Internet Engineering Task Force
INTERNET DRAFT

Ping Pan (Bell Labs)
Henning Schulzrinne (Columbia U)
Pat Calhoun (Sun)
15 November 1998

DIAMETER: Policy and Accounting Extension for SIP
draft-pan-diameter-sip-01.txt

Status of This Memo

Abstract

This document describes a policy and accounting information exchange mechanism between a DIAMETER policy server and a SIP proxy server. A DIAMETER server is responsible for maintaining a user policy and accounting database and a means to update it. A SIP proxy server needs to contact a DIAMETER server during multimedia session setup and teardown time to perform admission control and accounting tasks.

To provide proper data-forwarding level service guarantees to the SIP sessions, the DIAMETER servers are also responsible for interfacing

with the network resource management database. However, this is beyond the scope of this document.

The objectives of the proposed DIAMETER extension are 1) providing accurate accounting information, 2) flexible and 3) simple to implement. The protocol does not make any assumption about policy and billing algorithms at DIAMETER servers.

Contents

1. Introduction

DIAMETER [ZPC98] is a proposed successor to RADIUS[RRSW97]. It defines a base protocol [RC98] for policy information exchange among policy-enable entities, and thus provides a common protocol interface to services such as AAA (Authentication, Authorization and Accounting), network-edge resource management and VPN (Virtual Private Network).

SIP [HSSJ98] (Session Initiation Protocol) allows end users to establish and control multimedia sessions over the Internet. End users may choose SIP to set up IP telephone calls as an alternative to other protocols such as H.323. However, some of the important commercial telephony service elements (for example, user accounting, policy and billing systems) are beyond scope of SIP.

This document describes a policy/accounting mechanism that interfaces between SIP proxy servers and policy servers. The mechanism provides a vehicle for call admission control, and per-user per-call billing when used by ISP's at network edge. Figure-1 illustrates the proposed model.

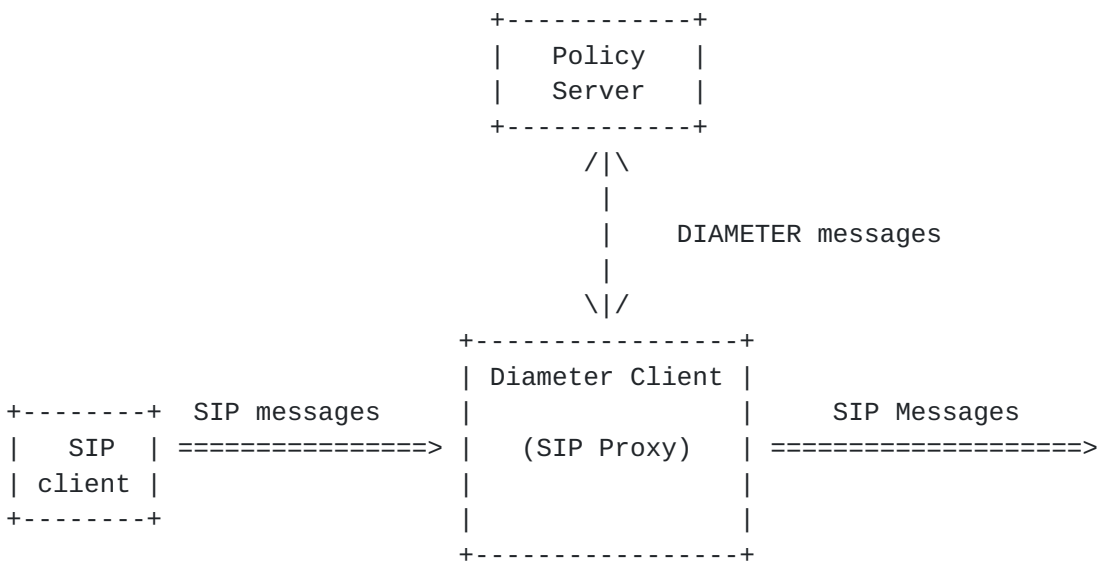


Figure-1: A model for SIP/DIAMETER interface.

The proposal is designed based on the following assumptions:

1. A policy server is the central decision entity. The clients (that is, SIP proxy servers) should always forward the

information to the server. However this does not preclude a client from maintaining a policy information cache for performance optimization purposes.

2. A policy server maintains a policy and accounting database for all users within an administrative domain, and a means to update it.

3. The extension relies on the DIAMETER base protocol to provide massaging reliability. There is no need to implement other reliable message delivery mechanisms between clients and servers.

The proposed extension does not perform policy and accounting processing itself. It is important to remember:

1. The protocol does NOT make any assumptions about the policy decision and accounting algorithms used at servers, rather it carries "decisions" in response to policy requests.

2. The protocol does NOT make any assumptions about the implementation details of the SIP proxy server. However, when a policy event takes place, a SIP proxy must send all relevant information to the server for policy evaluation.

3. The communication mechanism among policy servers is NOT in the scope of this document.

4. To provide IP telephone service, it may require some sort of interaction between the policy server at the caller-side and the one at the callee-side. However, such interaction requires further investigation and is not included in this document.

2. Terminology

- Caller: The device that initiating a session invitation. Throughout the draft, we assume a caller is a SIP proxy server that sets up sessions for telephone users at a source network.

- Callee: The device that a caller is trying to invite to a session. We assume a callee is a SIP proxy server that manages sessions for telephone users at a remote network.

- Policy Server: A host or router that stores policy rules, and is capable to communicate with its clients via DIAMETER protocol.

- Client: A SIP proxy server that interface with a "trusted" policy server to perform policy and accounting checking, and some

level of admission control. A client can be a SIP caller, or a SIP callee, or both.

- Policy Event: The event that takes place at a client and requires policy checking. Such event could be the reception of a SIP INVITE, ACK, CANCEL, or BYE message.

- Policy Event Message: The message that triggers a policy event at a client.

- AVP: The DIAMETER protocol consists of a header followed by objects. Each object is encapsulated in a header known as an Attribute-Value-Pair.

3. Description of Operation

3.1. Outline

DIAMETER client (in this case, SIP Proxy Server) and policy server exchange DIAMETER messages to open and confirm a client-server connection at boot-up time. The initial data between a policy server and a client are device availability, client/server identification and the level of supported features. The information is encoded in standard DIAMETER Device-Reboot-Indication and Host-IP-Address AVP's.

Both client and policy servers must support DIAMETER SIP extension. In case a client going down, the server must download known client configuration to the client after reboot.

A client queries its policy server when a SIP policy event occurs. A policy event could be due to the arrival of a SIP INVITE, ACK, CANCEL or BYE message. SIP OPTION and REGISTER messages will not trigger policy events.

When the server receives a query, it will perform policy checking, admission control and accounting. If the server needs to inform the results of the policy checking to a client, it can send a reply message to the client.

A client, by default, has one primary and several alternative servers. In case of primary server failure, the client can try to open a new DIAMETER connection with one of its alternative servers. After the new connection is established, the client must notify the server of all its pending policy requests.

A policy server can asynchronously download policy decisions to a client. In turn, the policy decisions may trigger SIP messages to be generated at the client to re-direct or cease existing sessions.

Optionally, a client can cache all or a part of the policy decisions locally. In this case, a server must asynchronously download the decision information to the client. However, the server must be responsible for updating any decision change to the client.

3.2. Initialization Operation

At the boot-up time, servers and clients inform each other about the features that need to be supported. As a part of the feature discovery process, the DIAMETER Device-Reboot-Indication AVP must contain the feature number that has been assigned to the SIP/DIAMETER extension. For a client that has multiple servers, it must exchange feature information with all its servers at initialization time.

3.3. Caller Detailed Operation

When a caller (a SIP proxy server) is being notified to set up a call for a user, it first initiates a DIAMETER request command to its policy server with all the information about the user. The server, in turn, checks the request against the admission control policy database, and returns the findings in a DIAMETER response message. If the response is OK, the caller will sends a SIP INVITE message to the callee.

If the callee accepts the call, it replies a SIP 200 (SUCCESS) signal to the caller. Upon reception, the caller confirms the call by sending back a SIP ACK message. At the same time, the call must also send a notification to the server to start the accounting process. The notification is in DIAMETER request message format.

When a caller receives a call termination notification from the user, or a SIP BYE message from the callee, it informs the policy server to stop the accounting.

When a caller sends a SIP CANCEL message to cancel a pending request, it must also inform the policy server.

3.4. Callee Detailed Operation

After a callee receives an INVITE message, it initiates a SIP request command to the server for policy checking. If the server replies a

denial response, the callee will reject the session invitation by sending a SIP 4XX (Error) signal to the caller. The original INIVITE message MUST be dropped at the callee. If the server permits the invitation, the callee needs to relay the INIVITE message to the destination user, or (as a proxy) to directly reply a SIP 200 signal to the caller.

A SIP caller always sends a SIP ACK message to the callee to confirm the establishment of a session. When an ACK message being received, the callee MUST send a SIP request message to the policy server to start the accounting process.

When the callee decides to terminate a call or receives a BYE message, the callee MUST send a SIP request message to the server to stop the accounting process of the call.

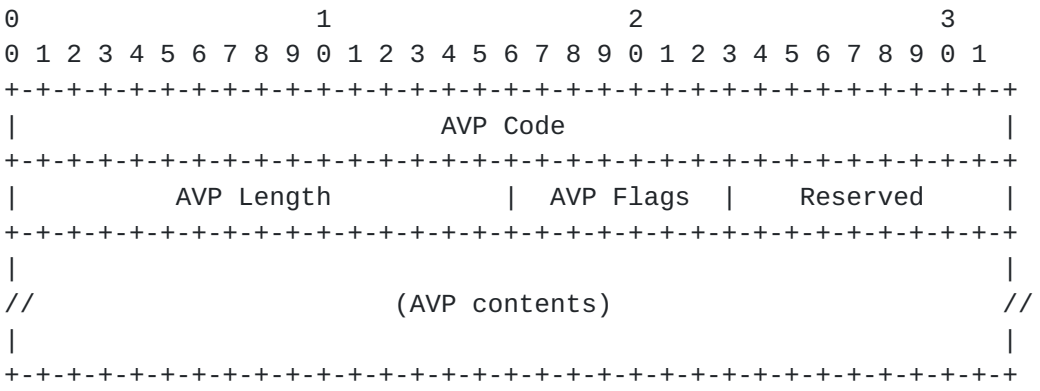
After the callee receives a SIP CANCEL, it needs to inform the policy server to remove the pending requests.

3.5. Server Considerations

DIAMETER/SIP policy servers may or may not support SIP protocol. As a result, clients have the option to either 1) send the entire SIP message to the servers, or 2) parse the SIP message first and send pre-defined SIP AVP's to the servers.

4. AVP Formats

Each DIAMETER message consists of multiple AVP's, that is 32-bit aligned, with the following format:



Code

Identifies the AVP; values of this field are defined below.

AVP Length

A 16-bit field contains the total object length in bytes. Must always be a multiple of 4, and at least 8.

AVP Flags

0x01:	Mandatory-Support
0x02:	SS-Encrypted-Data
0x03:	PK-Encrypted-Data
0x04:	Vendor-Specific-AVP

Readers can refer [RC98] for detailed DIAMETER base protocol information.

4.1. Device-Reboot-Indication AVP extension

Clients and servers send the Device-Reboot-Indication messages at initialization or reboot time. The message originator must include all supported extensions within the message. The responder must include all supported extensions as long as they were present within the request message.

The DIAMETER SIP extension uses Extension Id 6.

The Extension Id may also be used in Device-Feature-Request, Device-Feature-Response and Extension-Id AVP's.

4.2. DIAMETER-Command AVP extension

The Command AVP must be the first AVP following the DIAMETER header. There must only be one Command AVP per message. The command information is in the AVP's Command Code field. The message format can be found in [RC98].

This document defines the following DIAMETER Command Codes. All DIAMETER implementations supporting this extension MUST support all of the following:

Command Name	Command Code

SIP-Admission-Request	600
SIP-Admission-Response	601
SIP-Accounting-Request	602
SIP-Accounting-Response	603
SIP-Termination-Request	604
SIP-Termination-Response	605

4.3. DIAMETER Error-Code AVP extension

The Error-Code AVP contains the explicit message error code. Note: an Error-Code AVP must be coupled with the Result-Code AVP that consists of DIAMETER_SEE_ERROR_CODE information.

The extension defines the following additional error code for SIP operation:

0x6001:	Missing Call-ID in the request
0x6002:	Missing To in the request message
0x6003:	Missing From in the request message
0x6010:	Prohibited Caller
0x6011:	Prohibited Callee

4.4. SIP Specific AVP's

This section defines the extension specific AVP's.

The following are the mandatory AVP's which must be recognized by all DIAMETER implementations supporting this extension.

Attribute Name	AVP Code
SIP-Sequence	600
SIP-Call-ID	601
SIP-To	602
SIP-From	603

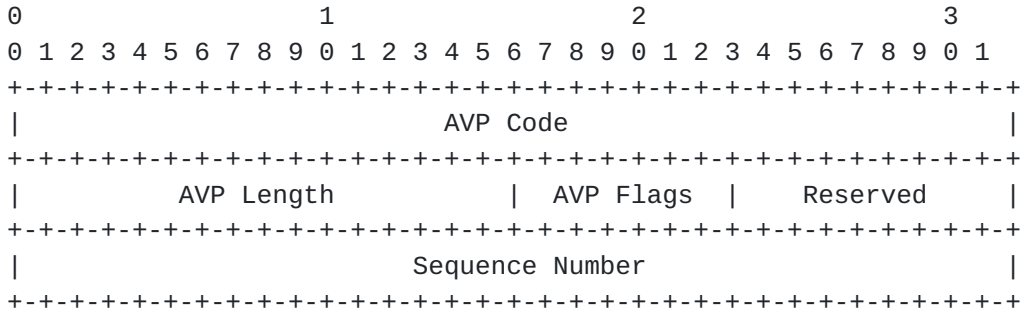
The following is an optional AVP.

Attribute Name	AVP Code
SIP-Entire-Msg	604

4.4.1. SIP-Sequence AVP

Each SIP-Request or SIP-Response MUST accompany with a sequence number. When a DIAMETER device receives a request, it checks the received sequence number against the sequence number in the last transmitted SIP-Request of the same SIP session. If they are not equal, the response is ignored.

The AVP may be replaced by a DIAMETER global sequence number AVP in the future.



Code

SIP-Sequence: 600

AVP Length:

The length of this attribute MUST be 12.

AVP Flags

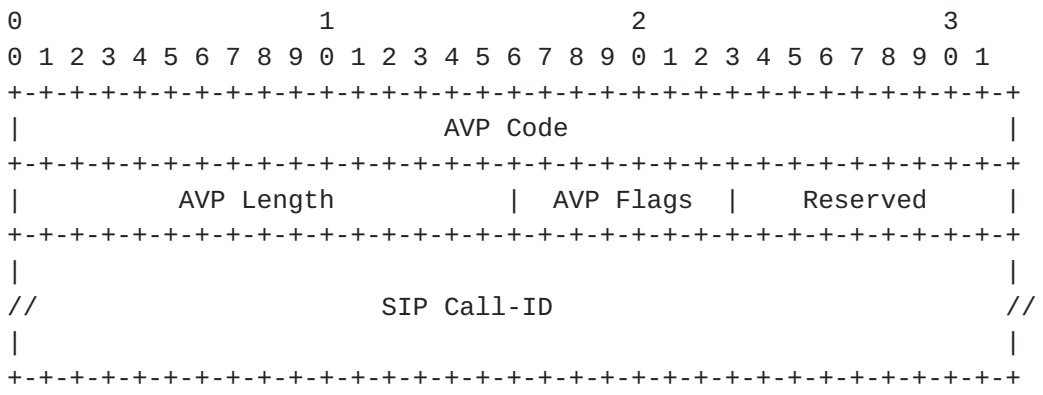
The AVP Flags field MUST have bit one (Mandatory Support) set.

Sequence Number:

A number between 0xff to 0xffffffff

4.4.2. SIP-Call-ID AVP

SIP uses Call-ID to identify a particular call session between two users. DIAMETER servers can use Call-ID's to keep track of all on-going calls for billing and accounting purposes. The SIP-Call-ID AVP has the following format:



Code

SIP-Call-ID: 601

AVP Length:

The length of this attribute depends on the size of SIP Call-ID.

AVP Flags

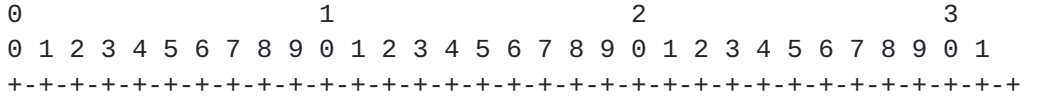
The AVP Flags field MUST have bit one (Mandatory Support) set.

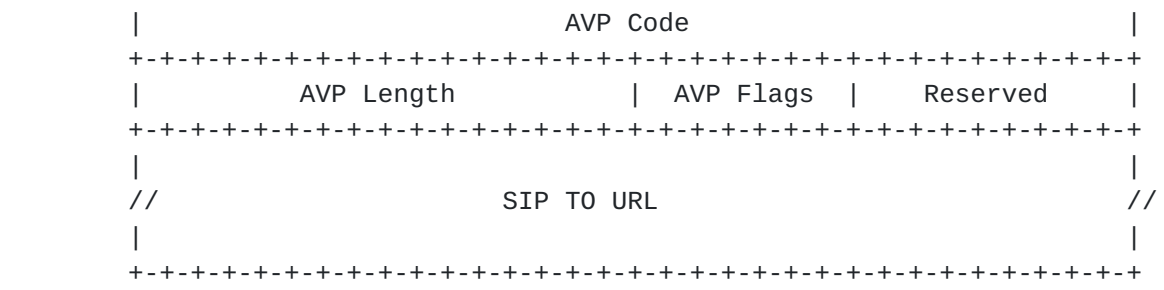
SIP Call-ID:

A copy of the original SIP Call-ID data

4.4.3. SIP-To AVP

This identifies the invited user of the session.





Code

SIP-TO-ID: 602

AVP Length:

The length of this attribute depends on the size of SIP TO URL.

AVP Flags

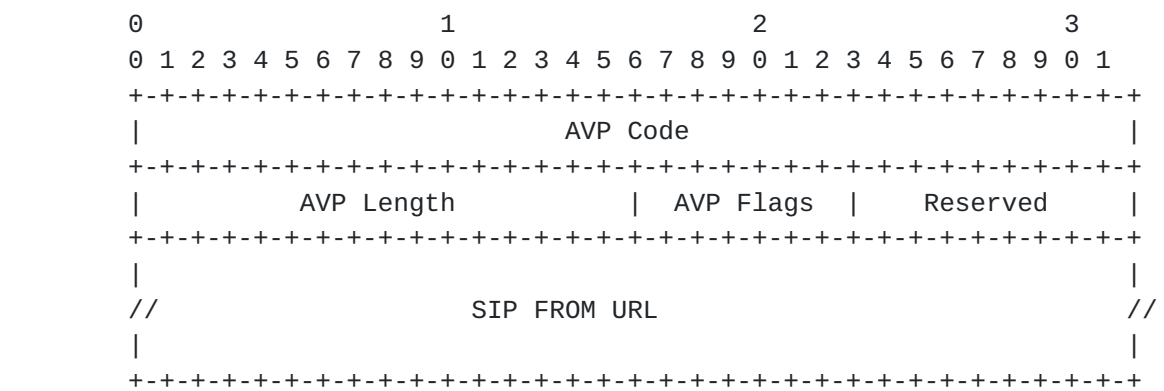
The AVP Flags field MUST have bit one (Mandatory Support) set.

SIP Call-ID:

A copy of the original SIP URL for the invited user

4.4.4. SIP-From AVP

This AVP identifies the invitation initiator ID in SIP URL format.



Code

SIP-FROM-ID: 603

AVP Length:

The length of this attribute depends on the size of SIP FROM URL.

AVP Flags

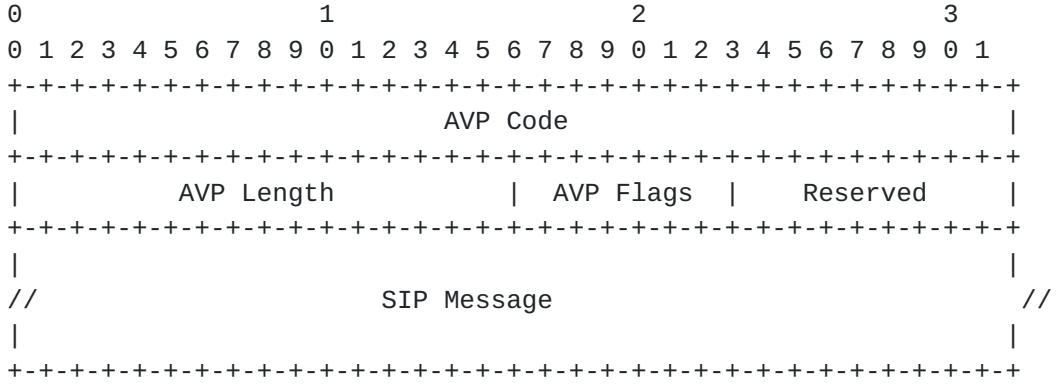
The AVP Flags field MUST have bit one (Mandatory Support) set.

SIP Call-ID:

A copy of the invitation initiator's SIP URL.

4.4.5. SIP-Entire-Msg AVP

The AVP encapsulates an entire SIP message. In order to ease the processing overhead at clients, and to provide adequate information, a SIP request message may send the entire SIP message to the server for parsing and processing.



Code

SIP-Entire-Msg: 604

AVP Length:

The length of this attribute depends on the size of SIP message.

AVP Flags

The AVP Flags field MUST not have bit one (Mandatory Support) set.

SIP Message:

A copy of the original SIP message.

5. Command Format

5.1. SIP Admission Control Commands

During SIP call setup time, a SIP caller sends an admission control request to the DIAMETER server before sending a SIP INVITE message. At callee's side, it sends an admission control request to the DIAMETER server after receiving a SIP INVITE message.

The format of the request message is the following:

```
<Admission Control Request> ::= <DIAMETER Header>
                                <Command AVP>
                                <Host-IP-Address>
                                <SIP-Sequence>
                                <SIP-Call-ID>
                                <SIP-To>
                                <SIP-From>
                                [<SIP-Entire-Msg>]
                                <Timestamp AVP>
                                <Initialization-Vector AVP>
                                {<Integrity-Check-Vector AVP> ||
                                 <Digital-Signature AVP> }
```

The Host-IP-Address AVP contains the client's IP address.

The server bases on the request to conduct admission control for the session, and reply a response back to the client in the following format:

```
<Admission Control Response> ::= <DIAMETER Header>
                                 <Command AVP>
                                 <Host-IP-Address>
```

```
                                <Result-Code>
                                [<Error-Code>]
                                <SIP-Sequence>
                                <SIP-Call-ID>
                                [<SIP-To>]
                                [<SIP-From>]
                                <Timestamp AVP>
                                <Initialization-Vector AVP>
                                {<Integrity-Check-Vector AVP> ||
                                 <Digital-Signature AVP> }
```

The Host-IP-Address AVP contains the server's identification. If the server does not admit the call session, it must reply an Error-Code AVP to identify the rejection reason. SIP client and server, by default, use SIP Call-ID to represent a call session. However an implementation may use SIP To and From to manage call sessions in their database, so the response may need to consist of SIP-To and SIP-From AVP's.

5.2. SIP Accounting Commands

After a SIP call session being established, the clients need to send an accounting request command to the servers to start up the accounting process. The message format is:

```
<Accounting Request> ::= <DIAMETER Header>
                         <Command AVP>
                         <Host-IP-Address>
                         <Timestamp>
                         <SIP-Sequence>
                         <SIP-Call-ID>
                         <SIP-To>
                         <SIP-From>
                         [<SIP-Entire-Msg>]
                         <Timestamp AVP>
                         <Initialization-Vector AVP>
                         {<Integrity-Check-Vector AVP> ||
                          <Digital-Signature AVP> }
```

The Timestamp AVP contains the timing information at client. Servers must base on this information to keep the duration of call sessions.

The servers must reply an accounting response back to the clients.

```
<Accounting Response> ::= <DIAMETER Header>
                          <Command AVP>
                          <Host-IP-Address>
                          <SIP-Sequence>
                          <Result-Code>
                          [<Error-Code>]
                          <SIP-Call-ID>
                          [<SIP-To>]
                          [<SIP-From>]
                          <Timestamp AVP>
                          <Initialization-Vector AVP>
                          {<Integrity-Check-Vector AVP> ||
                           <Digital-Signature AVP> }
```

If the server cannot process an accounting request, it must reply an Error-Code AVP to identify the error condition.

5.3. SIP Termination Commands

A SIP Termination request may come from either client-side or server-side. At a client, when it receives a hang-up signal from end users, or a SIP BYE message, or a SIP CANCEL message (for callee only), it must inform the server to stop the accounting process. Due to user policy, the server can send a termination request to the client to stop an on-going call. In turn, the client must send a SIP BYE to the other party to cease a call.

A termination request has the following format:

```
<Termination Request> ::= <DIAMETER Header>
                          <Command AVP>
                          <Host-IP-Address>
                          <SIP-Sequence>
                          <SIP-Call-ID>
                          <SIP-To>
                          <SIP-From>
                          <Timestamp AVP>
                          <Initialization-Vector AVP>
                          {<Integrity-Check-Vector AVP> ||
                           <Digital-Signature AVP> }
```

When a DIAMETER receives a termination request, it must reply:

```
<Termination Response> ::= <DIAMETER Header>
                           <Command AVP>
                           <Host-IP-Address>
                           <Result-Code>
                           [<Error-Code>]
                           <SIP-Sequence>
                           <SIP-Call-ID>
                           [<SIP-To>]
                           [<SIP-From>]
                           <Timestamp AVP>
                           <Initialization-Vector AVP>
                           {<Integrity-Check-Vector AVP> ||
                            <Digital-Signature AVP> }
```

6. Impact on Other Protocols

SIP is an out-band signaling protocol, and the actual voice data may use a different route than the path that SIP messages traverse. For IP telephony, voice data is transmitted in the form of RTP[SCFJ96]. To ensure voice data being delivered properly, users can make the use of end-to-end resource reservation protocols[BZB+97] to set up reserved "flows". Another alternative is to mark the packet header as one of traffic classes in Assured Forwarding[HBWW98] or Expedited Forwarding [JNP98] so that the data packets can be delivered with low delay and rate guarantees inside the network. Both approaches imply that the network-edge routers may need to interface with policy servers to manage link resources. However, the detailed mapping and management between IP telephone sessions and link resource management requires further investigation, and is beyond the scope of this document at this point.

During a SIP session, the call can be dropped due to either link failure or users hanging up the phone without sending SIP BYE messages. In both cases, the exact call duration becomes difficult to track. If the call goes through PSTN gateways, it's necessary for the gateways to inform the policy servers about "connection lost" and thus stop the billing clock. If the call is a full Internet call, it's up to the network resource management agents (such as RSVP policy servers, or Bandwidth Brokers) to notify the policy

servers to terminate the call's accounting process. However, the detailed operation needs further evaluation, and thus excluded from the current draft.

7. Security Considerations

The security of SIP/DIAMETER messages is provided by the DIAMETER User Authentication Extensions[BC98].

References

[BC98] W. Bulley and P. Calhoun. DIAMETER user authentication extensions. Internet Draft, Internet Engineering Task Force, July 1998. Work in progress.

[BZB+97] B. Braden, L. Zhang, S. Berson, S. Herzog, and S. Jamin. Resource ReSerVation protocol (RSVP) -- version 1 functional specification. RFC 2205, Internet Engineering Task Force, October 1997.

[HBWW98] J. Heinanen, F. Baker, Weiss W., and J. Wroclawski. Assured forwarding phb group. Internet Draft, Internet Engineering Task Force, October 1998. Work in progress.

[HSSJ98] M. Handley, H. Schulzrinne, E. Schooler, and Rosenberg J. SIP: session initiation protocol. Internet Draft, Internet Engineering Task Force, November 1998. Work in progress.

[JNP98] V. Jacobson, K. Nichols, and K. Poduri. An expedited forwarding phb. Internet Draft, Internet Engineering Task Force, August 1998. Work in progress.

[RC98] A. Rubens and P. Calhoun. DIAMETER base protocol. Internet Draft, Internet Engineering Task Force, October 1998. Work in progress.

[RRSW97] C. Rigney, A. Rubens, W. Simpson, and S. Willens. Remote authentication dial in user service (RADIUS). RFC 2138, Internet Engineering Task Force, April 1997.

[SCFJ96] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson. RTP: a transport protocol for real-time applications. RFC 1889, Internet Engineering Task Force, January 1996.

[ZPC98] G. Zorn, P. Pan, and P. Calhoun. DIAMETER framework document. Internet Draft, Internet Engineering Task Force, May 1998. Work in progress.

Authors' Address

Ping Pan
Bell Laboratories
Lucent Technologies
101 Crawfords Corner Road
Holmdel, NJ 07733
USA
Phone: (732)-332-6744
Email: pingpan@dnrc.bell-labs.com

Henning Schulzrinne
Dept. of Computer Science
Columbia University
1214 Amsterdam Avenue
New York, NY 10027
USA
Phone: 1-212-939-7042
Email: schulzrinne@cs.columbia.edu

Pat Calhoun
Technology Development
Sun Microsystems, Inc.
15 Network Circle
Menlo Park, California, 94025
USA
Phone: 1-650-786-7733
Email: pcalhoun@eng.sun.com