Network Working Group
INTERNET-DRAFT
Category: Informational
draft-lior-radius-prepaid-extensions-01.txt
Expires: 30 December 2003

A. Lior
Bridgewater Systems
P. Yegani
Cisco
K. Chowdhury
Nortel
L. Madour
Ericsson Canada
Y. Li
Bridgewater Systems

June 30, 2003

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

Status of this Memo

Copyright Notice

Abstract

The draft presents an extension to the Remote Authentication Dial-In User Service (RADIUS) protocol to support PrePaid data services for a wide range of deployments such as Dial, Wireless, WLAN. Consideration for roaming using mobile-ip is also given.

Table of Contents

1. Introduction

This draft describes RADIUS protocol extensions supporting PrePaid Data Services.

PrePaid data services are cropping up in many wireless and wireline based networks. A PrePaid Data Service subscriber is one that purchases a contract to deliver a data service for either a period of time, or a quantity of data. The subscriber purchases the Data Service using various means such as buying a PrePaid Card, or online. How the subscriber purchases his PrePaid Data Service depends on the deployment and is not in scope for this document.

In some deployments, the PrePaid data service will be combined with a PrePaid voice service. This is not an issue for this document other than the fact that the PrePaid Data Services described in this paper should work with other PrePaid data services.

The fundamental business driver for a carrier to provide PrePaid data services is to increase participation (subscriber base) and thus to increase revenues. Therefore, it makes sense that PrePaid services meet the following goals:

- Leverage existing infrastructure, hence reducing capital expenditures typically required when rolling a new service;
- Protect against revenue loss;
- Protect against fraud;
- Be as widely deployable over Dialup, Wireless and WLAN networks.

The protocol described in this document maximizes existing infrastructure as much as possible û hence the use of the RADIUS protocol. The protocol is used in ways to protect against revenue loss or revenue leakage. This is achieved by allocating small quotas to each data session and having the ability to update the quotas dynamically during the lifetime of the PrePaid data session. As well, mechanisms have been designed to be able to recover from errors that occur from time to time.

Protection against fraud is provided by recording of accounting records, by providing mechanisms to thwart replay attacks. As well,

mechanisms have been provided to terminate data sessions when fraud is detected.

PrePaid System will become more prevalent and sophisticated as the various networks such as Dialup, Wireless and WLAN converge. This protocol extension is designed to meet the challenges of converged networks.

The draft mainly addresses how to use the RADIUS protocol to achieve a PrePaid Data Service. The details of the PrePaid System, such as its persistent store, its rating capabilities, how it maintains its accounts are not covered at all. However, in order to define the RADIUS protocol extensions it is necessary to discuss the functional behavior of the PrePaid System.

1.1 Terminology

Access Device
PrePaid Client
PrePaid Server
Home agent (HA)
Home network
Home AAA (HAAA)
Broker AAA (BAAA)
Visited AAA (VAAA)
Foreign Agent (FA)
WLAN

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. Use-cases

In this section we present a set of use cases that will help establish the requirements needed to deliver PrePaid data services. These use cases donÆt address how the PrePaid account is established

or maintained. It is assumed that the PrePaid subscriber has obtained a valid account from a service provider such as a wireless operator or a WLAN operator.

To make the document as general as possible, the use cases cover the experience from the Access Device and not from the UserÆs Device. The connection between the UserÆs Device, which typically involves setting up a PPP session is specific to a given network technology and the details are not required to deliver a PrePaid service.

2.1 Simple use-case

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

The Access Device sends a RADIUS Access-Request to the AAA system to authenticate the subscriber, and identify and authorize the service. The Access-Request includes the subscriberÆs credentials and may include the PrePaid capabilities of the Access Device. PrePaid capabilities will be included if the Access Device supports PrePaid functionality..

The AAA System proceeds with the authentication procedure. This may involve several transactions such as in EAP. Once the subscriber has been validated, the AAA system determines that the subscriber is a PrePaid subscriber and requests that the PrePaid System authorize the PrePaid subscriber. The request may include the PrePaid Capabilities of the serving Access Device.

The PrePaid System will validate that the subscriber has a PrePaid Account; it will validate that the Account is Active; and will validate that the Access Device has the appropriate PrePaid capabilities. If all is in order, the PrePaid System will authorize the subscriber to use the network. Otherwise it will reject the request. The response is sent back to the AAA System. The response includes attributes such as, an allocation of a portion of the subscriberÆs account called the initial quota (in units of time or volume) and optionally a threshold value.

In order to support concurrent PrePaid sessions, at any time, the

PrePaid System allocates a portion of the subscribers account to a given PrePaid session. For example, the subscriber may be on a PrePaid voice call and may also have a concurrent PrePaid data session. Throughout the lifetime of a session the Access Device will request quota updates from the PrePaid System.

The AAA system incorporates the PrePaid attributes received from the PrePaid System with the service attributes into an Access Response message that it sends back to the Access Device. Note the AAA System is responsible for authorizing the service whereas the PrePaid System is responsible for PrePaid authorization.

Upon receiving the Access Response, the Access Device allows the PrePaid data session to start and it starts to meter the session based on time or volume.

Once the usage for the session approaches the allotted quota (as expressed by the threshold), the Access Device will, as instructed by the PrePaid System, request an additional quota. The re-authorization for additional quota flows through the AAA system to the PrePaid System. The PrePaid System revalidates the subscriberÆs account; it will subtract the previous quota allocation from the userÆs balance and if there is a balance remaining it will reauthorize the request with an additional quota allotment. Otherwise, the PrePaid System will reject the request. Note the replenishing of the quotas is a re-authorization procedure and does not involve re-authentication of the subscriber.

It is important to note that the PrePaid System is maintaining session state for the subscriber. This state includes how much was allocated during the last quota allocation for a particular session and how much is left in the account. Therefore, it is required that all subsequent messages about the PrePaid session reach the correct PrePaid System.

Upon receiving a re-allotment of the quota, the Access Device will, continue the data service session until the new threshold is reached. If the Access Device receives a rejection, then it will let the subscriber use up the remaining quota and then terminate the session.

Alternatively, instead of terminating the session, the Access Device 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 purchase a PrePaid Service.

2.2 Quota Recovery

In the above scenario, should the subscriber terminate the session before the session the quota is used up, the remaining balance allotted to the session must be credited back to the subscriberÆs account.

As well, while the Access Device is waiting for the initial quota, the subscriber may have dropped the session. The initial quota must be credited back to the subscribers account.

2.3 Support for concurrent PrePaid sessions

The subscriber at any given time may initiate more than one session. To support concurrent sessions the PrePaid System allocates a portion of the account to any given session at any given time.

Each session is treated independently.

2.4 Support for Roaming

For some networks it is essential that PrePaid Data Services be offered to roaming subscribers. Support for static and dynamic roaming models are needed. Static roaming is where the subscriber logs onto a foreign network. The foreign network has a roaming agreement directly with the home network or through a broker network or networks. The subscriber remains logged into the network until the subscriber changes location. When changing location a new connection and a new login procedure is required.

Dynamic roaming allows to subscriber to move between foreign networks while maintaining a connection with the home network seamlessly. As the subscriber moves between networks, the data session is handed off between the networks.

In both roaming scenarios, the subscriber always authenticates with the home network. PrePaid authorization and quota replenishing for the session need to be received at the home network and more specifically at the PrePaid System where state is being maintained.

Dynamic roaming is particularly challenging. A subscriber that established a PrePaid Data Session may roam to another Access Device that doesnÆt not support PrePaid functionality. The system should be capable to continue the PrePaid session.

2.5 PrePaid termination

When fraud is detected by the PrePaid System, or when an error is detected, it may be beneficial for the PrePaid system to terminate a specific session for the subscriber or all the sessions of a subscriber.

Some errors can occur such that the PrePaid System is in a state where it is not sure whether the session is in progress or not. Under conditions such as this, the PrePaid system may wish to terminate the PrePaid data session to make sure that resources are not being utilized for which it canÆt charge for reliably.

Some handoff procedure used during dynamic roaming may require that the PrePaid system explicitly terminate the subscribers PrePaid data session at an Access Device. For example, if time based PrePaid service is being used and the mobile subscriber performs a dormant handoff, the PrePaid System needs to explicitly terminate the PrePaid session at the old Access Device.

3. Architecture

A PrePaid Data Service deployment consists of Access Devices, AAA servers, and PrePaid Servers. The subscriber device is not implicated in the delivery of PrePaid Data Services. In mobile-ip, the Home Agent may also be implicated in delivering a PrePaid Data Service.

In order to be have as general a solution as possible, in this paper we generalize the Access Devices, which in reality may be a NAS from in Dialup deployments, PDSN in CDMA2000 deployments or an 802.11

WLAN Access Point. To actively participate in PrePaid procedures outlined here, the Access Device MUST have PrePaid Client capabilities. PrePaid Client Capabilities include the ability to meter the usage for a PrePaid data session; this usage includes time or volume usage. An exception to this rule is during dynamic roaming scenarios, where the Access Device can relegate its PrePaid Client Capabilities to the Home Agent (HA). Furthermore, the Access Device may also have Dynamic Session Capabilities that include the ability to terminate a data session and/or change authorization attributes associated with a specific data session by processing Disconnect Messages and Change of Authorization messages as per [CHIBA].

In this document the AAA server uses the RADIUS protocol. There are three kinds or categories of AAA servers. The AAA server in the home network, the HAAA, is responsible for authentication of the subscriber and also authorization of the service. In addition, the HAAA communicates with the PrePaid servers using the RADIUS protocol to authorize PrePaid subscribers. In roaming deployments the AAA server in the visited network, the VAAA, is responsible for forwarding the RADIUS messages to the HAAA. The VAAA may also modify the messages. In roaming deployments, the visited network may be separated from the home network by one or more broker networks. The AAA servers in the broker networks, BAAA are responsible for the routing of the RADIUS message to the HAAA.

The PrePaid Server is described in functional terms related to itÆs interface with the HAAA. The PrePaid Server maintains the accounting state of the PrePaid subscribers. As well, the PrePaid Server maintains state for each active PrePaid data service session. This state includes, allocated quotas, the last known activity counters (time or volume) for the PrePaid subscriberÆs data session and the servicing Access Device. These counters are continuously being updated during the lifetime of the PrePaid data service.

The various deployments scenarios for PrePaid are presented in the remainder of this section. The first deployment is the basic PrePaid data service and is depicted in figure 1. Here the Access Device and the HAAA and the PrePaid Server are collocated in the same operator network.

The Subscriber Device establishes a connection with one of several Access Devices in the network. The Access Device communicates with one or more HAAA servers in the network. To provide redundancy more then one HAAA is available to use by an Access Device.

The network will have one or more PrePaid Servers. Multiple PrePaid Servers will be used to provide redundancy and load sharing. The interface between the HAAA and the PPS is the RADIUS protocol in this specification. 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 whatever protocol is used between the HAAA and the PPS.

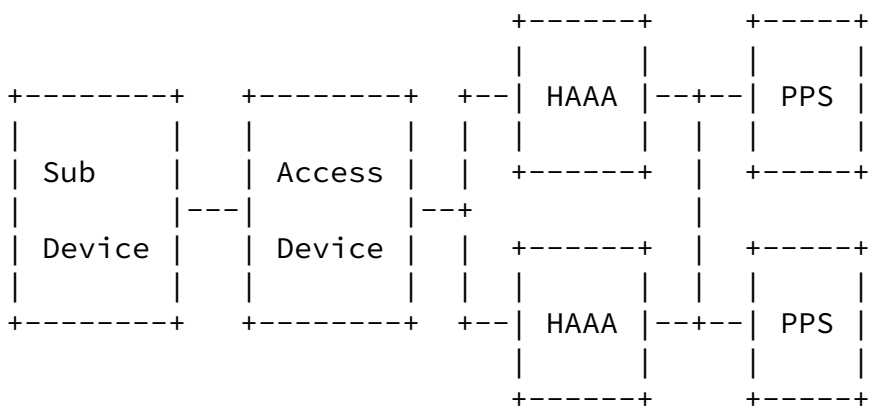
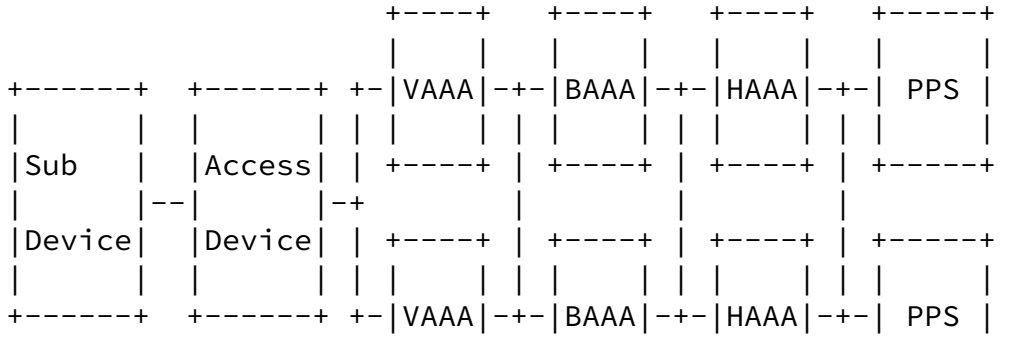


Figure 1 Basic PrePaid Architecture

The following figure shows a static roaming PrePaid architecture that is typical of a wholesale scenario for Dial-Up users or a broker scenario used in Dial-Up or WLAN roaming scenarios.



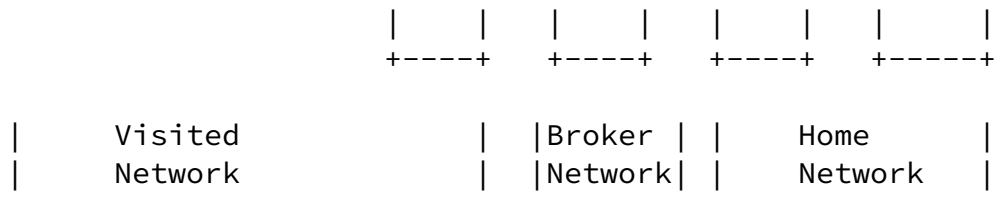
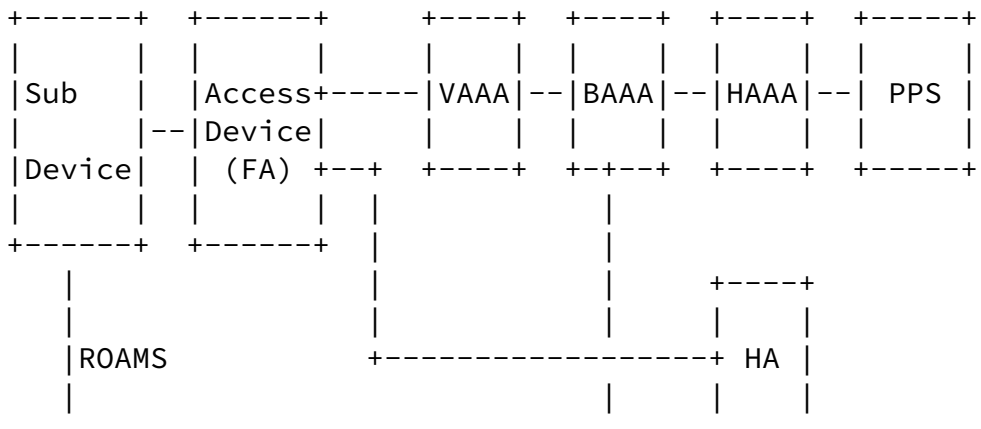


Figure 2 Static Roaming PrePaid Architecture

As in the basic PrePaid architecture the subscriberÆs device establishes a connection with the Access Device (NAS, WLAN Access Point). The Access Device communicates with the Visiting AAA server (VAAA) using the RADIUS protocol. Again for redundancy there maybe more then one VAAA. The VAAA communicate using the RADIUS protocol with AAA servers in the broker network (BAAA). There maybe more then one Broker Network between the Visited Network and the Home

Network. The Home Network is the same as in the simple architecture.

To support dynamic roaming the network will most likely utilize mobile-ip. Figure 3 illustrates a typical mobile-ip deployment. Note that typically the mobile device would be moving between networks that use the same technology such as Wireless or WLAN. Increasingly, device will be able to roam between networks that use different technology such as between WLAN and Wireless and Broadband. Fortunately, mobile-ip can address this type of roaming and therefore we need not be concerned with the underlying network technology.



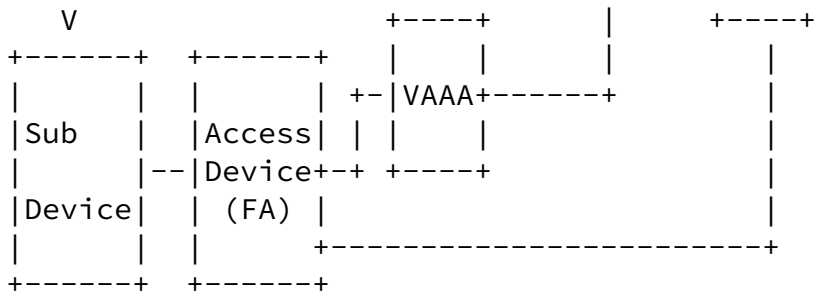


Figure 3 Roaming using mobile-ip

In the figure 3, the Subscriber device establishes a PrePaid session between the Access Device in the foreign network, which has PrePaid capabilities and the Home Agent (HA). The setup for this service is identical to the cases covered above. Notice that the Access Device is known as the Foreign Agent (FA). As the subscriber device moves to another network it establishes a connection with another Access

Device in another foreign network. The PrePaid data service should continue to be available. When a device associates to another Access Device it MUST re-authenticate at the new Access Device and de-associate or logoff the old Access Device. Furthermore, any unused quota at the old Access Device MUST be promptly credited back to the subscribers account. The reason we say promptly, is because if the subscriber is very low on resources to start with, the subscriber may not have enough resources to log on to the new Access Device. The speed at which resources can be returned depend on the type of handoff procedure that is used: dormant handoff vs. active handoff vs. fast handoff.

As well, notice that if the Access Devices could communicate with each other then there could be a way to accelerate a faster handoff procedure. In particular, it could accelerate the return of the unused portion of the quotas from the old Access Device.

Unfortunately, standards are evolving with each network technology creating their own scheme to make the handoff procedures more efficient.

4. Operations

4.1 General Requirements

4.1.1 Broker AAA Requirements

Broker AAA servers MUST support the Message-Authenticator(80) attribute as defined in [RFC2869]. If BAAA servers are used, the BAAA servers function is to 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 PrePaid Server current as to what is happening with the PrePaid data session. Therefore, BAAA SHOULD deliver RADIUS Accounting messages using the pass through mode described in [RFC2866].

4.2 Authentication and Authorization

The Access Device initiates the authentication and authorization procedure by sending a RADIUS Access-Request as usual.

If the Access Device has PrePaid Client capabilities, it MUST include the PPCC attribute in the RADIUS Access-Request. The PPCC attribute indicates to the PrePaid server the PrePaid capabilities possessed by the Access Device. These are required in order to complete the PrePaid authorization procedures.

If the Access Device supports the Disconnect-Message or the Change-of-Auhtorization capabilities, then it SHOULD include the Dynamic-Capabilities attribute.

In certain deployments, there may be other ways in which to terminate a data session, or change authorization of an active session. For example, some Access Devices 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.

If the authentication procedure involves multiple Access-Requests (as in EAP), the Access Device MUST include the PPCC attribute and the Dynamic-Capabilities attribute (if used) in at least the last

Access-Request of the authentication procedure.

The Access-Request will be sent as usual to the HAAA. The packet may be proxied through zero or more BAAA.

Once the Access-Request arrives at the HAAA, the HAAA will authenticate the subscriber. If the subscriber is not authenticated, the HAAA will send an Access-Reject message back to the client. If the subscriber is authenticated, the HAAA will determine whether or not the subscriber is a PrePaid subscriber. The techniques used to determine whether or not a subscriber is a PrePaid subscriber is beyond the scope of this document. If the subscriber is not a PrePaid subscriber, then the HAAA will respond as usual with an Access-Accept or Access-Reject message. If the subscriber is a PrePaid Subscriber the HAAA SHALL forward the Access-Request to a PrePaid server for further authorization.

The Access-Request will contain the PPCC attribute, the Dynamic-Capabilities attribute if one was included; the User-Name(1) attribute MAY be set to a value that would represent the SubscriberÆs PrePaid Identity. This attribute is used by the PrePaid server to locate the PrePaid SubscriberÆs account. For

added security, the HAAA MAY also set the User-Password(2) attribute to the password used between the HAAA and the PrePaid server.

The PrePaid server lookups the subscriberÆs PrePaid account and will authorize the subscriber taking into consideration the Access Device PrePaid Client Capabilities.

Upon successful authorization, the PrePaid server will generate an Access-Accept containing the PPAQ attribute, which contains the following sub-attributes:

- The QUOTA-Id which is set by the PrePaid server to a unique value that is used to correlate subsequent quota requests;

- Volume and/or Time Quotas, one of which is set to a value representing a portion of the subscribers account;

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

Access Device requests additional quota;

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

Depending on site policies, upon unsuccessful authorization, the PrePaid server will generate an Access-Reject or an Access-Accept and set the Filter-Id(11) or the Ascend-Data-Filter (if supported) attribute and the Session-Timeout(27) attribute such that the PrePaid subscriber could get access to a restricted set of locations for a short duration to allow them to replenish their account, or create an account; or to browse free content.

Upon receiving the Access-Accept from the PrePaid Server, the HAAA will append the usual service attributes and forward the packet to the Access Device. The HAAA SHALL NOT append or overwrite any attributes already set by the PrePaid server. If the HAAA, receives an Access-Reject message, it will simply forward the packet to its client. Depending on site policies, if the HAAA fails to receive an Access-Accept or Access-Reject message from the PrePaid server it MAY do nothing or send an Access-Reject or an Access-Accept message back to its client.

4.3 Session Start Operation

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

Note that the PrePaid Server role is not to record accounting messages and therefore it SHOULD not respond with an Accounting Response packet.

4.4 Mid-Session Operation

During the lifetime of a PrePaid data session the Access Device SHOULD be configured to generate Accounting-Request (Interim) and will request to replenish the quotas using Authorize Only Access-

Request messages.

Once the allocated quota has been reached or the threshold has been reached, the Access Device MUST send an Access-Request with Service-Type(6) set to a value of ôAuthorize Onlyö and the PPAQ attribute.

The Access Device MUST also include NAS identifiers, and Session identifier attributes in the Authorize Only Access-Request. The Session Identifier should be the same as those 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 either User Password or Chap Password. In order to authenticate the message, the Access Device must include the Message-Authenticator(80) attribute. The Access Device will compute the value for the Message-Authenticator based on [RFC2869].

When the HAAA receives the Authorize-Only Access-Request that contains a PPAQ, 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 but not a Message-Authenticator(80) it SHALL silently discard the message. An Authorize Only Access-Request message that does not contain a PPAQ is either in error or belongs to another application (for example, a

Change of Authorization message [CHIBA]). In this case the Authorize Only Access-Request will either be silently discarded or handled by another application (not in scope of this document).

Once the Authorize Only Access-Request message is validated, the HAAA SHALL forward the Authorize Only Access-Request to the appropriate PrePaid Server. The HAAA MUST forward the Authorize Only Access-Request to the PrePaid server specified in the PPAQ. The HAAA MUST sign the message using the Message-Authenticator(80) and the procedures in [RFC2869]. As with the Access-Request message, the HAAA MAY modify the User-Name(1) attribute to a value that represents the userÆs internal PrePaid account in the PrePaid server. Note the PrePaid server could use the Quota-ID sub-attribute contained within the PPAQ to locate the user account.

Upon receiving the Authorize Only Access-Request containing a PPAQ attribute, the PrePaid server MUST validate the Message-Authenticator(80) as prescribed in [RFC2869]. If the message is invalid, the PrePaid server MUST silently discard the message. If it received an Authorize Only Access-Request message that does not contain a PPAQ it MUST silently discard the message.

The PrePaid server will lookup the PrePaid session by using the PrePaid Quota Id contained within the PPAQ. The PrePaid Server would, take the last allocated quota and subtract that from the UserÆs balance. If there is remaining balance, the PrePaid server re-authorizes the PrePaid session by allocate an additional quota. The PrePaid server may want to calculate a different threshold values as well.

Upon successful re-authorization, the PrePaid server will generate an Access-Accept containing the PPAQ attribute. The Access-Accept message MAY contain Service-Type(6) set to Authorize-Only and MAY contain the Message-Authenticator(80).

Depending on site policies, upon unsuccessful authorization, the PrePaid server will generate 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 PrePaid subscriber could get access to a restricted set of locations for a short duration to allow them to replenish their account, or create an account; or to browse free content.

Upon receiving the Access-Accept from the PrePaid server, the HAAA SHALL return the packet to its client. If the HAAA, receives an Access-Reject message, it will forward the packet. Depending on site policies, if the HAAA fails to receive an Access-Accept or an Access-Reject message from the PrePaid server it MAY do nothing or it MAY send an Access-Reject message back to its client.

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

Upon receiving an Access-Accept message containing either Filter-Id(11) or Ascend-Data-Filter attributes, and or Session Timeout(27). The Access Device SHALL restrict the subscriber session accordingly.

4.5 Dynamic Operations

The PrePaid server may want to take advantage of the dynamic capabilities that are supported by the Access Device as advertised in the Dynamic-Capabilities attribute during the initial Access-Request.

There are two types of actions that the PrePaid server can perform: it can request that the session be terminated; or it can request that the filters associated with the session be modified.

Both of these actions require that the session be uniquely identified at the Access Device. As a minimum the PrePaid server:

-MUST provide either the NAS-IP-Address(4) or NAS-Identifier(32)
-MUST 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.

4.5.1 Unsolicited Session Termination Operation

This capability is described in detail in [CHIBA]. The PrePaid server send a Disconnect Request packet that MUST contain identifiers that uniquely identify the subscriberÆs data session and the Access Device holding that session.

Upon receiving the Disconnect Request packet the HAAA will either act on it or will proxy it to another AAA server until it is received by the a AAA that is in the same network as the serving Access Device.

Each AAA MUST route the Disconnect Request packet. How the routing decision is made is an implementation detail.

Once the Disconnect Request packet reaches AAA that is in the same network as the serving Access Device, if the Access Device supports Disconnect-Request (as per [CHIBA]), it sends the message directly to the Access Device; otherwise it uses other mechanisms such as SNMP or Telnet to command the Access Device to terminate the session.

If the Access Device receives a Disconnect-Request packet, it will respond with either a Disconnect-ACK packet if it was able to terminate the session or else it will respond with a Disconnect-NAK packet.

If the AAA server is performing the disconnect operation, it MUST respond with a Disconnect-ACK message if it successfully terminated the session or a Disconnect-NAK message if it failed to terminate the session.

If any AAA server is unable to route the Disconnect-Request it MUST respond with a Disconnect-NAK packet.

4.5.2 Unsolicited Change of Authorization Operation

The PrePaid Server MAY send a Change-of-Authorization message as described in [CHIBA] to restrict internet access when the subscriber has no more balance.

The PrePaid server sends a Change-of-Authorization packet it MUST contain identifiers that will uniquely identify the subscriber session and the Access Device serving that session.

Upon receiving the Change-of-Authorization packet the HAAA will either act on it or proxy it to another AAA server until it is received by a AAA server that is in the same network as the serving Access Device.

Each AAA must route the packet to the serving network. How the routing decision is made is an implementation detail.

Once the Change-of-Authorization packet reaches a AAA that is in the same network as the serving Access Device, if the Access Device supports Change-of-Authorization message, it will forward the

message to the Access Device; otherwise, it will use other mechanisms such as SNMP or Telnet to command the Access Device to change its filters.

If the Access Device receives a Change-of-Authorization packet, it will respond with either a Change-of-Authorization-ACK packet if it was able to change the filter or else it will respond with a Change-of-Authorization-NAK packet.

If the AAA server is performing the change of filter operation, it MUST respond with a Change-of-Authorization-ACK message if it successfully or a Change-of-Authorization-NAK packet if it failed to change the filter.

If a AAA server was unable to route the Change-of-Authorization it MUST respond with a Change-of-Authorization-NAK packet.

4.6 Termination Operation

The termination phase is initiated when either: the Subscriber logs off; the quotas have been consumed, or when the Access Device receives a Disconnect Message. In all of these instances, if the session is a PrePaid data session, the Access Device will send an Authorize-Only Access-Request message with a PPAQ Update-Reason attribute set to either ôClient Service terminationö or ôRemote Forced disconnectö and the currently used quota.

The BAAA MUST forward this packet to the next BAAA or the HAAA.

The HAAA MUST validate the Authorize Only Access-Request using the Message-Authenticator(80) as per [RFC2869] and if valid, use the PrePaidServer subtype in the PPAQ to forward the Authorize Only Access-Request packet to the serving PrePaid Server or if needed, its alternate.

The PrePaid Server MUST validate the Authorize Only Access Request and use the information contained in the PPAQ attribute to adjust the subscriberÆs balance and to close the session. The PrePaid Server SHALL respond back with an Access-Accept message.

4.7 Mobile IP Operations

In roaming scenarios using mobile-ip, as the mobile subscriber roams between networks, or between different types of networks such as between WLAN and CDMA2000 networks, the PrePaid data session is maintained transparently.

As the subscriber device associates with the new Access Device, the Access Device sends a RADIUS Access-Request and the subscriber is re-authenticated and reauthorized. If the Access Device has PrePaid Client capabilities, it MUST include the PPCC attribute in the RADIUS Access-Request. In this manner the procedure follows the Authentication and Authorization procedure described earlier.

The Access-Request message is routed to the home network and MUST reach the PrePaid System that is serving the PrePaid session. The PrePaid system will then correlate the new authorization request with the existing active session and will assign a quota to the new request. Any outstanding quota at the old Access Device will be returned to the PrePaid system due to the usual mobile-ip handoff procedures. Specifically, the quota will be returned when the Access Device sends the Authorize Only Access-Request with PPAQ Update-Reason subtype 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 [CHIBA] to the Access Device.

If the subscriber has roamed to an Access Device that does not have any PrePaid Capabilities, PrePaid data service may still be possible by requesting the Home Agent (providing it has PrePaid Capabilities) to assume responsibilities for metering the service. The procedure for this scenario will be given in the next release of this draft.

4.8 Accounting Considerations

Accounting messages are not required to deliver PrePaid Data Service. Accounting message will typically be generated for PrePaid

Data Service. This because accounting message are used for auditing purposes as well as for bill generation.

Accounting messages associated with PrePaid Data Sessions should include the PPAQ attribute.

4.9 Interoperability with Diameter

RADIUS PrePaid solutions need to interoperate with Diameter protocol. Two possibilities exist: The AAA infrastructure is Diameter based and the Access Device are RADIUS based; or the Access Device is Diameter based and the AAA infrastructure is RADIUS based.

The Diameter Credit Control Application [DIAMETERCC] describes how to implement a PrePaid using an all Diameter based infrastructure.

<This section to be completed.>

5. Attributes

As currently written, this draft is using the RADIUS [RFC2865] namespace.

Subsequent version will probably be written to use VSAs. However, the Vendor Identifier that would be proposed would be PrePaid Application.

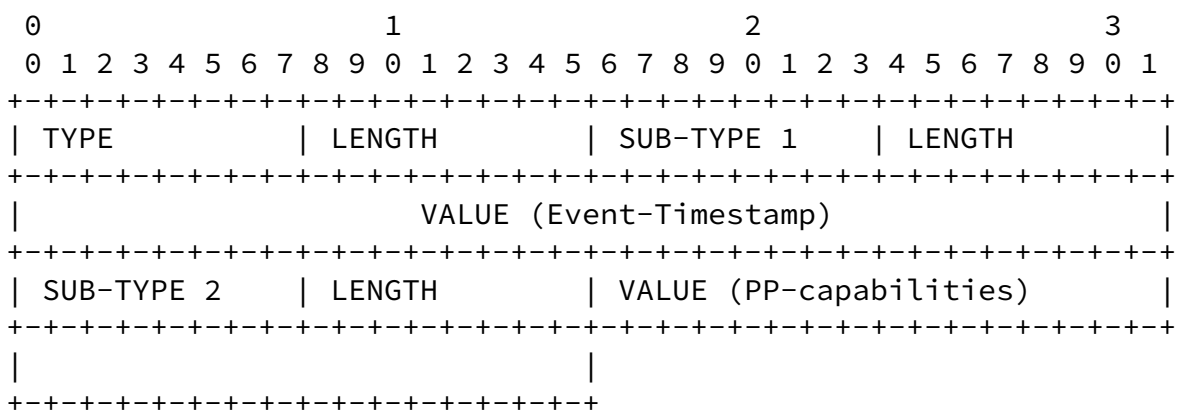
Note: as currently written, this draft proposes to use container types, or attributes that contain sub-attributes, that will have attributes from the PrePaid space and also attributes belonging to RADIUS space. The technique for encoding such a structure will be identified in future release of this document.

Note: The attributes presented in this version of the draft, represent the bare minimum attributes required to implement a PrePaid solution. The use of the ôAuthorize Onlyö Pattern allows the ability to extend PrePaid by adding additional PrePaid VSA in the future.

5.1 PPCC attribute

The PPCC at tribute is sent in the Access-Request message and is

used to describe the Access Devices PrePaid capabilities. The attribute is encrypted using the procedures defined in [RFC2868] section 3.5.



TYPE: value of PPCC
LENGTH: 14

SUB-TYPE 1: 55
LENGTH: 6
DESCRIPTION:
The Event-Timestamp as defined by [RFC2869]

SUB-TYPE 2: value of PP-capabilities
LENGTH: 4
DESCRIPTION:
    BIT-MAP with the following values:
    1 Time metering
    2 Volume metering
    >2 Reserved

5.2 Dynamic-Capabilities attribute

The Dynamic Capabilities attribute is sent in the Access-Request and describes the capabilities of the Access Device. Mainly it describes the method for support for unsolicited session termination and the method for support of unsolicited change of filters.

Subtype: Session-Termination-Methods 1

-None
-Disconnect-Message [CHIBA]
-Telnet
-SNMP

Subtype: Dynamic-Authorization-Capabilities 1
-None
-CoA [CHIBA]
-Telenet
-SNMP

5.3 PPAQ Attribute

The PPAQ attribute is sent in Authorize Only Access-Request and Access-Accept messages. In Authorize Only Access-Request messages it is used to report usage and request further quota; in an Access-Accept message it is used to allocate the quota (initial quota and subsequent quotas).

The attribute consists of a number of subtypes. Subtypes not used are omitted in the message.

Type: 26
Length: variable, greater than 8
Vendor-ID: 5535
Vendor-Type: 90
Vendor-Length: variable, greater than 2

Sub-Type (=1): Sub-Type for QuotaIDentifier attribute
Length: length of QuotaIDentifier attribute (= 6 octets)
QuotaIDentifier (QID):

The QuotaIDentifier Sub-Type is generated by the PrePaid server at allocation of a Volume and/or Duration Quota. The on-line quota update RADIUS Access-Request message sent from the Access Device to the PPS shall include a previously received QuotaIDentifier.

Sub-Type (=2): Sub-Type for VolumeQuota attribute
Length: length of VolumeQuota attribute (= 6 octets)
VolumeQuota (VQ):

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

Sub-Type (=3): Sub-Type for VolumeQuotaOverflow
Length: length of VolumeQuotaOverflow attribute (= 4 octets)
VolumeQuotaOverflow (VQO):

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

Sub-Type (=4): Sub-Type for VolumeThreshold attribute
Length: length of VolumeThreshold attribute (= 6 octets)
VolumeThreshold (VT):

The VolumeThreshold Sub-Type shall always be present if VolumeQuota is present in a RADIUS Access-Accept message (PPS to Access Device direction). It is generated by the PrePaid server and indicates the volume (in octets) that shall be used before requesting quota update. This threshold should not be larger than the VolumeQuota.

Sub-Type (=5): Sub-Type for VolumeThresholdOverflow
Length: length of VolumeThresholdOverflow attribute (= 4 octets)
VolumeThresholdOverflow (VTO):

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

Sub-Type (=6): Sub-Type for DurationQuota attribute
Length: length of DurationQuota attribute (= 6 octets)
DurationQuota (DQ):

The optional DurationQuota Sub-Type is only present if Duration Based charging is used. In RADIUS Access-Accept message (PPS to Access Device direction), it indicates the Duration (in seconds) allocated for the session by the PrePaid server. 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.

Sub-Type (=7): Sub-Type for DurationThreshold attribute
Length: length of DurationThreshold attribute (= 6 octets)
DurationThreshold (DT):

The DurationThreshold Sub-Type shall always be present if DurationQuota is present in a RADIUS Access-Accept message (PPS to Access Device direction). It represents the duration (in seconds) that shall be used by the session before requesting quota update. This threshold should not be larger than the DurationQuota and shall always be sent with the DurationQuota.

Sub-Type (=8): Sub-Type for Update-Reason attribute
Length: length of Update-Reason attribute (= 4 octets)
Update-Reason attribute (UR):

The Update-Reason Sub-Type shall be present in the on-line RADIUS Access-Request message (Access Device 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. Main SI released
8. Service Instance not established

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

The optional, multi-value PrePaidServer indicates the address of the serving PrePaid System. If present, the Home RADIUS server uses this address to route the message to the serving PrePaid

Server. 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 the order of the attributes.

NOTES:

Either Volume-Quota or Time-Quota MUST appear in the attribute.
Volume Threshold may only appear if Volume Quota appears
If the Access Device can measure time, and if Time-Threshold appears with Volume Quota, then the Access device should trigger a quota replenishment when the Current Time >= Time-Threshold.

5.4 Table of Attributes

TO BE COMPLETED.

Request	Accept	Reject	Challenge	#	Attribute
Authorize_Only	Request	Accept	Reject		

6. Security Considerations

The protocol exchanges described are susceptible to the same vulnerabilities as RADIUS and it is recommended that IPsec be employed to afford better security.

If IPsec is not available the protocol in this draft improves the security of RADIUS. The various security enhancements are explained in the following sections.

6.1 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...

6.2 Replenishing Procedure

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

To be completed.

7. IANA Considerations

To be completed.

This draft does create RADIUS attributes. However, the authors recognize that it may not be possible to obtain such attributes. Therefore, in subsequent drafts it will be proposed to use a Vendor space as an Application Space.

8. 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.

[CHIBA] Chiba, M., Dommety, G., Eklund, M., Mitton, D., Aboba, B., "Dynamic Authorization Extensions to Remote Authentication Dial-In User Service (RADIUS)", Internet Draft (work in progress), draft-chiba-radius-dynamic-authorization-07.txt, February 2003.

[DIAMETERCC] Work in Progress.

Acknowledgments

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
Nortel Networks
2221, Lakeside Blvd,
Richardson, TX-75082
chowdury@nortelnetworks.com

Lila Madour
Ericsson Canada
5400 Decarie, TMR
Quebec, Canada
Lila.madour@ericsson.ca

Yong Li
Bridgewater Systems
303 Terry Fox Drive
Suite 100
Ottawa Ontario
Canada
Yong.li@bridgewatersystems.com

Intellectual Property Statement

proprietary rights by implementers or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

Full Copyright Statement

Expiration Date

This memo is filed as <draft-lior-radius-extensions-for-prepaid-01.txt>, and will expire 30th December, 2003.