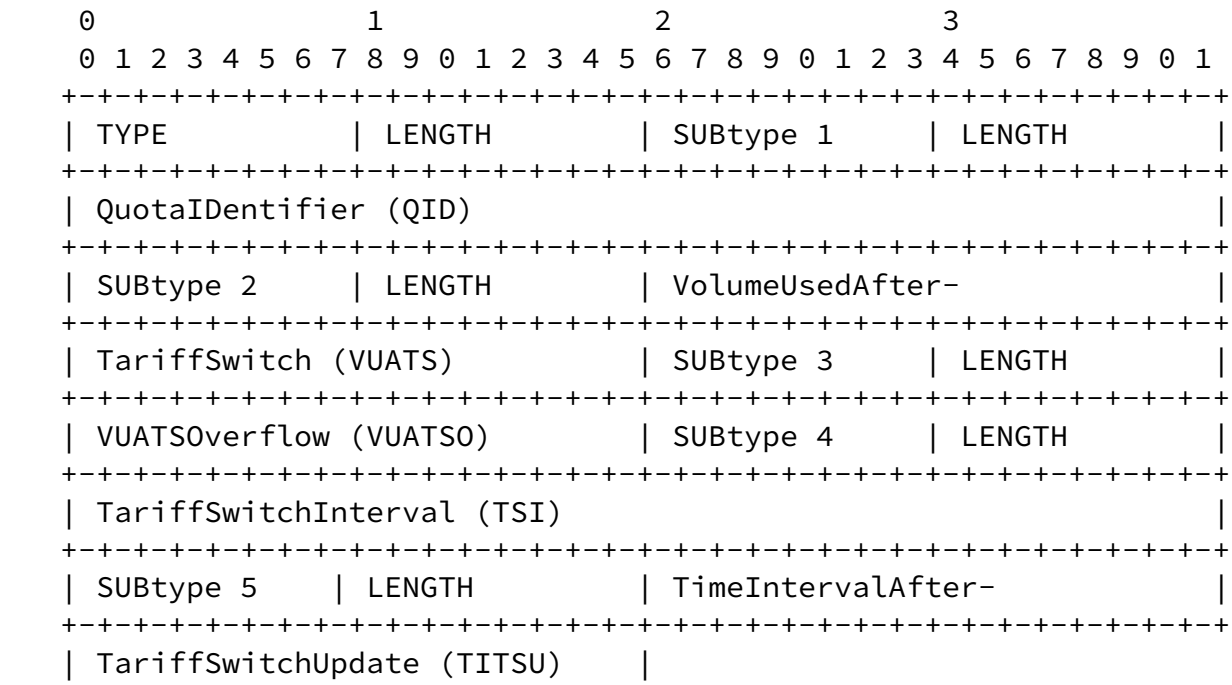
When the PPAQ contains a Pool-Id it MUST also contain the Pool-Multiplier.

4.4 Prepaid Tariff Switching (PTS)

This specification defines the PTS attribute to allow for changeovers from one rate to another during service provision.

Support for tariff switching is OPTIONAL for both PPC and PPS. PPCs use the flag "Tariff Switching supported" of the AvailableInClient subtype of the PPAC attribute to indicate support for tariff switching. PPSs employ the PTS attribute to announce their support for tariff switching. Details of this will be specified after the format of the PTS attribute has been defined.

If a RADIUS message contains a PTS attribute, it MUST also contain at least one PPAQ attribute. If a RADIUS Access-Request message contains a PTS attribute or a "Tariff Switching supported" flag, it MUST also contain an Event-Timestamp RADIUS attribute (see [RFC2869]).



```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type : Value of PTS
Length: variable, at least 8

Subtype (=1): QuotaIDentifier (QID)
Length : Length of QuotaIDentifier Subtype (= 6 octets)

The QID subtype MUST be present in each PTS attribute. In an online RADIUS Access-Request message sent from the PPC to the PPS, its value MUST be a quota identifier received previously from the PPS and MUST be the same as a quota identifier of one of the PPAQ attributes included the same RADIUS message.

A PPAQ attribute that is transported along with a PTS attribute and has the same quota identifier value as the PTS attribute in its own QID subfield shall be referred to as "accompanying PPAQ attribute". If a PPS receives an Access-Request message from a PPC, it associates a unique quota identifier to this request. Thus, a quota identifier also identifies a particular service.

Subtype (=2): VolumeUsedAfterTariffSwitch (VUATS)
Length : Length of VolumeUsedAfterTariffSwitch Subtype (= 6 octets)

The VolumeUsedAfterTariffSwitch subtype SHALL be used in online RADIUS Access-Request messages (PPC to PPS direction). It indicates the volume (in octets) used during a session after the last tariff switch for the service specified via the QID subfield and the accompanying PPAQ attribute (see the remarks under "Subtype 1: QID").

Subtype (=3): VUATSOverflow (VUATSO)
Length : Length of VUATSOverflow Subtype (= 4 octets)

If an online RADIUS Access-Request message contains a VUATS subfield and if the VolumeUsedAfterTariffSwitch has wrapped around 2^32 over the course of provisioning the service

identified via the QID subfield, then the VUATSO subfield MUST be present in the PTS attribute. In this case, it indicates how many times the VolumeUsedAfterTariffSwitch has wrapped around 2^32. In all other cases, the VUATSO subfield MUST NOT be present in the PTS attribute.

Subtype (=4): TariffSwitchInterval (TSI)
Length : Length of TSI Subtype (= 6 octets)

The TSI subtype MUST be present in each PTS attribute that is part of a RADIUS Access-Accept message (PPS to PPC direction). It indicates the interval (in seconds) between the value of Event-Timestamp RADIUS attribute (see [RFC2869]) of the corresponding RADIUS Access-Request message and the next tariff switch condition.

Subtype (=5): TimeIntervalafterTariffSwitchUpdate (TITSU)
Length : Length of TITSU Subtype
(= 6 octets)

The PPS MUST include the TITSU subtype if there is another tariff switch period after this period. The TITSU attributes encodes the number remaining seconds of current tariff period. If this attribute is zero or omitted, it is assumes that the current tariff period lasts until further notice. If TITSU is specified, the PPC must send a quota update before the current period ends.

If a RADIUS message contains a PTS attribute, it MUST also contain at least one PPAQ attribute. The PTS is associated with the PPAQ by the QID. If multiple services are supported and if the PPAQ is associated with a service as indicated by the Service-Id sub-atrribute of the PPAQ, then the PTS refers to the tariff switch for that service. If the PPAQ does not have a Service-Id, then the PTS refers to tariff switch for the Access-Service.

If a PPC supports tariff switching then it MUST set the 0x00000040 (Tariff switching supported) flag of the AvailableInClient subtype of the PPAC attribute that is contained in the Access-Request packet

starting the session.

4.5 Table of Attributes

TO BE COMPLETED.

Request	Accept	Reject	Challenge	#	Attribute
Authorize_Only	Request	Accept	Reject		

5. Security Considerations

The extended RADIUS protocol described in this document is subject to a number of potential attacks, in a manner similar to the RADIUS without these extensions. It is recommended that IPsec be employed to protect against certain of the attacks.

If IPsec is not available, usage of the extensions described in this document improve the overall security of RADIUS. The various security enhancements are explained in the following sections.

5.1 Authentication and Authorization

RADIUS is susceptible to replay attacks during the Authentication and Authorization procedures. A successful replay of the initial Access-Request could result in an allocation of an initial quota.

To thwart such an attack...

5.2 Replenishing Procedure

A successful replay attack of the Authorize Only Access-Request could deplete the subscribers prepaid account.

To be completed.

6. IANA Considerations

This document requires the assignment of new Radius attributes type numbers for the following attributes:

1) Prepaid-Accounting-Capability (PPAC)
   with subtype:
   AvailableInClient

2) Prepaid-Accounting-Operation (PPAQ)
   with subtypes:
   QuotaID (QID)

   VolumeQuota (VQ)
   VolumeQuotaOverflow (VQO)
   VolumeTreshold (VT)
   VolumeTresholdOverflow (VTO)
   DurationQuota (DQ)
   DurationTreshold (DT)
   UpdateReason (UR)
   PrePaidServer (PPS)
   ServiceID (SID)
   RatingGroupId (RGID)
   TerminationAction (TA)
   PoolID (PID)
   PoolMultiplier (PM)
   Cost (COST)
   TariffChangeTime (TCT)

3) Prepaid-Tariff-Switch (PTS)

4) Session-Termination-Capability (STC)

5) International-Mobile-Subscriber-Identity (IMSI)

7.

Normative References

[RFC2026] Bradner, S., "The Internet Standards Process -- Revision 3", RFC 2026, October 1996.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997.

[RFC2865] Rigney, C., Rubens, A., Simpson, W. and S. Willens, "Remote Authentication Dial In User Server (RADIUS)", RFC 2865, June 2000.

[RFC2866] Rigney, C., "RADIUS Accounting", RFC 2866, June 2000.

[RFC2869] Rigney, C., Willats, W., Calhoun, P., "RADIUS Extensions", RFC 2869, June 2000.

[RFC2868] Zorn, G., Leifer, D., Rubens, A., Shriver, J.,

Holdrege, M., Goyret, I., "RADIUS Attributes for Tunnel Protocol Support" , RFC 2868, June 2000.

[RFC3576] Chiba, M., Dommety, G., Eklund, M., Mitton, D., Aboba, B., "Dynamic Authorization Extensions to Remote Authentication Dial-In User Service (RADIUS)", RFC 3576, February 2003.

[RFC3748] Aboba, B., et al., "Extensible Authentication Protocol", RFC 3748, June 2004.

8. Informative References

[DIAMETERCC] Hakkala, H., et al., "Diamter Credit-Control Application", Internet Draft, AAA WG, April 2004, Work in Progress.

[REDIRECT] "RADIUS Redirection", Internet Draft, Work in progress.

9.

Call Flows

This section describes the flows associated with various scenarios that are mentioned in this document. The following fields are used in the call flows:

RADIUS packets:

AR	Access Request
ARA	Access Accept
AC	Accounting Requests
A	Authorize-Only Access-Request
AA	Access-Accept for Authorize-Only Access-Request

RADIUS Attributes:

PPAQ	PPAQ as defined in this specification
SID	One or more attributes representing the Session that the RADIUS packets is correlated to.
PPAC	PPAC as defined in this specification
ASID	Acct-Session-Id as defined by RADIUS
MSID	Acct-Multi-Session-Id as define by RADIUS

PPAQ fields:

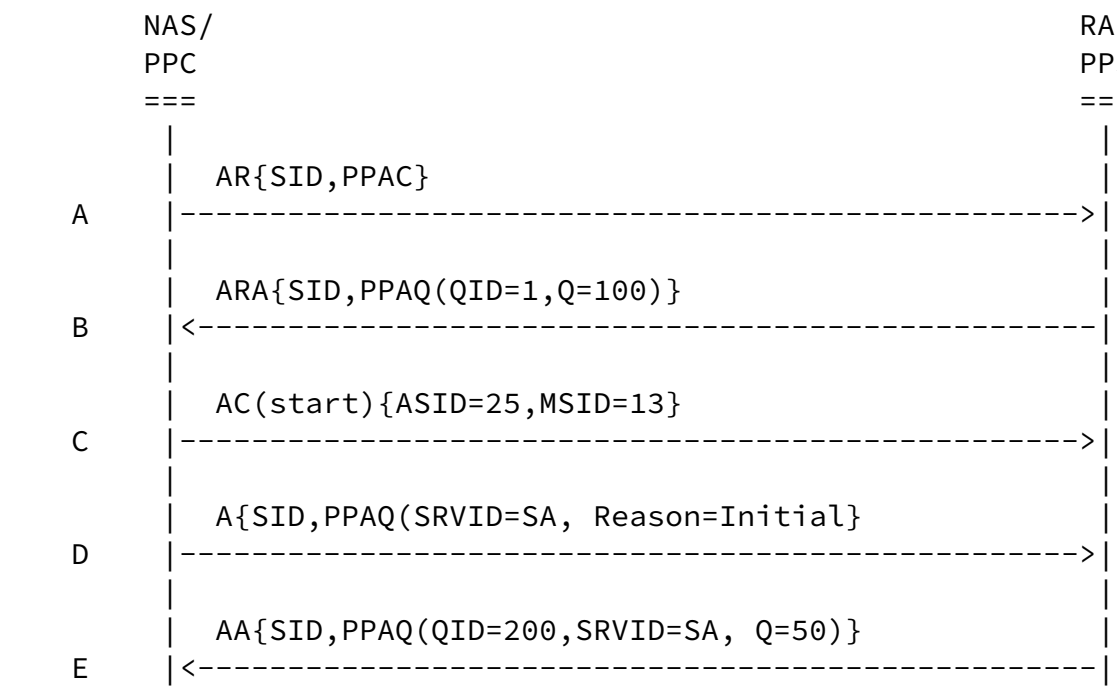
SRVID	Service-Id
Reason	Update-Reason
QID	Quota-Id

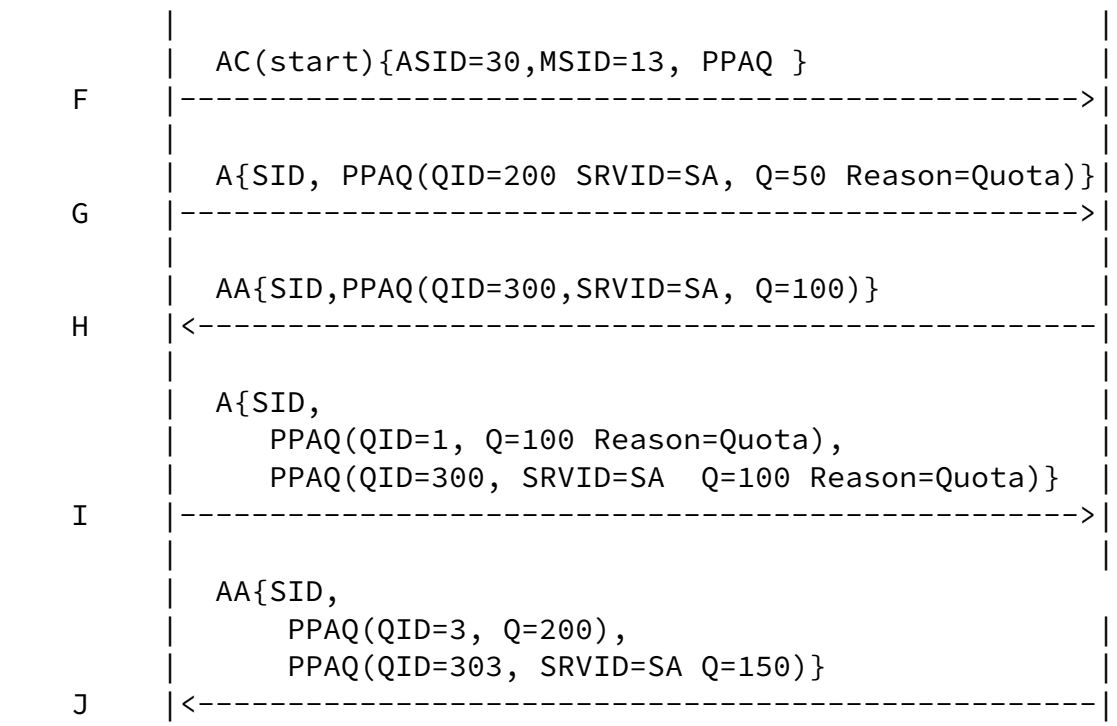
9.1 Simple Concurrent Services

In this scenario the PPC authenticates and authorizes the user. The PSS responds with Quota for the ôAccess Serviceö instance. The NAS

then request quota for Service-A.

Accounting is turned on.





A This is the initial Access-Request that indicates the prepaid capabilities of the NAS. In this example indicates that Concurrent Sessions are supported. Access-Request also includes SID (Session Id) which is the Session Identifier assigned by this NAS to session. The formal of the session identifier is outside the scope of this document.

B RADIUS authenticates the user and determines that he has a prepaid account. RADIUS responds with a PPAQ for the ôAccess Serviceö (PPAQ does not contain a Service-ID or Rating-Group-ID). The PPAQ has a QID=1 assigned by the Prepaid System and Quota of Q=100. The quota could be time or volume and may or may not have a threshold associated with it.

C The NAS starts the Access Service and generates an Accounting-Request (Start) message as normal. It includes the Acct-Session-Id and may include the Acct-Multi-Session-Id.

D The NAS is about to start a new Service, call it Service-A. It sends an Authorize-Only access request to RADIUS. The SID links this Authorize-Only access request to the initial Authentication & Authorization (Step-A and Step-B).The Authorize-Only message contains a PPAQ requesting quota for Service-A, Update-Reason = Initial-Request.

E The PPS checks the resources available to the user and assigns 50 units (time/volume etc) to this service. RADIUS sends an Access Accept message contain a PPAQ assigning quota Q=50 for Service-A. The PPAQ contains a QID = 200.

F The NAS starts Service-A and sends an Accounting-Request (Start) message for that service. Acct-Multi-Session-Id can be used to tie all of the sessions in the accounting streams together.

G Quota for Service-A requires refreshing, the quota was completely used). An Authorize-Only message is sent containing a PPAQ with QID = 200 which corresponds to the prior QID received for this service. Note QID is sufficient for the PPS server to link this request to the previous request and hence to the original authentication steps. Therefore SID is not really required. The PPAQ will report the used part of the quota (50 units).

H RADIUS deducts the used quota from the users accounts and reserves 50 more additional units for a total quota of 100 (Q=100) for Service-A. It sends back a PPAQ with QID=300.

I NAS needs to refresh both the ôAccess Serviceö and Service-A. It sends an Authorize Only message contain two PPAQs, one for the Main Service with QID=1 and one for Service-A with QID=300. Each PPAQ reports the resources that were consumed so far and the reason why the update is being sent.

J RADIUS responds back with two PPAQs. The PPAQ without the Service-Id grants an additional 100 units for a total of 200 units to the ôAccess Serviceö û QID=3; the other PPAQ, containing SRVID=SA grants an additional 50 units for a total quota to service-a of 150 units û QID=303.

This step illustrates why SRVID needs to be specified in the PPAQ. Without it the NAS would be unable to differentiate between the PPAQs. QIDs are not sufficient to correlate the PPAQ to a service since they may be changed by the PPS at every transaction.

Note how each PPAQ attribute represents a sequential conversation about a service between the PPC and the PPS in this example. The links between the messages are the QIDs and the Service-Ids.

Also note that a SID is needed to tie the Authorize-Only messages to the Authentication steps. This SID is only really needed the first time a PPAQ is sent.

Although accounting messages have an Accounting-Session-ID, that is not enough to enable the back end system to associate that accounting message with a particular Service. We therefore need the PPAQ in the accounting message.

9.2 One-time Charging

In this One-time charging example, the PPC authenticates and authorizes the user and requests charging for a service event requested by the user. The PPC already knows the price to charge for the service event identified by SRVID=SA.

Contributor

We would like to thank Hannes Tschofenig for his contributions to this draft.

Acknowledgments

The authors would like to thank Mark Grayson (Cisco), Nagi Jonnala and Tseno Tsenov for their contribution to this draft.

Author's Addresses

Avi Lior
Bridgewater Systems
303 Terry Fox Drive
Suite 100
Ottawa Ontario
Canada
avi@bridgewatersystems.com

Parviz Yegani, Ph.D.
Mobile Wireless Group
Cisco Systems
3625 Cisco Way
San Jose, CA 95134
USA
pyegani@cisco.com

Kuntal Chowdhury
Starent Networks
30 International Place, 3rd Flr
Tewksbury, MA 01876
kchowdhury@starentnetworks.com

Hannes Tschofenig
Siemens
Otto-Hahn-Ring 6
81739 Munich
Germany

hannes.tschofenig@siemens.com

Christian Guenther
Siemens
Otto-Hahn-Ring 6
81739 Munich
Germany
christian.guenther@siemens.com

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the IETF's procedures with respect to rights in IETF Documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE

REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Expiration Date

This memo is filed as draft-lior-radius-extensions-for-prepaid-06.txt, and will expire 20 July, 2005.

10. Appendix A û use cases

In this appendix we present a set of use cases and scenarios based on which the extensions in this document were designed. It is assumed that the subscriber possesses a valid prepaid account with a service provider, for example a WLAN operator.

In order to maintain generality, the use cases refer to the communications between the SAD and the network. The connection between the UserÆs Device and the SAD, which typically involves setting up a layer 2 session, e.g. a PPP session or a GPRS PDP Context, is specific to a given network technology and the details do not affect the operation of the prepaid service.

10.1 Simple prepaid use case

A subscriber connects to his home network. As usual, the Access Device that is servicing the subscriber uses the AAA infrastructure to authenticate and authorize the subscriber.

The SAD sends a RADIUS Access-Request to the AAA server in order to authenticate and authorise the subscriber with respect to the

requested service. The Access-Request contains the subscriber credentials and may contain the prepaid capabilities of the SAD. Prepaid capabilities MUST be included if the SAD supports them.

The AAA System proceeds with the authentication procedure. This may involve several message exchanges such as in EAP [RFC2284]. Once the subscriber has been authenticated, the AAA system determines that the subscriber is a prepaid subscriber and requests authorisation. The request MUST include the prepaid capabilities of the serving SAD.

The system validates that the subscriber has a prepaid account and

that the account is active. It further validates that the SAD has the appropriate prepaid capabilities. If all is in order, the prepaid system authorises the subscriber to use the network. Otherwise it rejects the request. The decision is sent to the AAA system. The response includes attributes to indicate the allocation of a portion of the subscriberÆs credit. This portion is called the ôinitial quotaö (in units of time or volume) and optionally a threshold value.

A portion only of the userÆs funds is allocated because the user may be engaged in other services that may draw on the same account. For example, the user may be engaged in a data session and a voice session. Although these two services would draw from the same account, they form separate parts of the overall system. If the entire quota was allocated to the data session then the user would have no more funds for a voice session.

The AAA system incorporates the attributes received from the prepaid System into an Access-Accept message that it sends to the SAD. Note that the AAA system is responsible for authorizing the service whereas the prepaid system is responsible for prepaid authorization.

Upon receiving the Access-Response, the SAD starts the prepaid data session and meters the session based on time or volume, as indicated in the message.

Once the usage for the session approaches the allocated limit (as expressed by the threshold), the SAD will request additional quota. Re-authorization for additional quota flows through the AAA system to the prepaid System. The prepaid System revalidates the subscriberÆs account and subtracts the previously allocated quota

from the current balance. If there is remaining balance, it reauthorizes the request with an additional quota allotment. Otherwise, the prepaid System rejects the request. Note the replenishing of the quotas is a re-authorization procedure and does not require the subscriber to authenticate himself again.

It is important to note that the prepaid System is maintaining session state for the subscriber. This state includes how much account balance was allocated during the last quota enquiry and how much is left in the account. Therefore, it is required that all messages about the session reach the same (and correct) prepaid

system.

Upon receiving a re-allotment of the quota, the SAD continues to provide the data service until the new threshold is reached. If the request for additional quota cannot be fulfilled then the SAD lets the subscriber use the remaining quota and terminates the session.

Alternatively, instead of terminating the session, the SAD may restrict the data session such that the subscriber can only reach a particular web server. This web server maybe used to allow the subscriber to replenish their account. This restriction can also be used to allow new subscribers to set up prepaid accounts in the first place.

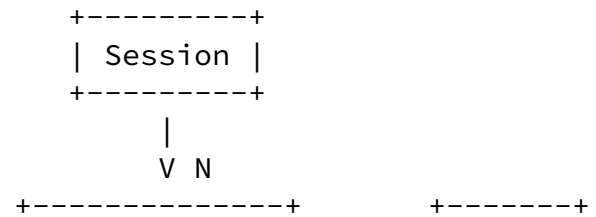
Should the subscriber terminate the session before the quota is exhausted, the remaining balance allotted to the session MUST be refunded into the subscriberÆs account.

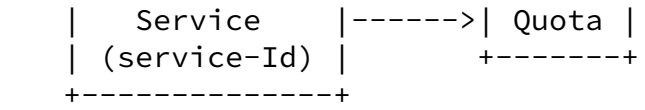
While the Access Device is waiting for the initial quota, the subscriber may have dropped the connection/session. The entire allocated quota MUST be credited back to the subscribers account in this case.

10.2 Support for Multi-Services

Examples of services that the user may be using are browsing the web, participating in a VoIP conversation, watching streaming video and downloading a file. Some operators may want to distinguish between these services. Some services are billed at different rates and services may be metered differently. Therefore, the prepaid solution needs to be able to distinguish services, and allocate

quotas to the services using different units (e.g. time, volume) and allow for those quotas to be utilized at different rates.



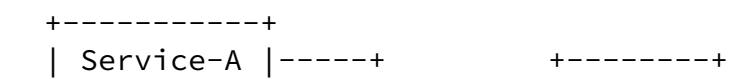


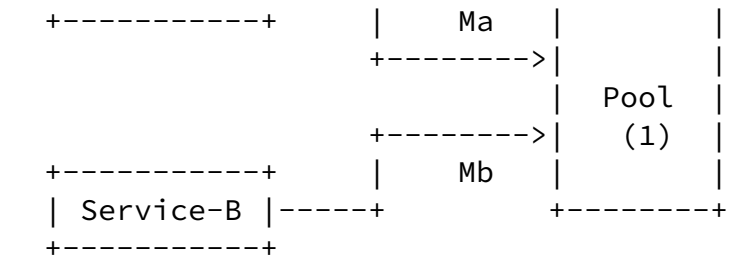
As shown in the above diagram, a Session may be associated with multiple (N) services. Each service is identified by a Service-ID. The format of the Service-ID is not in the scope of this document but the Service-ID could be expressed as an IP flow using the 5-tuple {Source-IP and Port, Destination-IP and Port, protocol type}. Each service is allocated an appropriate quota metric.

10.3 Resource Pools

When working with multiple services a new problem arises because one service may utilize its quota faster than another service. When the userÆs balance is close to exhaustion, a situation could arise where one service is unable to obtain quota while another service has plenty of quota remaining. Unless the quotas can be rebalanced, the SAD would then have to terminate that service. Indeed, even before that happens, the services could generate an excessive amount of traffic as the they update their quotas.

One method to solve these problems is to utilize resource pools. Resource pools enable the allocation of resources to several services of a session by allocating resources to a pool and have services draw their quota from the pool at a rate appropriate to that service. When the quota allocated to the pool is close to exhaustion, the entire pool is replenished.





As the figure above shows, Service-A and Service-B are bound to Pool(1). Ma and Mb are the pool multipliers (that are associated with Service-A and Service-B respectively) that determine the rate at which Service-A and Service-B draw from the pool.

The pool is initialized by taking the quota allocated to each service and multiplying it by Mn. Therefore, the amount of resources allocated to a pool is given by:

```
Poolr = Ma*Qa + Mb*Qb + . . .
```

A Pool is empty if:

```
Poolr <= Ca*Ma + Cb*Mb + . . .
```

where:
Ca,Cb are the consumed resources of Service-A and Service-B respectively.

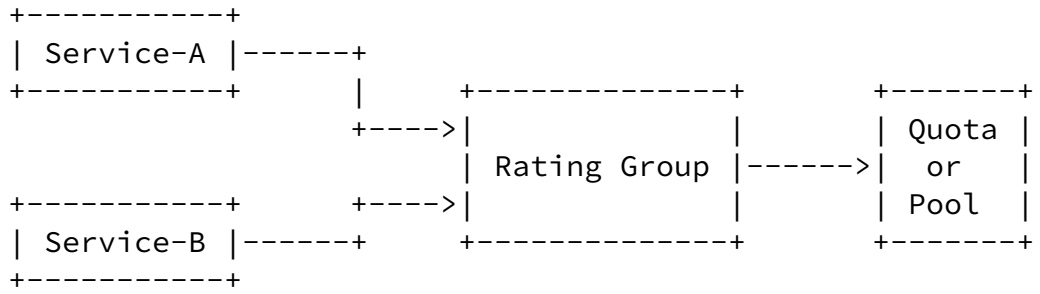
Note that the resources assigned to the pool are not associated with a metric. That is, Service-A can be rated at $1 per Mbyte and Service-B can rated at $0.10 per Minute. In this case if we allocate $5 worth of resources on behalf of service-A to the pool we would set Ma = 10 and place 50 units into the pool. If we allocate $5 on behalf of Service-B to the Pool, then M=1 and place 50 units into the Pool. The pool would have a total sum of 100 units to be shared between the two services. Each Mbyte used by Service-A will draw 10 units from the pool and each minute used by Service-B will draw 1 unit from the pool.

10.4 Support for Complex Rating Functions

The rating of a service can be quite complex. While some operators follow linear charging models, others may wish to apply more complex

functions. For example, a service provider may wish to rate a service such that the first N Mbytes are free, then the next M Mbytes are rated at $1 per Mbyte and volume above M bytes be rated at $0.50 per Mbyte. Such a function could be implemented by repeated message exchanges with the prepaid system.

To avert the need to exchange many messages while still supporting such complex rating functions the notion of a ôRating Groupö is introduced. A Rating Group is provisioned at the SAD. As illustrated in the figure below, a Rating Group is associated with one or more services and defines the rate that the services associated with the Rating Group consume the quota.



During consumption of a service that is associated with a Rating Group, the PPC sends the ID of the Rating Group to the PPS. The prepaid service authorizes the Rating Group by allocating a quota to it and optionally assigning it to a Resource Pool.

When service that belongs to an authorized Rating Group is instantiated, the PPC does not need to authorize this service. This limits the amount of traffic between the PPC and the PPS.

10.5 One-Time-based Charging

One-Time-based Charging is used for charging of service events without an ongoing session. That is, the service is provisioned instantaneously, as far as charging is concerned. An example of such an event is the purchase of a ring-tone. Subscription based services can also be modeled as a One-Time event. In this case the one-time service event is the purchase of a subscription

For a given user, one-time-based charging may occur in parallel with other charging models. For example, the subscriber may access a website which is metered (based on time or volume) while he also

purchase the right to use a ring tone (a one-time-based event). Note: it is up to the service providers to decide whether or not the user will be charged for the download of the tone and also be

charged for the time and volume required to download the ring-tone. The facilities provided by this document gives the service provider the capability to achieve their service charging business goals. For example, should the service provider choose not to charge for the download volume or time, then they can treat the download IP flow as a separate service that is exempt from charging.

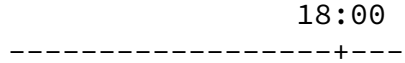
The SAD signals one-time-based charging to the PPS with an indication that identifies the service and the units that need to be debited from the userÆs account.

One-time-based charging may occur under two conditions: the (a) SAD may not have a authenticated context (or access to an authenticated context) for the subscriber), or (b) the SAD has access to authenticated context for the subscriber. In the former case the SAD will have to authenticate the subscriber. For example, the user maybe authenticated by the SAD providing access service. However when the user accesses the subscription server to purchase a subscription, the subscription server may not have access to the authentication context of the subscriber and thus will have to authenticate the subscriber from scratch. Authentication of the subscriber and the generation of the one-time charging event will happen in conjunction.

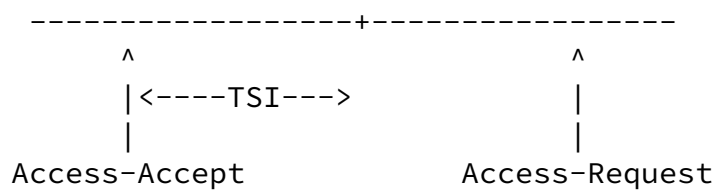
Note that one-time-based charging can also be used to credit the prepaid userÆs account. For example, the SAD can return resources to the subscriber by issuing a one-time charge request that includes the amount of resources to be credited into the account.

10.6 Support for Tariff Switching

The PPC and the PPS may support tariff switching as described earlier. For example, as shown in the figure below, traffic before 18:00 may be rated at ær1Æ and traffic after 18:00 hours is rated at ær2Æ. The PPC reports usage before and after the switch occurs. Tariff switching only makes sense for volume based metering where the volume is billed at different rates.



r1 | r2

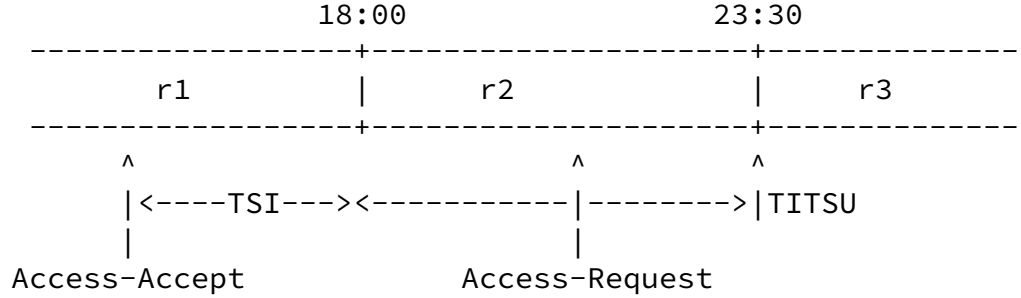


The PPC it indicates support for tariff switching by setting the appropriate bit in the PPAC. If the PPS needs to signal a tariff switch time it will send a PTS attribute which indicates the point in time when the switch will occur. This indication represents the number of seconds from current time (TarrifSwitchInterval TSI).

At some point after the tariff switch the PPC sends another Access-Request, as a result of either the user having logged off or the volume threshold being reached. The PPC reports how much volume was used using the PPAQ in total and how much volume was used after the tariff switch using the PTSÆs VUATS subtype.

If the PPC sends this message before the tariff switch, the PPS will respond with another PTS where the TSI is appropriately updated.

In situations with multiple tariff switches, as shown below, the PPS MUST specify the length of the tariff switch period using the TimeIntervalAfterTariffSwitchUpdate (TITSU) in the PTS attribute.



When a TITSU is specified in the PTS, the PPC MUST generate an Access-Request within the time after TSI and before TITSU expires. Note that, typically, the PPC will be triggered by the Volume Threshold. However, it is possible that, during period r2, insufficient traffic is generated and thus the threshold is not reached. Even in this case PPC MUST generate an Access-Request in

good time. Also note that separate services flows may have individual tariff periods.

10.7 Support for Roaming

In certain networks it is essential for prepaid data services to be available to roaming subscribers. Support for both static and dynamic roaming models is needed. In a static roaming scenario the subscriber connects to a foreign network which has a roaming agreement either directly with the home network, or through a broker network. When the subscriber logs into another foreign network, a new login procedure has to be executed.

In a dynamic roaming scenario the subscriber may move between networks while maintaining his connection. In such a scenario the data session is seamlessly handed off between the networks.

In both roaming scenarios, the subscriber always authenticates himself to the home network. Authorization for the prepaid session and quota replenishing occurs at the home network and more specifically at the prepaid system where state is being maintained.

Dynamic roaming is challenging because a subscriber who established a prepaid data session may move to another Access Device that does not support the prepaid functionality. Even in this case the system should be able to continue the prepaid session.

10.8 Termination of a prepaid session

When fraud or an error is detected, the either only the affected session, or all sessions of the affected subscriber should be terminated.

It may happen that the prepaid system enters a state where it is unclear whether or not the data session is in progress. Under such a condition, the system may wish to terminate the session in order to make sure that the user is not billed for this potential inactivity.

Certain handoff procedures used in dynamic roaming scenarios require that the system terminates the subscribers prepaid data session at a SAD. This is the case, for example, when time-based prepaid is used and the mobile subscriber performs a dormant handoff.

10.9 Querying and Rebalancing Prepaid Resources

It should be possible for the PPS to Query the current resource consumption at a SAD and adjust the userÆs account balance.

For example, a request to the PPS is made (e.g. a one-time charging event) but the userÆs account is depleted but resources have been allocated to the SAD. The PPS should have the ability to query the SAD and if it has the spare resources to reassign the quotas to the SAD and to the pending request. Note that the PPS doesnÆt know resource usage until the SAD request for more resources. This can be a long time.

In the absence of this capability the PPS can minimize the effect of this phenomenon by allocating small quotas û a practice that results in more message exchanges.