INTERNET DRAFT   Jari Arkko
Category: Standards Track   Oy LM Ericsson Ab
Title: draft-calhoun-diameter-accounting-00.txt   Pat R. Calhoun
Date: September 1999   Sun Microsystems, Inc.
                                                    Pankaj Patel
                                            Convergys Corporation
                                                       Glen Zorn
                                            Microsoft Corporation

DIAMETER Accounting Extension

Abstract

   The DIAMETER protocol provides Authentication and Authorization for
   dial-up PPP clients [2] and for Mobile-IP [3]. The ROAMOPS WG has
   been working on an accounting data format, called Accounting Data
   Interchange Format (ADIF) [10], as a method to transfer accounting

   information over a wide variety of transports. This document describes
   how ADIF can be securely transmitted over the DIAMETER protocol.

Table of Contents

1.0 Introduction

   The DIAMETER protocol provides Authentication and Authorization for
   dial-up PPP clients [2] and for Mobile-IP [3]. The ROAMOPS WG has
   been working on an accounting data format, called Accounting Data
   Interchange Format (ADIF) [10], as a method to transfer accounting
   information over a wide variety of transports. This document
   describes how ADIF can be securely transmitted over the DIAMETER
   protocol.

   This document describes how Accounting Records can be transmitted
   within the DIAMETER protocol in a secure fashion, even when the
   messages must traverse DIAMETER proxies [1, 9]. This extension allows
   for both real-time and batched accounting transfers.

   This document introduces AVPs that are very similar to some found in
   the base [1] and the end-to-end security extension [9]. However,
   since this extension requires that the AVPs in question must have
   bits set which are not currently permitted in both the stated drafts,
   a new version of the AVP has been defined here. However, a future

version of this document may make use of the original AVPs once the
[1] and [9] have been corrected. If there is interest in this
extension, the impact of changing [1] and [9] must be carefully
evaluated.

The Extension number for this draft is five (5). This value is used
in the Extension-Id Attribute value Pair (AVP) as defined in [7].

1.1 Copyright Statement

1.2 Requirements language

In this document, the key words "MAY", "MUST, "MUST NOT", "optional",
"recommended", "SHOULD", and "SHOULD NOT", are to be interpreted as
described in [6].

2.0 Command Codes

This section will define the Commands [1] for DIAMETER
implementations supporting the Mobile IP extension.

```
    Command Name            Command Code
    ---------------------------------
    Accounting-Request        ???
    Accounting-Answer         ???
```


2.1 Accounting-Request

Description

The Accounting-Request command is sent by a DIAMETER node in order
to exchange accounting information with a peer. The Accounting
information is contained within an ADIF record, as described in
[10].

The Accounting-request command MAY contain accounting information
for more than a single session, which allows it to send batched
accounting information. When the batch mode is used, the session-
Id AVP [1] and the Digital-Signature AVP [6] MUST be present, and
MUST have a tag of the same value as the ADIF-Record AVP.

Message Format

```
<Accounting-Request> ::= <DIAMETER Header>
                         <Accounting-Request Command AVP>
                         <Host-IP-Address AVP>
                         [<Host-Name AVP>]
                         (<Accounting-Session-Id AVP> &&
                          <Accounting-Record-Type> &&
                          <User-Name AVP> &&
                          <ADIF-Record AVP> &&
                          <Accounting-Digital-Signature AVP)
                         <Timestamp AVP>
                         <Initialization-Vector AVP>
                         {<Integrity-Check-Vector AVP> ||
                          <Digital-Signature AVP }
```

AVP Format

   A summary of the Accounting-Request packet format is shown below.
   The fields are transmitted from left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          AVP Code                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        AVP Length         |CFlags |C|Z|Reservd|P|E|T|V|H|M|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Command Code                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

AVP Code

   256   DIAMETER Command

AVP Length

   The length of this attribute MUST be 12.

Command Flags

   The Command Flags MUST be set to zero.

AVP Flags

   The 'M' bit MUST be set. The 'P' bits MAY be set if end to end
   message integrity is required. The 'E', 'V', 'H' and 'T' bits
   MUST NOT be set.

Command Code

The Command Code field MUST be set to ??? (Accounting-Request).

2.2 Accounting-Answer

Description

The Accounting-Answer command is used to acknowledge an
Accounting-Request command. The Accounting-Answer command contains
the same Accounting-Session-Id AVP that was sent in the
Accounting-Request command, and the MD5 hash in Accounting-
Confirmation AVP forms a confirmation that the right accounting
record was accepted. This can be signed using the Accounting-
Digital-Signature AVP for end-to-end message integrity and
possible non-repudiation.

Only the target DIAMETER Server, known as the home DIAMETER
Server, SHOULD respond with the Accounting-Answer command.

If the Accounting-Request command contained more than one ADIF-
Record AVP, the Accounting-Answer SHOULD contain the same number
of ADIF-Record AVPs. However, it is possible for the DIAMETER
Server to acknowledge each ADIF-Record in a separate response.
This allows the sender of the ADIF-Records to send a batch of
records, whose final destination are different.

Message Format

```
<Accounting-Answer> ::= <DIAMETER Header>
                        <Accounting-Answer Command AVP>
                        <Result-Code AVP>
                        <Host-IP-Address AVP>
                        [<Host-Name AVP>]
                        (<Accounting-Session-Id AVP> &&
                         <Result-Code AVP>
                         <Accounting-Confirmation AVP> &&
                         <Accounting-Digital-Signature AVP)
                        <Timestamp AVP>
                        <Initialization-Vector AVP>
                        {<Integrity-Check-Vector AVP> ||
                         <Digital-Signature AVP }
```
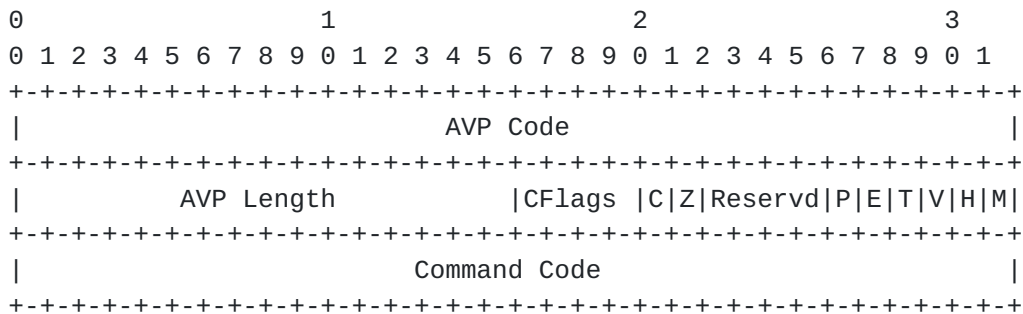
AVP Format

A summary of the Accounting-Answer packet format is shown below.
The fields are transmitted from left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          AVP Code                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          AVP Length          |CFlags |C|Z|Reservd|P|E|T|V|H|M|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Command Code                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

AVP Code

    256   DIAMETER Command

AVP Length

    The length of this attribute MUST be 12.

Command Flags

    The Command Flags MUST be set to zero.

AVP Flags

    The 'M' bit MUST be set. The 'P' bits MAY be set if end to end
    message integrity is required. The 'E', 'V', 'H' and 'T' bits
    MUST NOT be set.

Command Code

    The Command Code field MUST be set to ??? (DIAMETER-EAP-
    Answer).

3.0 DIAMETER AVPs

This section will define the mandatory AVPs which MUST be supported
by all DIAMETER implementations supporting this extension. The
following AVPs are defined in this document:

    Attribute Name   Attribute Code

    Accounting-Session-Id   ???
    Accounting-Record-Type   ???
    ADIF-Record   ???
    Accounting-Confirmation   ???
    Accounting-Digital-Signature   ???

      Accounting-Interim-Interval   ???

3.1 Accounting-Session-Id

   Description

      The Accounting-Session-Id AVP contains the same value as the
      session-Id [1] AVP, but has different rules. This AVP MAY
      have the tag bit set in order to allow accounting records to
      be sent in batches via the DIAMETER protocol.

   AVP Format

```
       0                   1                   2                   3
       0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                            AVP Code                           |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |         AVP Length          |      Reserved      |P|E|T|V|H|M|
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |    Data ...
       +-+-+-+-+-+-+-+-+
```

      AVP Code

         ???   Accounting-Session-Id

      AVP Length

         The length of this attribute MUST be at least 8.

      AVP Flags

         The 'M' bit MUST be set. The 'T' bit MAY be set if more than
         one Accounting record is being sent in an Accounting-Request
         message. The 'P' bit MAY be set if end to end message
         integrity is required, but may not be necessary if the
         Accounting-Digital-Signature is used. The 'H', 'E', 'V' bits
         MUST NOT be set.

       Data

         The Data field contains a Session-Id AVP as defined in [1].

3.2 Accounting-Record-Type

Description

   The Accounting-Record-Type AVP contains the type of record that
   can be found in the ADIF-Record AVP.

AVP Format

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          AVP Code                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         AVP Length            |     Reserved    |P|E|T|V|H|M|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Integer32                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

   AVP Code

      ???   Accounting-Record-Type

   AVP Length

      The length of this attribute MUST be at least 8.

   AVP Flags

      The 'M' bit MUST be set. The 'T' bit MAY be set if more than
      one Accounting record is being sent in an Accounting-Request
      message. The 'P' bit MAY be set if end to end message
      integrity is required, but may not be necessary if the
      Accounting-Digital-Signature is used. The 'H', 'E', 'V' bits
      MUST NOT be set.

   Integer32

      The Integer32 field contains the record type that can be found
      in the ADIF-Record AVP. The following values are currently
      defined:

         EVENT_RECORD   1
            An Accounting Event Record is used to indicate a service
            of indivisible nature has occurred. This record contains
            all information relevant to the service, and is the only
            record of the service.

         SESSION_RECORD   2
            An Accounting Session Record is used to indicate that a

service of a measurable length has been given. This
record contains all information relevant to the service,
and is the only record of the service.

START_RECORD   3
An Accounting Start Record is used to initiate an
accounting session, and contains accounting information
that is relevant to the initiation of the session.

INTERIM_RECORD   4
An Interim Accounting Record contains cumulative
accounting information for an existing Accounting
session. Interim Accounting Records SHOULD be sent
everytime a re-authentication or re-authorization occurs.

STOP_RECORD   5
An Accounting Stop Record is sent to terminate an
accounting session and contains cumulative accounting
information relevant to the existing session.

START_RECORD, INTERIM_RECORD, and STOP_RECORD are used as an
alternative mechanism to represent SESSION_RECORDs, but to give
more timely information about the session to the DIAMETER
Server. The selection of whether to use these records is
directed by the Accounting-Interim-Interval AVP.

3.3 ADIF-Record

Description

This attribute contains an ADIF record, as defined in [10].

AVP Format

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           AVP Code                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        AVP Length          |     Reserved      |P|E|T|V|H|M|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Data ...
+-+-+-+-+-+-+-+-+
```

AVP Code

???   ADIF-Record

    AVP Length

       The length of this attribute MUST be at least 8.

    AVP Flags

       The 'M' bit MUST be set. The 'T' bit MAY be set if more than
       one Accounting record is being sent in an Accounting-Request
       message. The 'P' bit MAY be set if end to end message
       integrity is required, but may not be necessary if the
       Accounting-Digital-Signature is used. The 'H', 'E', 'V' bits
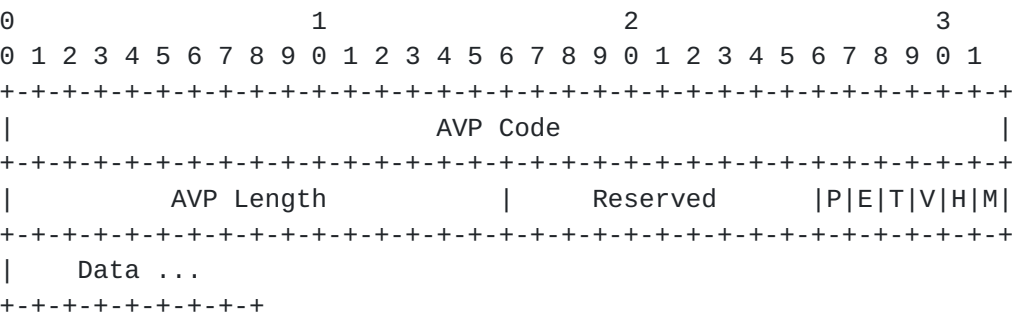   MUST NOT be set.

    Data

       The Data field contains an ADIF payload as defined in [10].

3.4 Accounting-Confirmation

  Description

     This AVP contains an MD5 hash of a previous ADIF-Record, and is
     used to confirm receipt of the ADIF-Record. When signed via the
     Accounting-Digital-Signature, this AVP provides the sender of the
     Accounting-Request with proof that the receiver accepted the
     Accounting record.

  AVP Format

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |                          AVP Code                            |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |         AVP Length          |     Reserved      |P|E|T|V|H|M|
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |    Data ...
     +-+-+-+-+-+-+-+-+
```

    AVP Code

       ???   Accounting-Confirmation

    AVP Length

       The length of this attribute MUST be at least 8.

AVP Flags

   The 'M' bit MUST be set. The 'T' bit MAY be set if more than
   one Accounting record is being sent in an Accounting-Request
   message. The 'P' bit MAY be set if end to end message
   integrity is required, but may not be necessary if the
   Accounting-Digital-Signature is used. The 'H', 'E', 'V' bits
   MUST NOT be set.

Data

   The Data field contains an MD5 hash of the ADIF-Record AVP
   being confirmed.

[3.5](#) Accounting-Digital-Signature

Description

   The Accounting-Digital-Signature is similar to the Digital-
   Signature described in [9], except that it is used to sign all
   AVPs with the same tag value as the one found in this AVP.

AVP Format

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           AVP Code                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         AVP Length          |    Reserved      |P|E|T|V|H|M|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Address                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Transform ID                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Data ...
+-+-+-+-+-+-+-+-+
```

AVP Code

   ???   Accounting-Digital-Signature

AVP Length

   The length of this attribute MUST be at least 17.

AVP Flags

The 'M' and 'T' bits MUST be set. The 'P', 'H', 'E' and 'V'
bits MUST NOT be set.

Address

The Address field contains the IP address of the DIAMETER host
which generated the Digital-Signature.

Transform ID

The Transform ID field contains a value that identifies the
transform that was used to compute the signature. The following
values are defined in this document:

RSA [9]   1

Data

The Data field contains a digital signature of all AVPs within
the message that have the same AVP tag as the one found in this
AVP.

3.6 Accounting-Certificate

Description

The Accounting-Certificate AVP is created by the home DIAMETER
server as a result of a successful Authentication and/or
Authorization. This "token" is used in the subsequent Accounting-
Request messages as a proof that the user was in fact authorized
for the service. The document [7] and section 4.1 provides further
information on this AVP.

AVP Format

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            AVP Code                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          AVP Length            |     Reserved      |P|E|T|V|H|M|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Length of Session-Id      |Length of Accounting-Session-Id|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Length of User-Name       |  Length of Digital-Signature  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Digital-Signature Transform    |            Reserved           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Session-Lifetime                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            Timestamp                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Session-Id...          |     Accounting-Session-Id    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          User-Name...           |      Digital-Signature...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
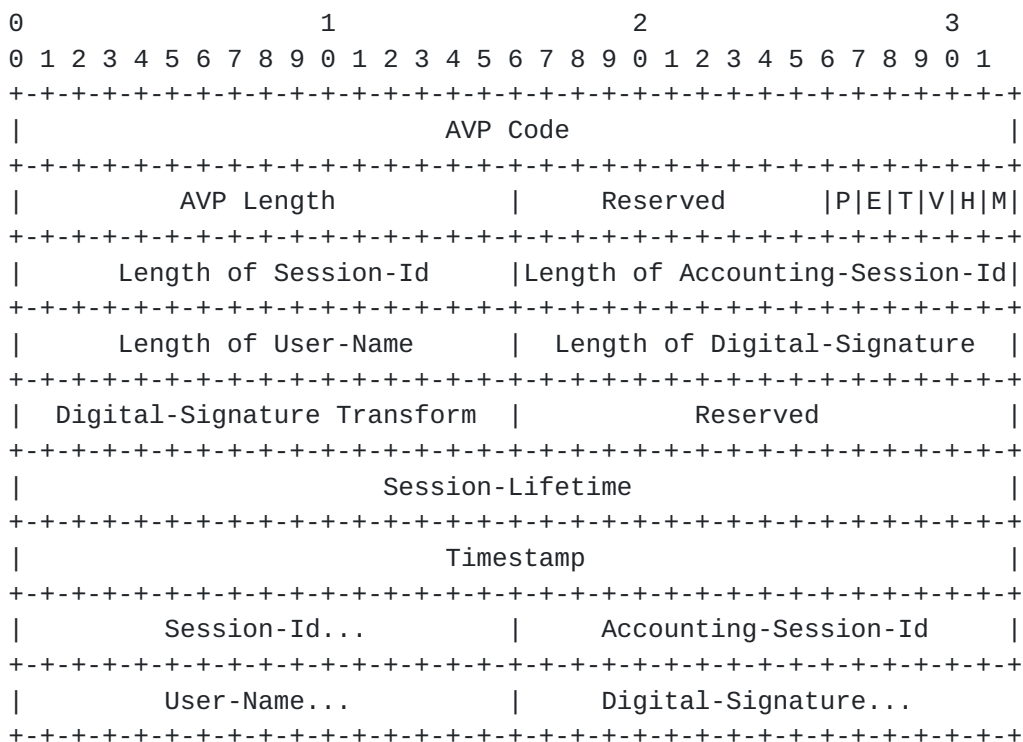
AVP Code

   ???   Accounting-Certificate

AVP Length

   The length of this attribute MUST be at least 32.

AVP Flags

   The 'M' bit MUST be set. The 'T' bit MAY be set if more than
   one Accounting record is being sent in an Accounting-Request
   message. The 'P' bit MAY be set if end to end message
   integrity is required, but may not be necessary if the
   Accounting-Digital-Signature is used. The 'H', 'E', 'V' bits
   MUST NOT be set.

Length of Session-Id

   This 16 bit field contains the length of the Session-Id field
   found in this AVP.

Length of Accounting-Session-Id

   This 16 bit field contains the length of the locally generated
   Accounting-Session-Id value that is found in this AVP.

Length of User-Name

   This 16 bit field contains the length of the User-Name field
   found in this AVP.

Length of Digital-Signature

   This 16 bit field contains the length of the Digital-Signature
   field found in this AVP.

Digital-Signature Transform

   This 16 bit field contains the transform used to generate the
   Digital-Signature field, as defined in the Digital-Signature
   AVP in [9].

Session-Lifetime

   This 32 bit field contains the number of seconds that the
   session has been autorized for. This field MUST be the same as
   the value of the Session-Timeout AVP [1].

TimeStamp

   This 32 bit field contains a timestamp representing when this
   AVP was created. The format of this field is identical to the
   Timestamp AVP defined in [1].

Session-Id

   This variable length field contains the Session-Id, and MUST be
   identical to the value found in the Session-Id AVP [1].

Accounting-Session-Id

   This variable length field contains a Session-Id created by the
   home DIAMETER server for the purposes to matching accounting
   records.

User-Name

   This variable length field contains the User-Name and MUST be
   identical to the value of the User-Name AVP [1].

Digital-Signature

   This variable length field contains a signature of the AVP's
   data, not including the AVP header and is generated using the

transform specified in the Digital-Signature-Transform field.

[3.7](#) Accounting-Interim-Interval

Description

The Accounting-Interim-Interval AVP is sent from the DIAMETER
authenticating/authorizing server to the DIAMETER Client. The
Client uses information in the AVP to decide how and when to
produce accounting records. With different values in this AVP,
service sessions can result in one, two, or two+N accounting
records, based on the needs of the home-organization.

AVP Format

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           AVP Code                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          AVP Length           |    Reserved    |P|E|T|V|H|M|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            Value                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
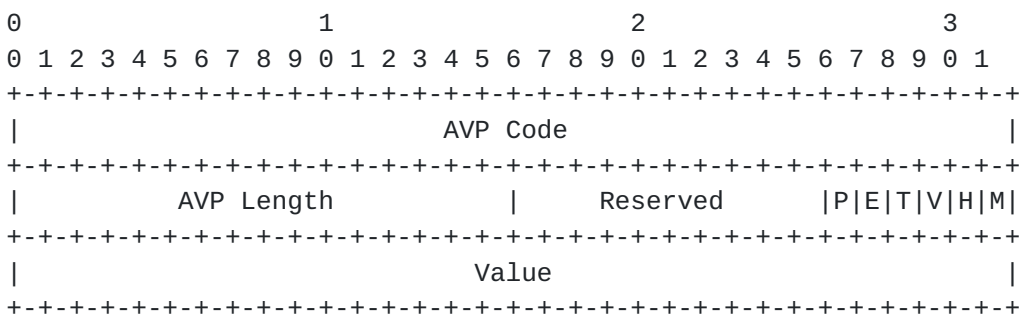
AVP Code

   ???   Accounting-Interim-Interval

AVP Length

   The length of this attribute MUST be 12.

AVP Flags

   As defined in the DIAMETER Base Protocol.

Value

   The following accounting record production behaviour is
   directed by the inclusion of this AVP:

      1. The omission of the Accounting-Interim-Interval AVP means
      that only a SESSION_RECORD or EVENT_RECORD records are
      produced from the service.

      2. The inclusion of the AVP with Value field set to 0 means

that START_RECORD and STOP_RECORD records are produced.

3. The inclusion of the AVP with Value field set to a non-
zero value means that START_RECORD, INTERIM_RECORD, and
STOP_RECORD records are produced. The DIAMETER Client SHOULD
that INTERIM_RECORD records are produced roughly in with the
interval which is the number in the Value field of this AVP
interpreted as the number of seconds. The Client MUST ensure
that the interim record production times are randomized so
that large accounting packet storms are not created either
among records or around a common service start time.

4.0 Protocol overview

This accounting protocol is based on an authorization-server directed
model with capabilities for both efficient batch and fast real-time
delivery of accounting information. Several fault resilience methods
[11] have been built in to the protocol in order minimize loss of
accounting data in various fault situations and under different
assumptions about the capabilities of the used devices.

4.1 Authorization-Server Directed Model

The authorization-server directed model means that at authorization
time, the device generating the accounting data gets information from
the authorization server regarding the way accounting data shall be
forwarded. This information includes a certificate to prove that the
session truly was authorized, as well as accounting record timeliness
requirements.

When the user's home DIAMETER Server successfully authenticates
and/or authorizes a session, it generates the Accounting-Certificate
AVP that is returned in the response. The document [7] describes a
possible format for the AVP, which is also described in section 3.6.

As discussed in [11], batch transfer of accounting data is more CPU-
and bandwidth efficient than real-time transfer. However, there are
many applications where real-time transfer is a requirement for at
least some of the accounting records. These applications include
roaming, where most (local) accounting records can be transferred in
batch mode, but roaming (visiting) accounting records should be
transferred fast due to the needs of credit limit checks and fraud
detection. For these reasons this accounting protocol defines both
batch and real-time transfer modes, and allows their use
simultaneously. The authorization server (chain) directs the
selection of proper transfer strategy, based on its knowledge of the

user and relationships of roaming partnerships. The server (or
proxies in between) use the Accounting-Delivery-Max-Batch,
Accounting-Delivery- Max-Delay, and Accounting-Interim-Interval AVPs
to control the operation of the DIAMETER Client. The first two
attributes set the requirements in terms of number of records and
maximum delay before accounting data transfer for this session SHOULD
begin. The DIAMETER Client MAY deliver the data earlier due to a
full batch of records, device reboot, lack of memory, or explicit
configuration. The DIAMETER Client MUST begin the transfer in the
given limits unless prevented from doing so by network partitions,
client or server failures, network congestion, or client overload.

The Accounting-Interim-Interval AVP, when present, instructs the
DIAMETER Client to produce accounting records continuously even
during a session.

Typically, the authorization server uses a few batching/real-time
classes, such as the local users whose data might be transferred once
in an hour and the roaming users whose data would be transferred
immediately. Each Accounting-Delivery-Max-Batch / Accounting-
Delivery- Max-Delay AVP pair with different values forms one pool of
accounting data in the DIAMETER Client. That is, a new record is
placed to same pool as the previous one if the authorization server
returned same values for both AVPs and the pool has not been emptied
in between.

4.2 Protocol Messages

The DIAMETER Client generating the accounting data will use the
Accounting-Request message to send one or more accounting records to
the DIAMETER Server. The Server MUST reply with the Accounting-Answer
message with appropriate confirmations.

It is possible that a DIAMETER Proxy breaks up a batch of accounting
records and sends them towards different DIAMETER Home Servers. In
this case it is possible that a separate Accounting-Answer message
contain the response for each block. Therefore, a Client MUST be
prepared to handle this scenario.

Upon receipt of an Accounting-Request, a home DIAMETER Server MUST
generate a response. The response includes the Result-Code, which MAY
contain an error if the ADIF-Record, or some other AVP, is not
acceptable. Furthermore, an Accounting-Confirmation MUST be returned.
The Accounting-Confirmation is an MD5 hash of the ADIF-Record data
which is being confirmed.

Each DIAMETER Accounting protocol message MAY be compressed using

IPComp in order to reduce the used network bandwidth. DIAMETER peers
MUST use a negotiation mechanisms such as ISAKMP/IKE in order to
ensure that both peers are able to handle IPComp. Note that it
usually makes sense to compress only Accounting-Request messages with
possibly lengthy ADIF data, not Accounting-Answer messages.

[4.3](#) Fault Resilience

DIAMETER Base protocol mechanisms are used to overcome small packet
loss and network faults of temporary nature.

DIAMETER Clients MUST implement the use of alternate servers to guard
against server failures and certain network failures. DIAMETER
Servers or related off-line processing systems MUST detect duplicate
accounting records caused by the sending of same record to several
servers and duplication of messages in transit. This detection MUST
be based on the inspection of Accounting-Record-Id and Host-IP-
Address AVP pairs.

DIAMETER Clients MAY have non-volatile memory for the safe storage of
accounting records over reboots or extended network failures, network
partitions, and server failures. If such memory is available the
Client SHOULD store new accounting records there as soon as the
records are created and until a positive acknowledgement of their
reception from the DIAMETER Server has been received. Upon a reboot,
the Client MUST starting sending the records in the non-volatile
memory to the accounting server with appropriate modifications in
termination cause, session length, and other relevant information in
the records.

A further extension of this protocol may include AVPs to control how
many accounting records may at most be stored in the DIAMETER Client
without committing them to the non-volatile memory or transferring
them to the DIAMETER Server.

The Client SHOULD NOT remove the accounting data from any of its
memory areas before the correct Accounting-Answer has been received.
The Client MAY remove oldest, undelivered or yet unacknowledged
accounting data if it runs out of resources such as memory. It is an
implementation dependent matter for the client to accept new sessions
under this condition.

[4.4](#) Session Records

In all accounting records the Accounting-Session-Id AVP, ADIF-Record
AVP, and User-Name AVPs MUST be present. If only one accounting
record is present in the message, the whole message may be protected

using the Digital-Signature, as defined in [9].

However, if the accounting records are being in sent in batch mode, the sender can create several "blocks" of accounting records by making use of the AVP Tag field (bit 'T' [1]). Each block is individually signed, unless all blocks are destined for the same home DIAMETER Server.

Different types of session records are sent depending on the actual type of accounted service and the authorization server's directions for interim accounting. If the accounted service is of an indivisible nature, then the Accounting-Record-Type AVP MUST be present and set to the value EVENT_RECORD. This can be used to account for services such as "send an e-mail to this wireless terminal". If the accounted service is of a measurable length, then the AVP MUST contain the value SESSION_RECORD. In both cases only one accounting record is generated.

If the authorization server has directed interim accounting to be on but with no specified interim interval, two accounting records MUST be generated for each service of type SESSION_RECORD. When the initial Accounting-Request is sent for a given session is sent, the Accounting-Record-Type AVP MUST be set to the value START_RECORD. When the last Accounting-Request is sent, the value MUST be STOP_RECORD.

If a specified interim interval exists, the DIAMETER Client MUST produce additional records between the START_RECORD and STOP_RECORD, marked INTERIM_RECORD. The production of these records is directed both by Accounting-Interim-Interval as well as any re-authentication or -authorization of the session. If a batch size of greater than 1 has been specified by the authorization server, then the DIAMETER Client MUST ensure that new interim records overwrite previous interim records for the same session and batch as this reduces the amount of memory required to store the records. In effect, this means that interim records are delivered at least as often as dictated by Accounting-Delivery-Max-Delay.

5.0 IANA Considerations

The numbers for the Command Code AVPs (section 2) is taken from the numbering space defined for Command Codes in [1]. The numbers for the various AVPs defined in section 3 were taken from the AVP numbering space defined in [1]. The numbering for the AVP and Command Codes MUST NOT conflict with values specified in [1] and other DIAMETER related Internet Drafts.

This document introduces the Accounting-Record-Type AVP, which may
contain pre-defined values. This document defines the values 1-3.
All remaining values are available for assignment via IETF Consensus
[8].

6.0 Acknowledgments

Thanks to the various people that have contributed to accounting
related requirements at the IETF. This document could not have been
put together without all of those napkin design sessions.

7.0   References

[1] P. R. Calhoun, A. Rubens, "DIAMETER Base Protocol",
    draft-calhoun-diameter-08.txt, Work in Progress,
    August 1999.
[2] P. R. Calhoun, "DIAMETER Authentication Extension",
    draft-calhoun-diameter-auth-06.txt, Work in Progress,
    August 1999.
[3] P. R. Calhoun, C. Perkins, "DIAMETER Mobile IP Extension",
    draft-calhoun-diameter-mobileip-02.txt, Work in Progress,
    August 1999.
[4] C. Rigney, A. Rubens, W. Simpson, S. Willens, "Remote
    Authentication Dial In User Service (RADIUS)." RFC 2138,
    April 1997.
[5] C. Rigney, "RADIUS Accounting." RFC 2139, April 1997.
[6] S. Bradner, "Key words for use in RFCs to Indicate
    Requirement Levels", BCP 14, RFC 2119, March 1997.
[7] G. Zorn, P. R. Calhoun, "Limiting Fraud in Roaming",
    draft-ietf-roamops-fraud-limit-00.txt, May 1999.
[8] Narten, Alvestrand,"Guidelines for Writing an IANA
    Considerations Section in RFCs", BCP 26, RFC 2434,
    October 1998
[9] P. Calhoun, W. Bulley, "DIAMETER Proxy Server Extensions",
     draft-calhoun-diameter-proxy-02.txt, Work in Progress,
     August 1999.
[10] B. Aboba, D. Lidyard, "The Accounting Data Interchange
    Format (ADIF)", draft-ietf-roamops-actng-05.txt,
    Work in Progress, November 1998.
[11] B. Aboba, J. Arkko. Introduction to Accounting Management.
     draft-aboba-acct-01.txt. Work in progress, June 1999.

8.0 Authors' Addresses

    Questions about this memo can be directed to:

    Jari Arkko
    Oy LM Ericsson Ab
    02420 Jorvas
    Finland

     Phone: +358 40 5079256
    E-Mail: Jari.Arkko@ericsson.com

    Pat R. Calhoun
    Network and Security Research Center, Sun Labs
    Sun Microsystems, Inc.
    15 Network Circle
    Menlo Park, California, 94025
    USA

     Phone: 1-650-786-7733
       Fax: 1-650-786-6445
    E-mail: pcalhoun@eng.sun.com

    Pankaj Patel
    Convergys Corporation
    4600 Montgomery Road
    Cincinnati, OH 45212
    USA

     Phone: 1-513-723-2018
    E-Mail: pankaj.patel@convergys.com

    Glen Zorn
    Microsoft Corporation
    One Microsoft Way
    Redmond, WA 98052
    USA

     Phone: 1-425-703-1559
    E-Mail: gwz@acm.org

9.0 Full Copyright Statement