

AAA cost advertisement extensions

<[draft-caron-aaa-cost-advertisement-00.txt](#)>

1 Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

2 Abstract

In many roaming scenarios, it is necessary to be able to carry cost information between the different parties in order to facilitate credit checking, real-time accounting, cost presentation to the user. It is also necessary that this information be interpretable by automated systems, that these systems be able to modify it to take commissions into account, and that non-repudiation mechanisms be available. This document proposes such a system to be used with AAA architectures.

Table of Contents

<u>1</u>	Status of this Memo.....	<u>1</u>
<u>2</u>	Abstract.....	<u>1</u>
<u>3</u>	Introduction.....	<u>2</u>
<u>4</u>	Terminology.....	<u>3</u>
<u>5</u>	Conventions used in this document.....	<u>3</u>

6	Description of the overall setup.....	3
-------------------	---------------------------------------	-------------------

Caron	Informational - Expires December 2002	1
INTERNET-DRAFT AAA Cost Advertisement Extensions		June 2002

7	Billing formats.....	4
8	AAA attributes.....	7
8.1	Cost advertisement attribute.....	7
8.2	Cost acceptance attribute.....	10
9	Examples.....	12
9.1	Fixed visited network cost.....	12
9.2	Fixed end-user cost.....	14
10	Security Considerations.....	15
11	References.....	15
12	Author's Address.....	17

[3](#) Introduction

In many roaming contexts, in particular public WLAN roaming, costs incurred for connection to foreign networks can vary significantly. Costs can also vary according to the user's subscription plan, and to the exact relationship (possibly multi-level) between the visited network and the commercial operator that bills the end-user, in such a manner that it is difficult to determine these costs in advance.

For these reasons, it appears necessary to be able to:

- verify that a user can use such a connection, based on its subscription plan and any credit-checking that could be needed;
- present costs to the user during connection setup time;
- be able to carry billing and accounting information in real time between the different parties involved (the visited network, the commercial operator, and eventually one or many roaming operators in between).

This billing and accounting information is not necessarily the same over the whole chain, since intermediate roaming operators are likely to take a commission on transaction they handle and for which they manage compensation.

It is also important for all parties to be sure that they will get payment for the services provided, and hence non-repudiation mechanisms are needed on all commercial relationships involved:

- between the end-user and its home network (out of the scope of this document)

- between each pair of operators along the path between the visited network and the home network, via possible one or many roaming operators.

Caron Informational - Expires December 2002
INTERNET-DRAFT AAA Cost Advertisement Extensions

2
June 2002

Finally, cost information can be expressed in many different ways, ranging from a simple fixed cost per connection to complex variable costs based on duration or volume. Similarly, the commissions can be either added to the cost requested by the visited network (the cost to the end-user being then higher), or accounted separately (the cost to the end-user being exactly what the visited network proposes, but the home network getting a smaller share of the total). Any specification must account for this variety of different formats.

This document aims to describe such a specification for carrying cost information within AAA protocols, more specifically RADIUS [1,2,3] or Diameter [4].

[4](#) Terminology

WISP Wireless Internet Service Provider. An organization which provides access to the Internet via Wireless LAN infrastructure.

WLAN Wireless LAN, using e.g. IEEE 802.11 protocols.

[5](#) Conventions used in this document

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 [RFC-2119](#) [5].

[6](#) Description of the overall setup

To help in the understanding of the specification, we will use a typical example of a multi-level roaming scenario, in which two roaming operators are intermediaries between the visited network and the home network:

```

+-----+      +-----+      +-----+      +-----+      +-----+
|USER|  --->  |WISP|  --->  |ROAM1|  --->  |ROAM2|  --->  |HOME|
+-----+      +-----+      +-----+      +-----+      +-----+
/      /                                          |
```

$+ \text{---} + < \text{-----} +$

Caron Informational - Expires December 2002
INTERNET-DRAFT AAA Cost Advertisement Extensions

the costs associated with this connection. These requests follow the direction of the top arrows in the above diagram.

7 Billing formats

The format begins with a header structure:

- Decimals in the number of decimals in the decimal representation of currency units. For instance, if Decimals is 2, then a value of 150 means 1.50 of the currency unit.
- Currency is the ISO 4217 code of the currency used. It is expected that on any given relationship, only one currency will be used (the currency used for the actual billing between the two entities), and that roaming operators will perform conversion between currencies if

they have relationships with entities using different currencies. This information is used for confirmation purposes, and for events of currency changes (like the switch from national currencies to the Euro).

- Number of types is the number of different billing types following, as described further.

After the cost header, comes the type header, which describes the type of billing to be performed:

Type	Number of units
------	-----------------

- Type describes what is counted to perform billing. Possible values are:

Caron Informational - Expires December 2002 4
INTERNET-DRAFT AAA Cost Advertisement Extensions June 2002

- 1 Transaction: this is a one-off cost
- 2 Duration: billing is based on duration in seconds
- 3 Bytes in: billing is based on bytes received
- 4 Bytes out: billing is based on bytes sent
- 5 Bytes total: billing is based on total bytes

- Number of units indicates the number of billing units that follow. Must be 1 for Type 1.

Billing units are described using the following format:

Amount
Quantity
Repeat

- Amount is the amount of money that should be billed. The value stored here should be divided by 10^{decimals} to get the number of currency units.

- Quantity is the number of seconds or bytes that this amount will cover. 0 means none, and all ones means unlimited. This field is ignored for a Type of Transaction.

- Repeat is the number of times this unit will be repeated before moving on to the next one. 0 means unlimited. This field is ignored for a Type of Transaction.

Here are some examples:

```
00  'E' 'U' 'R'
00  01  00  00
00  01  00  01
00  00  00  0A
00  00  00  00
00  00  00  00
```

This indicates we bill in Euros (EUR), and amounts are given with no decimals (0). There is one billing type, which is a transaction, with only one unit, indicating an amount of 10.

In short: a cost of 10 euros for the transaction.

The same information could be represented as follows:

```
00  'E' 'U' 'R'
00  01  00  00
```

Caron Informational - Expires December 2002
INTERNET-DRAFT AAA Cost Advertisement Extensions

5
June 2002

```
00  02  00  01
00  00  00  0A
FF  FF  FF  FF
00  00  00  00
```

The difference being that billing is based on duration, but the first (and only) duration billing unit is unlimited (FFFFFFFF).

An example of volume billing:

```
04  'U' 'S' 'D'
00  01  00  00
00  05  00  01
00  00  00  0F
00  00  04  00
00  00  00  00
```

Here we bill in US dollars (USD), with 4 decimals. There is one billing type, which is based on total volume, and one unit, which indicates that each kilobytes (0x400 = 1024 bytes) is billed 0.0015 USD (the value is 15 but we have 4 decimals). Measured quantities

should be rounded up to the next billing quantity.

An example of billing with an initial payment for a long period, then smaller increments for additional time:

```
02  'E' 'U' 'R'
00  01  00  00
00  02  00  02
00  00  01  F4
00  00  03  84
00  00  00  01
00  00  00  32
00  00  00  3C
00  00  00  00
```

In this case we bill in euros with 2 decimals. There is one billing type, which is based on duration, and two units. The first unit indicates a cost of 5.00 EUR (0x1F4 = 500) for the first 15 minutes (0x384 = 900 seconds). This unit is used once, after which additional time is billed 0.50 EUR (0x32 = 50) per minute (0x3C = 60 seconds), indefinitely.

This last examples describes a scenario where we bill based on two different quantities (here volume in and volume out):

```
02  'E' 'U' 'R'
00  02  00  00
00  03  00  01
00  00  00  0A
```

Caron Informational - Expires December 2002
INTERNET-DRAFT AAA Cost Advertisement Extensions

6
June 2002

```
00  00  04  00
00  00  00  00
00  04  00  01
00  00  00  14
00  00  04  00
00  00  00  00
```

In this scenario we still bill in euros with 2 decimals, and there are two billing types. The first one is based on volume in, and has one unit of 0.10 EUR per kilobyte received, indefinitely. The second billing type is based on volume out, and has one unit of 0.20 EUR per kilobyte sent, indefinitely.

Many other combinations are possible, such as billing based on duration and volume, free initial periods, discounts after a certain

time or volume, etc.

8 AAA attributes

In order to support the required functionality, the following new attributes are required:

- a cost advertisement attribute
- a cost acceptance attribute

8.1 Cost advertisement attribute

The cost advertisement attribute Cost-Advertisement (code TBD) is used in authorization requests, or in protocols such as RADIUS that do not make a distinction between authentication and authorization requests, in Access-Request packets.

In this last case, and if authentication takes several round-trips (with Access-Challenge responses for authentication protocols such as CHAP, ARAP, or EAP), the cost advertisement attribute should be ignored by the AAA server until authentication is complete. Intermediate proxies not being able to determine in advance whether an Access-Request will be the final one, should handle all requests the same.

The attribute format (excluding code and length portions which are specific to the AAA protocol), is defined below:

Flags	
Type	Length
Cost data	

Caron	Informational - Expires December 2002	7
INTERNET-DRAFT	AAA Cost Advertisement Extensions	June 2002

Type	Length
Cost data	

- Flags is a bitmap of global flags. Currently, all bits are

reserved, and should be set to 0.

- Type indicates the type of cost information following. It can have the following values:

- 0 indicates this is the cost requested. Further parties along the authorization chain should increment this cost to include their commission or charges. In this case, there should be only one cost element (type, length, cost data) present in the packet.

- 1 indicates this is the cost that the visited network (the party originating the request) wants to charge the end-user. Further parties along the authorization chain should leave this cost unchanged, but add or increment a cost information element with type 2. The initial request (from the visited network to the first roaming operator along the path) might contain only one cost element (type, length, cost data). Further along the path, there should be two elements, one with type 1 representing the cost the user should be charged, and one with type 2 representing commissions and charges of other parties. Only per-connection costs (i.e. with no variable duration-based or volume-based costs) are allowed.

- 2 indicates this is the added cost that intermediate parties want to charge for this transaction. Only per-connection costs (i.e. with no variable duration-based or volume-based costs) are allowed.

- Length is the length of the cost data (excluding type and length)

- Cost data is cost information encoded as specified in [section 7](#).

There can be one or two cost elements (type, length, cost data) in the request. There can be one of type 0 or 1, or two of types 1 and 2 respectively. It is illegal to have a request containing:

- a cost element of type 0 and another cost element;
- more than one cost element of the same type;
- a cost element of type 2 with no cost element of type 1.

Such requests should be rejected with code TBD.

Upon reception of a request containing a Cost-Advertisement attribute, roaming operators should:

- store cost elements received for this request;
- if there is a cost element of type 0, increment it with their charges;
- if there is a cost element of type 1 and no cost element of type 2, create one cost element of type 2 with their charges;
- if there is a cost element of type 1 and one of type 2, increment this last one with their charges;
- find which other party the request should be sent to, either via static tables, or using a dynamic protocol as described in [7];
- convert all cost information to the appropriate currency.

Note that a roaming operator might use several AAA proxies or relays. In such a case, some of the nodes might carry the attribute transparently, while others will perform the above functions.

Upon reception of an authorization request containing a Cost-Advertisement attribute, and after successful authentication and other authorization is performed, the home server should:

- store cost elements received for this request;
- if there is a cost element of type 0 or of type 1, use it for credit-checking purposes and optional end-user cost advertisement;
- if the user does not pass credit-check tests, or rejects the cost, authorization can be rejected, and none of the attributes defined in this document need to be present;
- if there is a cost element of type 0, send it back in a Cost-Accept attribute (defined below), with a proper digital signature;
- if there is a cost element of type 1, deduct cost information from cost element of type 2 and any local costs that should be deducted, and send the result back in a Cost-Accept attribute (defined below), with a proper digital signature.
- if there is a maximum amount a user can be billed (e.g. pre-paid users), then information from the Cost-Advertisement attributes can be used to compute a maximum amount of time the user is allowed to be connected, and sent back to the requestor in appropriate AAA attributes.

Discussion:

One might want to be able to carry cost information of type 1 in the original currency, for inclusion on the end user's bill. However, since this information is used to compute compensation between the different parties, which happens in fixed currencies, the information must also be converted. An extra informational cost element might need to be introduced to address this issue, but it might make inconsistencies in currency conversion (which would otherwise be "hidden" in the commissions/charges) a bit too obvious.

Discussion:

One might want to be able to support a maximum commission that can be deducted from the amount billed to the end-user to compute the amount paid back to the visited network, and further charges would be added the amount billed to the end-user (reproducing what happens with credit cards, where merchants pay a fixed commission, but international transactions incur additional fees for the end-user). This would require using the cost element types differently: 0 would be the base amount, 1 would be commissions charged to the visited network, and 2 commissions charged to the end-user, for instance.

Discussion:

Using maximum credit to give a maximum connection time works only for duration-based billing. In other situations, a maximum cost information might be needed instead, with the usual options when that amount is used up: terminate, re-authenticate...

[8.2](#) Cost acceptance attribute

The cost acceptance attribute Cost-Accept (code TBD) is used in positive authorization responses, when the corresponding request contained a Cost-Advertisement attribute. A client that submits a request with a Cost-Advertisement attribute, but does not receive a Cost-Accept attribute in the associated positive response, knows that at least one node on the AAA path does not support these extensions, and can drop the connection.

The cost acceptance attribute is used to carry:

- for requests that used cost elements with types 1 and 2, information the charges that will be levied off the cost billed to the user by intermediate parties;
- for all requests, digital signatures from the upstream operator

Caron	Informational - Expires December 2002	10
INTERNET-DRAFT	AAA Cost Advertisement Extensions	June 2002

Flags	
Cost Data Type	Cost Data Length
Signature Type	Signature Length
Cost Data	
...	
Signature Data	
...	

- Flags is a bitmap of global flags. Currently, all bits are reserved, and should be set to 0.
- Cost Data Type indicates the type of cost information following. It can have the following values:
 - 0 indicates that this is the net cost that is accepted for this transaction. It should be the same as the cost in a type 0 cost element submitted in a Cost-Advertisement attribute in the corresponding request, or value lower than that submitted in a type 1 Cost-Advertisement attribute;
 - no other values are defined yet.
- Cost Data length is the length of the cost data information, in bytes, excluding types, lengths, and signature data.
- Signature type indicates the type of signature. The following values are defined:
 - 0 indicates a signature of type MD5
 - 1 indicates a signature of type SHA-1
- Signature length is the length of the signature data field.

- Cost data is encoded as described in [section 7](#).
- Signature data contains a signature of the type described in the Signature type field, computed over the Cost Data field, using the key of the sender of the attribute.

Caron Informational - Expires December 2002
INTERNET-DRAFT AAA Cost Advertisement Extensions

11
June 2002

Transmission of key or certificate information between roaming partners is outside the scope of this specification.

[9](#) Examples

To illustrate the use of the attributes defined in this document, we will describe some examples of scenarios using the setup defined in [section 6](#).

[9.1](#) Fixed visited network cost

In this scenario, the visited network wants to be paid a fixed amount (1 EUR per minute), whatever the cost may be for the end-user. The first roaming operator takes a 10% commission, and converts to USD before sending to the second roaming operator. This operator adds a 1 USD per connection + 0.15 USD per minute charge, and converts to AUD before sending to the home server, which charges the end-user whatever amount they want.

Totally fictitious currency rates used are:

- 1 EUR = 1.2 USD
- 1 USD = 2 AUD

A single-roundtrip EAP method is used here, to illustrate how Cost advertisement extensions are handled in this case. When using an EAP method with more roundtrips, subsequent roundtrips are exactly similar to the first one regarding cost information.

```
WISP --> ROAM1
Access-Request
User-Name=toto@home
Cost-Advertisement
Type 0=1 EUR/mn
```

ROAM1 --> ROAM2
Access-Request
User-Name=toto@home
Cost-Advertisement
Type0=1.32 USD/mn

ROAM2 --> HOME
Access-Request
User-Name=toto@home
Cost-Advertisement
Type0=2 AUD + 2.94 AUD/mn

Caron Informational - Expires December 2002
INTERNET-DRAFT AAA Cost Advertisement Extensions

12
June 2002

ROAM2 <-- HOME
Access-Challenge
EAP-Message=EAP/Request/Method

ROAM1 <-- ROAM2
Access-Challenge
EAP-Message=EAP/Request/Method

WISP <-- ROAM1
Access-Challenge
EAP-Message=EAP/Request/Method

WISP --> ROAM1
Access-Request
User-Name=toto@home
EAP-Message=EAP/Response/Method
Cost-Advertisement
Type 0=1 EUR/mn

ROAM1 --> ROAM2
Access-Request
User-Name=toto@home
EAP-Message=EAP/Response/Method
Cost-Advertisement
Type0=1.32 USD/mn

ROAM2 --> HOME
Access-Request
User-Name=toto@home
EAP-Message=EAP/Response/Method

Cost-Advertisement
Type0=2 AUD + 2.94 AUD/mn

ROAM2 <-- HOME
Access-Accept
EAP-Message=EAP/Success
Cost-Accept
Type0=2 AUD + 2.94 AUD/mn
Signature by HOME

ROAM1 <-- ROAM2
Access-Accept
EAP-Message=EAP/Success
Cost-Accept
Type0=1.32 USD/mn
Signature by ROAM2

WISP <-- ROAM1
Access-Challenge
EAP-Message=EAP/Success

Caron Informational - Expires December 2002
INTERNET-DRAFT AAA Cost Advertisement Extensions

13
June 2002

Cost-Accept
Type0=1 EUR/mn
Signature by ROAM1

[9.2](#) Fixed end-user cost

In this scenario, the visited network wants to set the cost for the end-user (10 EUR), and will receive this less the commissions charged by intermediaries. ROAM1 wants 10% of the total (which is different from what happens in the first scenario), and converts to USD before sending to ROAM2. This one in turn wants 1 USD per connection, and converts to AUD before sending to HOME. HOME wants 20% of the total cost.

The initial EAP roundtrips are not shown here.

WISP --> ROAM1
Access-Request
User-Name=toto@home
EAP-Message=EAP/Response/Method
Cost-Advertisement
Type 1=10 EUR

ROAM1 --> ROAM2

Access-Request
User-Name=toto@home
EAP-Message=EAP/Response/Method
Cost-Advertisement
Type1=12 USD
Type2=1.2 USD

ROAM2 --> HOME
Access-Request
User-Name=toto@home
EAP-Message=EAP/Response/Method
Cost-Advertisement
Type1=24 USD
Type2=4.4 USD

ROAM2 <-- HOME
Access-Accept
EAP-Message=EAP/Success
Cost-Accept
Type0=19.2 AUD
Signature by HOME

ROAM1 <-- ROAM2
Access-Accept
EAP-Message=EAP/Success
Cost-Accept

Caron Informational - Expires December 2002
INTERNET-DRAFT AAA Cost Advertisement Extensions

14
June 2002

Type0=8.6 USD
Signature by ROAM2

WISP <-- ROAM1
Access-Challenge
EAP-Message=EAP/Success
Cost-Accept
Type0=6.45 EUR
Signature by ROAM1

[10](#) Security Considerations

In a roaming environment, where AAA transactions result in money exchanges, it is important that security of these transactions is guaranteed. For this reason, one should:

- use only secure AAA mechanisms, such as Diameter or RADIUS over IPsec.

- ensure that strong authentication mechanisms (such as EAP-SRP [8], EAP-TLS [9]...) are used.

Also, to ensure non-repudiation of cost acceptance, this specification introduces digital signature of Cost-Accept attributes. Proper security measures to protect the keys used should be put in place to ensure the validity of these signatures.

11 References

- 1 [RFC 2865](#), C. Rigney, Willens, S., Rubens, A., Simpson, W., "Remote Authentication Dial In User Service (RADIUS)", [RFC 2865](#), June 2000.
- 2 [RFC 2866](#), C. Rigney, "RADIUS Accounting", [RFC 2866](#), June 2000.
- 3 [RFC 2869](#), C. Rigney, Willats, W., Calhoun, P., "RADIUS Extensions", [RFC 2869](#), June 2000.
- 4 <[draft-ietf-aaa-diameter-10-2.txt](#)>, P. Calhoun, Arkko, J., Guttman, E., Zorn, G., Louhney, J., "Diameter Base Protocol", work in progress, April 2002.
- 5 [RFC 2119](#) Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997
- 6 [RFC 2486](#), B. Aboba, Beadles, M., "The Network Access Identifier", [RFC 2486](#), January 1999.

Caron	Informational - Expires December 2002	15
INTERNET-DRAFT AAA Cost Advertisement Extensions		June 2002

- 7 <[draft-caron-dns-based-roaming-00.txt](#)>, Caron, J., "DNS-Based Roaming", April 2000, work in progress.
- 8 <[draft-ietf-pppext-eap-srp-03.txt](#)>, Carlson, J., B. Aboba, H. Haverinen, "EAP SRP-SHA1 Authentication Protocol", July 2001, work in progress.
- 9 [RFC 2716](#), Aboba, B., D. Simon, "PPP EAP TLS Authentication Protocol", October 1999.

Caron Informational - Expires December 2002
INTERNET-DRAFT AAA Cost Advertisement Extensions

16
June 2002

[12](#) Author's Address

Jacques Caron
IP Sector Technologies

Ecluse 36c
2000 Neuchatel
Switzerland
Phone: +41 79 699 8389
Email: jcaron@ipsector.com