

RADIUS accounting for SIP servers

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/1id-abstracts.txt>

To view the list Internet-Draft Shadow Directories, see <http://www.ietf.org/shadow.html>.

Copyright Notice

Copyright (c) The Internet Society (2002). All Rights Reserved.

Abstract

This memo defines mappings of RADIUS accounting attributes for use with SIP servers. It also defines several new attributes to support the provision of RADIUS accounting for SIP servers.

1 Introduction

The Session Initiation Protocol (SIP) [1] is an application-layer control protocol that can establish, modify and terminate multimedia sessions or calls. A SIP system is composed of a number of logical components such as user agents, proxy servers, redirect servers and registrars.

RADIUS (Remote Authentication in Dial-In User Service) [2] can be used for carrying accounting information between a SIP server and a RADIUS server. In this architecture, the SIP server operates as a client of the RADIUS server. The client passes user accounting information derived from specific events in a SIP session to a designated RADIUS server in an accounting request packet. The RADIUS server sends back an accounting response to the client indicating that it has successfully received and processed the request. RADIUS servers discard the request packet if it had an error.

SIP servers can log calls, transactions or requests and responses. If it logs calls, it marks the beginning and end of calls with **Acct-Status-Type start** and **stop**, respectively. If it logs transactions, it includes both the request method and the final response for the transaction and logs them with **Acct-Status-Type Interim-Update**. If the server logs requests or responses, it generates two or more accounting requests, one for the request and one or more final responses. (TBD: Is there a point of logging all final responses in a forking proxy?)

For forking proxies, the server can log either only the single successful branch or log responses from all branches.

Some of the parameters to be logged can be mapped into the attributes defined in RFC 2865[2] and RFC 2866[3]. However, some new SIP specific attributes need to be defined for some SIP-specific accounting

and logging information. This document defines a set of attributes and also provides a mapping for several existing RADIUS attributes.

2 Conventions of This Document

In this document, the key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” are to be interpreted as described in RFC 2119 [4] and indicate requirement levels for compliant implementations.

3 Terminology

RADIUS server: Defined in RFC 2865 [2]. In the context of this document, the term RADIUS server refers to a server that accepts RADIUS accounting packets, and responds to them.

Accounting Request: Defined in RFC 2865 [2]; an accounting request is a specific RADIUS attribute, denoted `Accounting-Request`, used in a packet sent from a client to the RADIUS server. It requests the server to log the contents of the packet. The contents will be interpreted according to the definitions of attributes and types provided in RFC 2866 [3].

Accounting Response: Defined in RFC 2865 [2], an accounting response is a specific RADIUS attribute, denoted `Accounting-Response`, used in responses for accounting requests.

4 Table of Attributes

The following table provides a guide to which attributes may be found in `Accounting-Request` packets for SIP. The first part namely, Standard RADIUS attributes, specifies the RADIUS attributes that can be used in SIP servers. The SIP specific attribute section defines new attributes that are specific to SIP. No SIP specific attributes should be found in `Accounting-Response` packets. A value of 1 in the first column indicates that exactly one instance of the corresponding attribute **MUST** be present in a `Accounting-Request` packet; a value of 0-1 indicates that zero or one instance of the attribute **MAY** be present.

Standard RADIUS attributes:

Request	#	Attribute
1	1	User-Name
1	4	NAS-IP-Address
1	5	NAS-Port
1	6	Service-Type
1	30	Called-Station-ID
1	31	Calling-Station-ID
1	40	Acct-Status-Type
1	44	Acct-Session-Id
0-1	45	Acct-Authentic
0-1	46	Acct-Session-Time
0-1	49	Acct-Terminate-Cause
1	55	Event-Timestamp

SIP-specific attributes:

Request	#	Attribute
0-1	101	Sip-Method [*]
0-1	102	Sip-Response-Code [*]
1	103	Sip-Cseq
0-1	104	Sip-To-Tag
0-1	105	Sip-From-Tag
0-1	106	Sip-Branch-ID
0-1	107	Sip-Translated-Request-ID
0-1	108	Sip-Source-IP-Address
0-1	109	Sip-Source-Port

*: Either the Sip-Method Attribute or the Sip-Response-Code attribute must be present in all Accounting-Request packets.

5 Description of Attributes

Below, we describe the semantics of each RADIUS attribute when used for SIP servers. If no format is shown, it is the same as defined in RFC 2865 [2] or RFC 2866 [3].

5.1 User-Name

The User-Name attribute refers to the SIP address of the user responsible for the session. If the request used Digest authentication, this is the “user” parameter in the Authorization header field. Other authentication schemes provide similar mappings. If there was no authentication, the From header field is used instead. This attribute **MUST** be present in all Accounting-Request packets.

5.2 NAS-IP-Address

The NAS-IP-Address attribute indicates the IP Address of the SIP server which is requesting the accounting service provided by the RADIUS server. This attribute **MUST** be present in Accounting-Request packets.

5.3 NAS-Port

The NAS-Port attribute indicates the port number of the SIP Server that provides service to the user. This is usually 5060. This attribute **MUST** be present in Accounting-Request packets.

5.4 Service-Type

The Service-Type attribute indicates the type of service the user has requested, or the type of service to be provided. For SIP accounting the value **MUST** be 15 indicating Sip-Session. It **MUST** be present in Accounting-Request packets.

5.5 Calling-Station-Id

When used for SIP accounting, the RADIUS Calling-Station-Id attribute is the URL in the SIP From header field and identifies a SIP caller of any request or response through a SIP server. It **MUST** be present in Accounting-Request packets.

5.6 Called-Station-Id

When used for SIP accounting, the RADIUS Called-Station-Id attribute is the URL from the SIP To header field and identifies a SIP callee of any request or response through a SIP server. It **MUST** be present in Accounting-Request packets.

5.7 Acct-Status-Type

The Acct-Status-Type attribute indicates whether this Accounting-Request marks the beginning of the user service (Start) or the end (Stop). This attribute is also used by the SIP server to mark the start of accounting (for example, upon booting) by specifying Accounting-On and to mark the end of accounting (for example, just before a scheduled reboot) by specifying Accounting-Off.

For SIP accounting, the value field can contain one of the following RADIUS codes:

- 1 Start
- 2 Stop
- 3 Interim-Update
- 7 Accounting-On
- 8 Accounting-Off
- 15 Reserved for failures

5.8 Acct-Session-Id

The Acct-Session-Id attribute is derived from the Call-ID of the SIP session. The Call-ID is a SIP header field uniquely identifies a particular invitation or all registrations of a particular client. This attribute also makes it easy to correlate start and stop records in the RADIUS server log. The start and stop records for a given accounting session **MUST** have the same Acct-Session-Id. This attribute **MUST** be present in Accounting-Request packets.

5.9 Acct-Authentic

The Acct-Authentic attribute **MAY** be included in an Accounting-Request and indicates how the user was authenticated, whether by RADIUS, the SIP server itself (Local), or another remote authentication protocol (Remote). (TBD)

- 1 RADIUS
- 2 Local
- 3 Remote

5.10 Acct-Session-Time

The Acct-Session-Time attribute indicates how many seconds the user has received service for, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop. It is used

to represent the time between the arrival of the 200 (OK) response to an INVITE request from the caller and the arrival of the corresponding BYE request by either party. This attribute can only be generated by call-stateful SIP entities. These entities must receive both INVITE and BYE requests for each dialog, for example, proxies using record-routing or user agent servers.

A summary of the Acct-Session-Time attribute 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
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|      Type (=46) |      Length (=6) |                               Value
+-----+-----+-----+-----+-----+-----+-----+-----+
|                               Value (cont) |
+-----+-----+-----+-----+-----+-----+

```

Value: The Value field is four octets.

5.11 Acct-Terminate-Cause

The Acct-Terminate-Cause attribute indicates how the session was terminated, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop. This attribute can only be generated by call-stateful SIP entities.

A summary of the Acct-Terminate-Cause attribute 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
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|      Type (=49) |      Length (=6) |                               Value
+-----+-----+-----+-----+-----+-----+-----+-----+
|                               Value (cont) |
+-----+-----+-----+-----+-----+-----+

```

Value: The Value field is four octets, containing an integer specifying the cause of session termination, as follows:

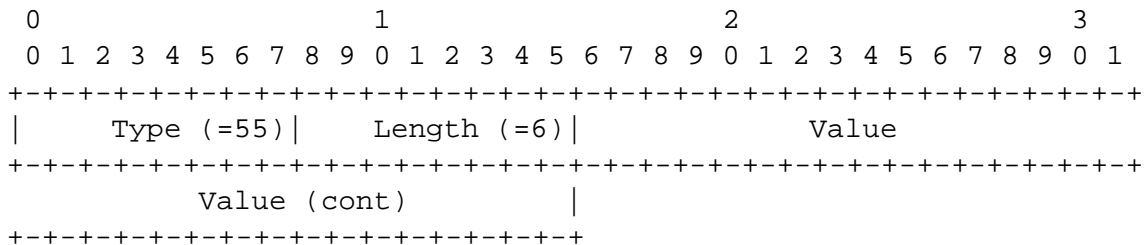
- 1 User Request (BYE)
- 3 Lost Service
- 4 Idle Timeout (e.g., loss of RTP or RTCP)
- 5 Session Timeout (e.g., SIP session timer)
- 6 Admin Reset
- 7 Admin Reboot
- 8 Port Error
- 9 NAS Error
- 10 NAS Request
- 11 NAS Reboot
- 15 Service Unavailable

RFC 2866 [3] provides further explanation.

5.12 Event-Timestamp

The Event-Timestamp attribute is included in an Accounting-Request packet to record the time that this event occurred on the SIP server, in seconds since January 1, 1970 00:00 UTC. This attribute MAY be present. It is useful for profiling and traffic measurement purposes.

A summary of the Event-Timestamp attribute format is shown below. The fields are transmitted from left to right.



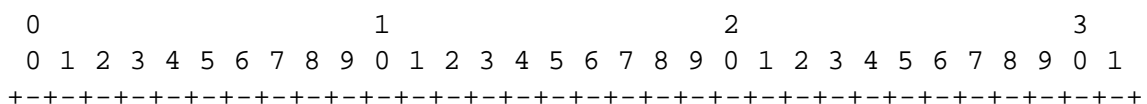
Value: The Value field is four octets encoding an unsigned integer with the number of seconds since January 1, 1970 00:00 UTC.

5.13 Sip-Method

The Sip-Method attribute indicates the SIP method. It can take values corresponding to INVITE, ACK, OPTIONS, CANCEL, BYE, REGISTER, SUBSCRIBE and NOTIFY. Other methods will be added in the future by IANA registration. A SIP entity MAY log any subset of these requests.

This attribute MUST be present in Accounting-Request packets if there is no SIP-Response-Code attribute in the packet. Both SIP-Reponse-Code and SIP-Method can appear in the same RADIUS packet.

A summary of the Sip-Method attribute format is shown below. The fields are transmitted from left to right.



```

|   Type (=101) |   Length (=6) |   Value
+-----+-----+-----+-----+-----+-----+
|   Value (cont) |
+-----+-----+-----+-----+-----+-----+

```

Value: The Value field is four octets, containing an integer specifying the Method, as follows:

- 0 INVITE
- 1 BYE
- 2 REGISTER
- 3 CANCEL
- 4 OPTIONS
- 5 ACK
- 6 SUBSCRIBE
- 7 NOTIFY

5.14 Sip-Response-Code

The **Sip-Response-Code** attribute indicates the SIP status code present in the SIP response to the SIP server. For example, a successful call setup may result in 200.

This attribute **MUST** be present in **Accounting-request** packets if there is no **Sip-Method** attribute in the packet. A packet **MAY** contain both header **Sip-Method** and **Sip-Response-Code**.

A summary of the **Sip-Response-Code** attribute format is shown below. The fields are transmitted from left to right.

```

0                               1                               2
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
+-----+-----+-----+-----+-----+-----+
|   Type(=102) |   Length (6) |   value ...
+-----+-----+-----+-----+-----+-----+

```

Value: The value field is 4 octets and contains the SIP response code.

5.15 Sip-CSeq

The **Sip-CSeq** attribute is the numeric part of **CSeq** header field value. It **MUST** be present in **Accounting-Request** packets.

A summary of the **Sip-CSeq** attribute format is shown below. The fields are transmitted from left to right.

```

0                               1                               2
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
+-----+-----+-----+-----+-----+-----+
|   Type(=103) |   Length (>=3) |   Text ...
+-----+-----+-----+-----+-----+-----+

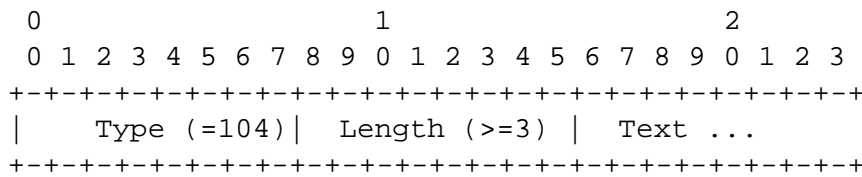
```

Text: The text field is the numeric part of the CSeq header field. (TBD: should this be an integer?)

5.16 Sip-To-Tag

The Sip-To-Tag attribute is the tag value from the SIP To header field and identifies a SIP callee of any request or response through a SIP server. It MUST be present in Accounting-Request packets if the request contained a tag.

A summary of the Sip-To-Tag attribute format is shown below. The fields are transmitted from left to right.

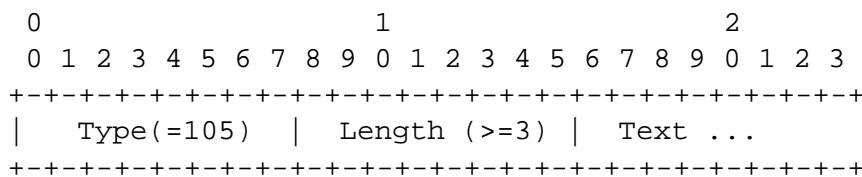


Text: The tag field.

5.17 Sip-From-Tag

The Sip-From attribute is the tag value from the SIP From header field and identifies a SIP caller of any request or response through a SIP server. It MUST be present in Accounting-Request packets if the request contained such a tag.

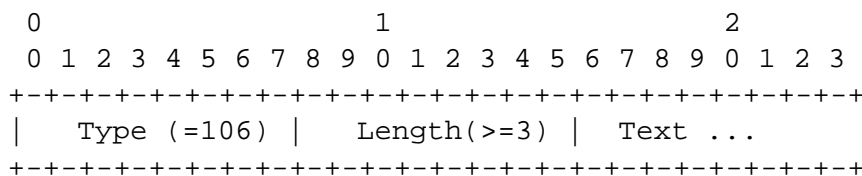
A summary of the Sip-From-Tag attribute format is shown below. The fields are transmitted from left to right.



Text: The text field is a SIP URI.

5.18 Sip-Branch-ID

The Sip-Branch-ID attribute indicates the branch ID for a particular request or response.



Text: The value of the branch ID.

5.19 Sip-Translated-Request-URI

The Sip-Translated-Request-URI attribute indicates the Request-URI of the SIP request, translated as per the SIP server's processing rules into a "canonical" URI. For an INVITE request, the "canonical" URI is the URI that the SIP server uses for proxying. For example, if the Request-URI is "sip:alice@wonderland.com", a SIP server might translate this to "sip:alice@p42.wonderland.com". The latter is then recorded as the translated request URI.

In other cases, such as a REGISTER request, the Sip-Translated-Request-URI MAY be same as the Request-URI. For example, if the Request-URI for the registrar serving wonderland.com is "sip:wonderland.com", the Sip-Translated-Request-URI will be just "sip:wonderland.com". However, other Request-URIs such as "sip:registrar.wonderland.com" may be translated to "sip:wonderland.com".

This attribute MUST be present in all Accounting-Request packets.

A summary of the Sip-Translated-Request-URI attribute format is shown below. The fields are transmitted from left to right.

```

      0                               1                               2
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
+-----+-----+-----+-----+-----+-----+-----+-----+
|   Type (=107) |   Length(>=3) |   Text ...
+-----+-----+-----+-----+-----+-----+-----+-----+

```

String: The string is a URI.

5.20 Sip-Source-IP-Address

The Sip-Source-IP-Address attribute indicates the IP source address of the request that triggered the accounting request. (TBD: do we need to log the source IP address of responses, too?)

A summary of the Sip-Remote-IP-Address attribute 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
+-----+-----+-----+-----+-----+-----+-----+-----+
|   Type (=108) |   Length (=6) |                               Address
+-----+-----+-----+-----+-----+-----+-----+-----+
|                               Address (cont) |
+-----+-----+-----+-----+-----+-----+-----+

```

Address: The address field is four octets and contains an IPv4 address.

5.21 Sip-Source-Port

The Sip-Source-Port attribute indicates the port number of the request that triggered the accounting request.

A summary of the Sip-Source-Port attribute 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
+-----+-----+-----+-----+-----+-----+-----+-----+
|   Type (=109) |   Length (=6) |                               Value
+-----+-----+-----+-----+-----+-----+-----+-----+
|                               Value (cont) |
+-----+-----+-----+-----+-----+-----+

```

Value: The Value field is four octets and represents a TCP or UDP port.

6 Reliability of Accounting Messages

Radius servers discard packets in case of an error, such as malformed or tampered packets. If the packet is accepted as valid, they send back an accounting response. As noted in Section 3.1 of RFC 2975 [5], “RADIUS accounting implementations are vulnerable to packet loss as well as application layer failures, network failures and device reboots.”

- It is RECOMMENDED that the client continue attempting to send the Accounting-Request packet until it receives an acknowledgement, using the SIP backoff timers for congestion control.
- The client MAY forward requests to an alternate server in the event that the primary server unreachable.
- The client SHOULD store records that cannot be delivered after the backoff timer has run its course, so that they can be delivered when the network is available again.
- It is a matter of client policy how to process requests where storage for undelivered accounting records has been exhausted.

RFC 2975 [5] contains additional advice.

7 Security Considerations

If a SIP proxy server is used for call accounting, the proxy uses the SIP Record-Route option during call setup to ensure that all subsequent signaling messages traverse through it. This is needed, for example, to know when the call ends. Security policies should make sure that the proxy server is not bypassed. For example, a gateway should be configured to reject all BYE requests that do not originate from the proxy server. Additional security issues considered in RFC 2865 [2] and RFC 2543 [1] are also applicable.

8 IANA Considerations

The packet type codes, attribute types, and attribute values defined in this document are registered by the Internet Assigned Numbers Authority (IANA) from the RADIUS name spaces.

9 Acknowledgments

Rick W. Porter provided useful input.

10 Authors' Addresses

Henning Schulzrinne
Dept. of Computer Science
Columbia University
1214 Amsterdam Avenue, MC 0401
New York, NY 10027
USA
electronic mail: schulzrinne@cs.columbia.edu

Anshul Kundaje
Dept. of Electrical Engineering
Columbia University
1214 Amsterdam Avenue, MC 0401
New York, NY 10027
USA
electronic mail: abk2001@cs.columbia.edu

Sankaran Narayanan
Dept. of Computer Science
Columbia University
1214 Amsterdam Avenue, MC 0401
New York, NY 10027
USA
electronic mail: sankaran@cs.columbia.edu

References

- [1] M. Handley, H. Schulzrinne, E. Schooler, and J. Rosenberg, "SIP: session initiation protocol," Request for Comments 2543, Internet Engineering Task Force, Mar. 1999.
- [2] C. Rigney, S. Willens, A. Rubens, and W. Simpson, "Remote authentication dial in user service (RADIUS)," Request for Comments 2865, Internet Engineering Task Force, June 2000.
- [3] C. Rigney, "RADIUS accounting," Request for Comments 2866, Internet Engineering Task Force, June 2000.
- [4] S. Bradner, "Key words for use in RFCs to indicate requirement levels," Request for Comments 2119, Internet Engineering Task Force, Mar. 1997.
- [5] B. Aboba, J. Arkko, and D. Harrington, "Introduction to accounting management," Request for Comments 2975, Internet Engineering Task Force, Oct. 2000.

Contents

1 Introduction

1

2	Conventions of This Document	2
3	Terminology	2
4	Table of Attributes	2
5	Description of Attributes	3
5.1	User-Name	3
5.2	NAS-IP-Address	3
5.3	NAS-Port	3
5.4	Service-Type	3
5.5	Calling-Station-Id	4
5.6	Called-Station-Id	4
5.7	Acct-Status-Type	4
5.8	Acct-Session-Id	4
5.9	Acct-Authentic	4
5.10	Acct-Session-Time	4
5.11	Acct-Terminate-Cause	5
5.12	Event-Timestamp	6
5.13	Sip-Method	6
5.14	Sip-Response-Code	7
5.15	Sip-CSeq	7
5.16	Sip-To-Tag	8
5.17	Sip-From-Tag	8
5.18	Sip-Branch-ID	8
5.19	Sip-Translated-Request-URI	9
5.20	Sip-Source-IP-Address	9
5.21	Sip-Source-Port	9
6	Reliability of Accounting Messages	10
7	Security Considerations	10
8	IANA Considerations	10
9	Acknowledgments	10
10	Authors' Addresses	11

Full Copyright Statement

Copyright (c) The Internet Society (2002). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or

other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.