Network Working Group
INTERNET-DRAFT
Category: Informational
draft-lior-radius-prepaid-extensions-00.txt
Expires: 25 August 2003

A. Lior
Bridgewater Systems

P. Yegani
Cisco

Y. Li
Bridgewater Systems
24 February 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....3
1.1 Terminology....4
1.2 Requirements language....4
2. Use-cases....4
2.1 Simple use-case....5
2.2 Support for concurrent Prepaid sessions....7
2.3 Support for Roaming....7
2.4 Prepaid termination....8
3. Architecture....8
4. Operations....12
4.1 General Requirements....12
4.1.1 Broker AAA Requirements....12
4.2 Authentication and Authorization....13
4.3 Session Start Operation....15
4.4 Mid-Session Operation....16
4.4.1 Accounting Operation....16
4.4.2 Quota Replenishing Operation....16
4.5 Dynamic Operations....18
4.5.1 Unsolicited Session Termination Operation....19
4.5.2 Unsolicited Change Filter Operation....19
4.6 Termination Operation....20
4.7 Mobile IP Operations....21
5. Attributes....22
5.1 PPCC attribute....22
5.2 Dynamic-Capabilities attribute....23
5.3 PPQ-Response attribute....24
5.4 PPQ Attribute....25
5.5 Service Type....26
5.6 Table of Attributes....26
6. Security Considerations....26
6.1 Authentication and Authorization....26
6.2 Accounting Messages....27
6.3 Replenishing Procedure....27
7. IANA Considerations....28
8. Normative References....28
9. Acknowledgments....28
10. Author's Addresses....29
11. Intellectual Property Statement....29
12. Full Copyright Statement....30
Expiration Date....30

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 therefore 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 - 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 a 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 AAA (HAAA)
Broker AAA (BAAA)
Visited AAA (VAAA)
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. Use-cases

In this section we present a set of use case that will help establish the requirements needed to deliver a prepaid data service. 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 with a provider.

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 authorize the subscriber.

The Access Device sends an 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 has Prepaid Client capabilities.

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 makes a request of the Prepaid System to 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 will include attributes for the Prepaid Client such as, the initial quota (time or volume) and maybe a threshold value.

The Prepaid System allocates a portion of the subscribers account so that we can support concurrent prepaid sessions. For example, the

subscriber may be on a prepaid voice call and may also have a concurrent prepaid data session. Throughout the life 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 determines the type of service whereas the Prepaid System is only 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, the Access Device will, as instructed by the Prepaid System, request for additional quotas. The re-authorization for additional quota flows through the AAA system to the Prepaid System. The Prepaid System revalidates the subscriberÆs account and if there is still a balance 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 not a re-authentication procedure but rather a re-authorization procedure.

It is important to note that the Prepaid System is maintaining session state for the subscriber. In this case the state is how much was allocated for the session and how much is left in the account. 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 to service 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.
Quota Recovery

In the above scenario, should the subscriber terminate the session before the session is terminated 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.

2.2 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.

2.3 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 some 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 around and maintain 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. As well, subsequent messaging for the session need to be received at the home network and more specifically at the Prepaid System where state is being maintained. This behavior is particularly challenging for dynamic roaming. To illustrate this,

supposing a subscriber establishes a prepaid session and is then handed off to an Access Device that does not support prepaid capabilities.

Static roaming is handled by proxy chains of broker AAA servers.

Static roaming or Dynamic roaming is handled by mobile-ip. Note mobile-ip may also involve proxy chains.

2.4 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.

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 Points. 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 the filters associated with a specific data session by processing Disconnect Messages and Change of Filter messages as per [CHIBA].

In this document RADIUS is used as the AAA server. 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 to route the RADIUS packets and hence donÆt play an active roll in the Prepaid Data Service delivery.

In this document the Prepaid Server are described in functional terms related to their 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. These counters are continuously being updated during the lifetime of the Prepaid data service.

The various deployments 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 provider 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.

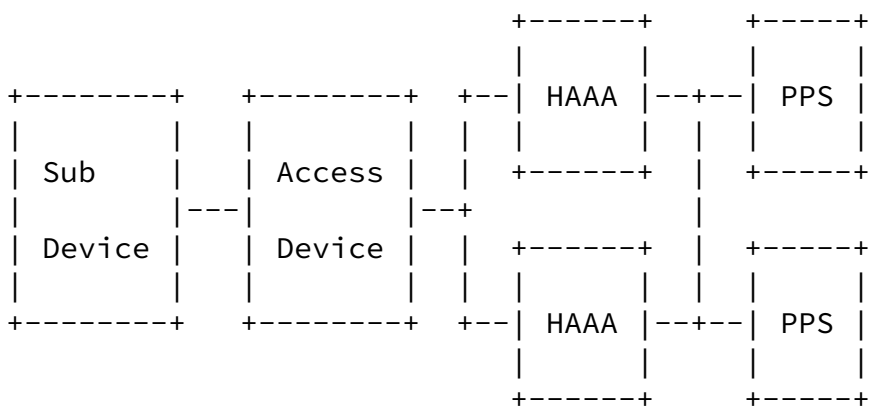
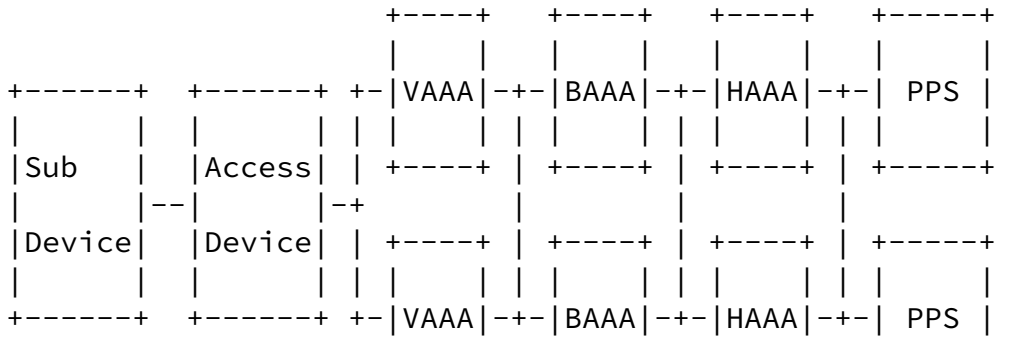


Figure 1 Basic Prepaid Architecture

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.



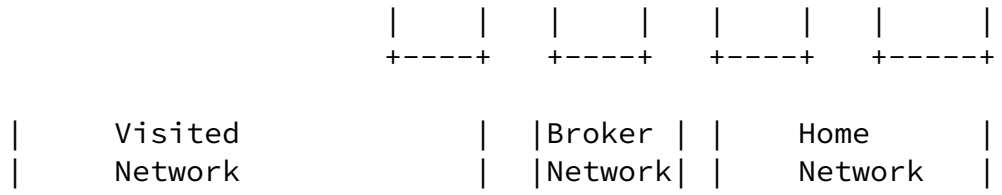
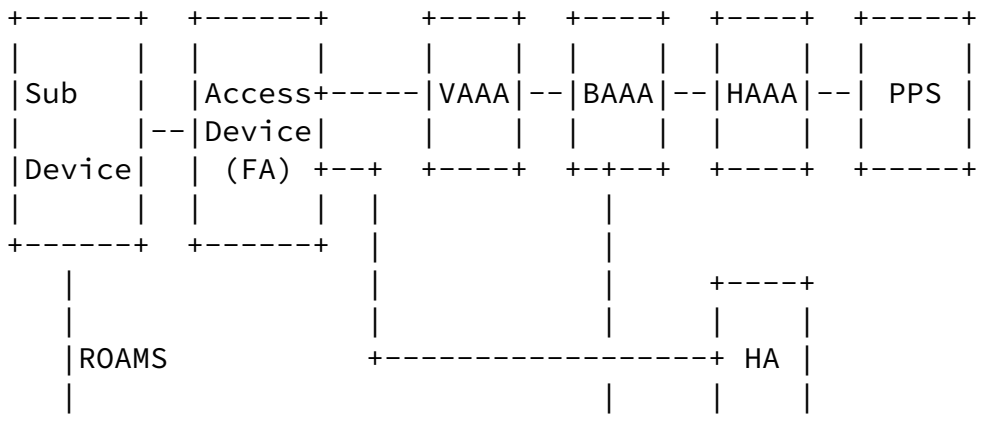


Figure 2 Static Roaming Prepaid Architecture

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 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.



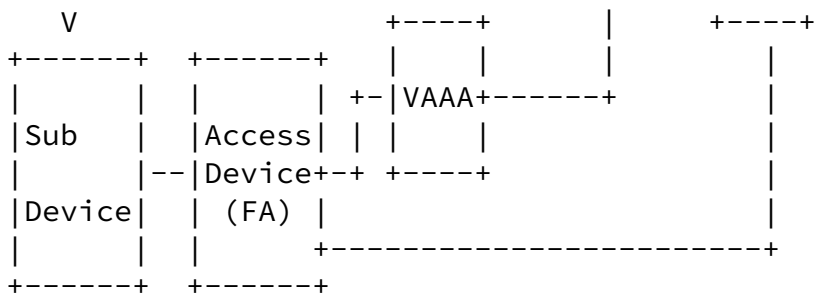


Figure 3 Roaming using mobile-ip

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

The intent of this document is to minimize the requirement impacts on the Broker AAA servers. The BAAA servers function is to forward the RADIUS packets as usual to the appropriate RADIUS servers with the following considerations.

Accounting messages are used to keep the Prepaid Server current as to what is happening with the prepaid data session. Therefore, Broker AAA servers SHOULD perform their forwarding function of accounting packets associated with prepaid data sessions in a pass through fashion as described in [RFC2866] section 2.1.

In addition, if the BAAA server fails to forward the prepaid data session accounting packets, it MAY store them locally but it SHOULD NOT generated an Accounting Response packet back to its client.

The BAAA MUST be capable of supporting the encryption procedures specified in [RFC2868] section 3.5.

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.

The PPCC is encrypted using the same procedure as in [RFC2868] Section 3.5 and includes the Event-Timestamp(55) which protects against replay attacks.

If the Access Device supports the Disconnect Message capabilities or the Change of Filter Message capabilities, then it SHOULD include

the Dynamic-Capabilities attribute. The Dynamic-Capabilities attribute will indicate to the PPS if the Access Device will support the Disconnect Message or the Change of Filter Message.

In certain deployments, there may be other ways in which to terminate a data session, or change the filter id on an Access device. 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 during the authentication procedure.
The Access Request will be sent as usual to the HAAA. The packet may be proxied through zero or more BAAA. The BAAA SHALL treat the PPCC as a undistinguished octets and re-encrypt the PPCC as it forwards the Access Request to the HAAA. No interpretation by the BAAA should be made.

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 would be set to a value that would represent the SubscriberÆs Prepaid Identity. This attribute will be 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 will validate the Access Request by decrypting the PPCC and checking the Event-Timestamp(55). The Prepaid server will lookup the subscriberÆs prepaid account and 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 initial PPQ-Response 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 updates;

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

-The Time of Volume Threshold that the Prepaid server MAY set to control when the Access Device requests additional quota.

The Prepaid Referral the first one is set to the IP address of the Serving Prepaid Server, the second one is set to an alternate Prepaid Server. This way the HAAA will be able to route subsequent packets to the serving Prepaid Server or its alternate.

Additionally, the Prepaid server MAY set the Terminate-Action(29) to RADIUS-Request(1); and MAY set Acct-Interim-Interval(85) to control how often interim Accounting Requests are generated.

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. The HAAA SHALL NOT append 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 Response 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) MUST be routed to the Prepaid Server so that it can confirm the initial quota allocation.

In addition to the usual attributes, the Accounting Request(Start) message MUST contain the PPQ attribute.

HAAA receives the Accounting Request(Start) packet and MAY record it. If the packet is associated with a prepaid subscriber (it contains a PPQ attribute) it SHALL forward the packet to the serving Prepaid server or its secondary if any.

The Prepaid server SHALL respond with an Accounting Response packet as usual.

The HAAA server SHALL respond with an Accounting Response packet if it forwarded the Accounting Request(Start) packet to the Prepaid server and it received the Accounting Response packet; and if it was

responsible for recording the Accounting Request(Start) packet, it did so successfully.

4.4 Mid-Session Operation

During the lifetime of a session the Access Device will generate accounting messages as usual and request to replenish the quotas.

4.4.1 Accounting Operation

During the normal data session the Access Device will generate Accounting Requests(start), Accounting Requests(stop) and Accounting Request(Interim).

These Accounting records are needed by the Prepaid server to keep an accurate running usage record for each data session and to be able to correctly credit the accounts of a prepaid subscriber during faults.

If these Accounting messages are associated with a Prepaid data service, then the Access Device MUST include the PPQ attribute.

The HAAA will forward any accounting packets received to the primary Prepaid server and failing that the secondary Prepaid server identified in the PPQ attribute.

The HAAA may record the accounting packets locally as well.

The Prepaid Server MUST respond with an Accounting Response packet.

The HAAA server MUST respond with an Accounting Response packet if it forwarded the Accounting Request packet to the Prepaid server and it received the Accounting Response packet; and if it was responsible for recording the Accounting Request packet, it did so successfully.

4.4.2 Quota Replenishing Operation

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 Prepaid and it MUST contain the PPQ attribute.

The other attributes should be the same as were used in the Access Request during the Authentication and Authorization phase except for the User Password or Chap Password, which should be left out. This Access Request is only used for reauthorization and not re-authentication and the passwords are not required. The encrypted PPQ attribute acts as the credential for the Access Request.

As during the Authentication and Authorization phase, the BAAA SHALL forward the Access Request message to the HAAA validating decrypting and re-encrypting the PPQ attribute. Note that the BAAA will treat

the PPQ as non-distinguished octets.

The HAAA SHALL receive the Access Request, decrypt the PPQ, validate it and use the PPS-referral attributes to route the Access Request to the correct Prepaid server. The HAAA MAY modify the User-Name(1) attribute as it has done during the initial Access Request. Note the Prepaid server will use the Quota-ID sub-attribute contained within the PPQ to locate the user account. The HAAA MAY add the Username-Password(2) attribute and set itÆs value to the password it shares with the Prepaid server. The HAAA will re-encrypt the PPQ.

The Prepaid server will validate the Access Request by decrypting the PPQ and checking the Event-Timestamp. If the User-Password(2) is specified, the Prepaid server will use it to ensure that the HAAA is valid.

The Prepaid server will lookup the prepaid session by using the Prepaid Quota Id contained within the PPQ. The Prepaid Server would then re-authorize the subscriber by allotting it a new quota. The Prepaid Server may want to calculate a different threshold values as well.

Note: At the Prepaid server, the PPQ and the QUOTA-ID is acting as the credential for the subscriber. The User-Name(1) attribute is used to route the Access Request to the correct HAAA. The User-Password if supplied, is used to authenticate the HAAA at the Prepaid server.

Upon successful re-authorization, the Prepaid server will generate an Access Accept containing the PPQ-Response attribute.

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 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. The Prepaid server MAY add the Terminate-Action(29) attribute with the value of RADIUS-Request, to allow the Access Device to try to get a new quota allocated before booting the subscriber off.

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 Response message from the Prepaid server it MAY do nothing or 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 PPQ-Response packet. Note that the Prepaid server MAY update the PPS-referral attributes 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 PPClient as advertised in the Dynamic-Capabilities attribute during Access Request.

There are two type 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 the Accounting-Session-Id(44)

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

4.5.1 Unsolicited Session Termination Operation

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.

The HAAA upon receiving the Disconnect Request packet will either act on it or will proxy it to another AAA server until it is received by a AAA that can process the Disconnection Request packet.

Each AAA MUST have the knowledge to route the packet. How the routing decision is made is an implementation detail.

Once the Disconnect Request packet reaches a AAA that can act on it. The AAA will either send the Disconnect Request packet to the Access Device directly or it may have to use 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 a AAA server was unable to route the Disconnect request it MUST respond with a Disconnect-NAK packet.

Issue: A reason code in the NAK message should be provided so that the prepaid server knows why the Disconnect failed. This may be under consideration now by Chiba et al.

4.5.2 Unsolicited Change Filter Operation

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

The HAAA upon receiving the Change of Filter packet will either act on it or will proxy it to another AAA server until it is received by a AAA that can process the Change of Filter packet.

Each AAA MUST have the knowledge to route the packet. How the routing decision is made is an implementation detail.

Once the Change of Filter packet reaches a AAA that can act on it. The AAA will either send the Change of Filter packet to the Access Device directly or it may have to use SNMP or Telnet to command the Access Device to change its filters.

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

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

Issue: A reason code in the NAK message should be provided so that the prepaid server knows why the Change of Filter failed.

4.6 Termination Operation

The termination phase is initiated when 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 generate and Accounting Request (stop) packet that MUST contain the PPQ attribute with Reason set to Terminate.

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

The HAAA MUST use the referral information in the PPQ to forward the Accounting Request(stop) packet to the serving Prepaid Server or its alternate if needed. The HAAA MAY record the Accounting Request(stop) packet.

The Prepaid Server SHALL use the information contained in the PPQ

attribute of the Accounting Request(stop) packet to adjust the subscriberÆs balance and to close the session. The Prepaid Server SHALL respond back with an Accounting Response.

The HAAA SHALL respond with an Access Response packet if it has received the Access Response from the Prepaid Server, and if it was responsible for recording the Accounting message, it did so successfully.

In addition to getting the Accounting Request(stop) packet, at the end of the data session. In more robust deployments, the Access Device MAY have been instructed by the Prepaid Server to generate an Access Request message by the inclusion of the Terminate-Action(29) attribute with a value of RADIUS-Request in the Access Accept message. In this case, if the session is prepaid, the Access Device generates an Access Request that MUST containing the PPQ attribute with a Service-Type(6) set to Prepaid. The Reason sub-attribute of the PPQ attribute SHALL be set to Terminate.

The BAAA SHALL forward the Access Request to the next BAAA or the HAAA.

Upon receiving an Access Request message with Service-Type(6) set to Prepaid, the HAAA SHALL use the referral information contained in the PPQ attribute to route the Access Request to the serving Prepaid Server or its alternate. The HAAA MAY add the User-Password(2) attribute with the password shared between it and the Prepaid Server.

Upon the receiving the Access Request, the Prepaid server will examine the PPQ attribute and use the Quota-ID to locate the session and adjust the subscriberÆs account accordingly and close the session. The Prepaid Server SHALL reply 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 Accounting Request (stop) message. The Prepaid system may issue a Disconnect Message to the Access Device as well.

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.

5. Attributes

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

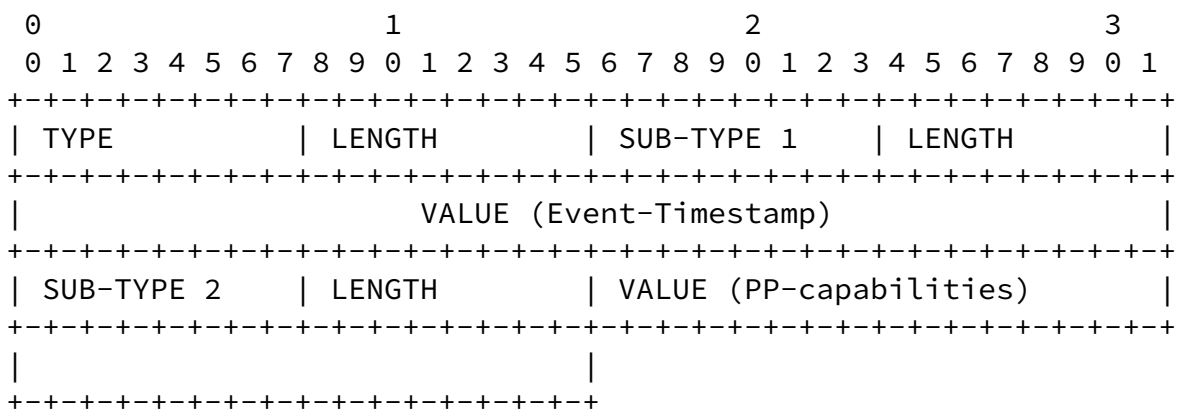
Subsequent version will probably be written to use VSAs. However, the Vendor Identifier that would be proposed would be Prepaid Application.

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.

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-Filter-Capabilities 1
-None
-CoF [CHIBA]
-Telenet
-SNMP

5.3 PPQ-Response attribute

The PPQ-Response attribute is sent in the Access Response and describes the current quota for a given prepaid data session.

Subtype Quota ID 1

Assigned by the Prepaid server at the start of the session. It is used to correlate all other transactions for the given prepaid data session.

Subtype Volume-Quota 0-1

Optional. The maximum number of octets that are allowed for this session since the beginning of the session.

Subtype Volume-Threshold 0-1

Optional. Defines when to trigger quota replenishment. Current Octets >= Volume-Threshold.

Subtype Time-Quota 0-1

Optional. The maximum number of seconds that are allowed for this session as measured from the beginning of the session.

Subtype Time-Threshold 0-1

Optional. Defines when to trigger quota replenishment. Current Octets >= Time-Threshold

Subtype Action 1

Defines what to do when the quota has been reached.

-Drop the session
-Replenish

Subtype PPS-Referral 1..2

The first PPS-Referral attribute MUST be included and contains the IP address of the primary serving Prepaid server. The second PPS-Referral attributes MAY be included and contains the IP address of the secondary serving Prepaid server.

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 PPQ Attribute

This attribute reports the current prepaid usage at the access device. It is contained in both the Access Request messages and Accounting Requests message.

Subtype Quota ID 1

The Quota-ID assigned by the Prepaid server during the Access Response.

Subtype Event-Timestamp(55) 1

Used to protect against replay attacks

Subtype Current-Volume 0-1

Optional. The current volume in octets since the session started.

Subtype Current-Time 0-1

Optional. The number of seconds since the session started.

Subtype Reason 1

The reason for sending this attribute:

-Interim,
-QuotaReplenish,
-Terminate

Subtype PPS-Referral 1..2

The IP address of the primary serving Prepaid Server and optionally the IP address of the secondary serving Prepaid server.

5.5 Service Type

The following is a new value for the Service-Type(6) attribute.

12 Prepaid

5.6 Table of Attributes

TO BE COMPLETED.

Request	Accept	Reject	Challenge	#	Attribute

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. The protocol given in this draft prevents replay attacks that can cause havoc such as the depletition the subscribers prepaid account.

The Access Request originating at a Prepaid Capable access device include the PPCC attribute which contains the Event-Timestamp(55) attribute and the PPCC is encrypted. Therefore the Prepaid System can use the attribute to detect replay attacks.

6.2 Accounting Messages

Accounting messages are signed by the RADIUS protocol but they are also susceptible to replay attacks. However, since accounting messages are designed for recording purposes, no harm come by a replay attack. The accounting subsystem should be able to detect and remove duplicate records. Accounting records associated with prepaid data session contain the PPQ attribute with contains the Event-Timestamp(55) attribute. Even though Accounting messages are still only used for record keeping, replay attacks can be detected and prevented.

6.3 Replenishing Procedure

The Access Request message used in the Replenishing procedure contains the User-Name(1) attribute but does not contain User-Password or Chap-Password. This is because this message is used for Re-authorizing additional quotas. Never-the-less security is a concern.

The subscriber password is not used because it is only available during subscriber authentication. The Access Device should not keep the subscriber's password. Furthermore, the password may not have been available in the first place since the EAP type of authentication may have been used. EAP only exists during authentication.

The User-Name(1) attribute contains the NAI of the subscriber. The purpose of this attribute is to route the Access Request message to the home network.

The Access Request contains the PPQ attribute which contains the Event-Timestamp(55) and the Quota-ID sub-attributes. This attribute is encrypted and provides the following security mechanisms. The inclusion of the Event-Timestamp(55) is used to prevent replay attacks. The Quota-ID was allocated by the Prepaid server and uniquely identifies the subscriber. Therefore the Prepaid Server uses the PPQ attribute as the credential of the subscriber. Since

this attribute is encrypted it forms a very reliable credential for the prepaid subscriber at the Prepaid server.

7. IANA Considerations

This draft does create RADIUS attributes nor any new number spaces for IANA administration. However, the authors recognize that it may not be possible to obtain such attributes. Therefore, is subsequent drafts it will be proposed to use a Vendor space as an Application Space.
This draft requires assignment of new values to existing RADIUS attributes. These include:

Attribute	Values Required
Service-Type	Prepaid(12)

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.

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

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

Intellectual Property Statement

Full Copyright Statement

Expiration Date

This memo is filed as <draft-lior-radius-extensions-for-prepaid-00.txt>, and will expire 25th August, 2003.