

INTERNET DRAFT
Category: Standards Track
Title: [draft-calhoun-diameter-eap-03.txt](#)
Date: August 1999

Pat R. Calhoun
Sun Microsystems, Inc.
Allan Rubens
Ascend Networks Inc.
Jeff Haag
Cisco Systems

DIAMETER
Extensible Authentication Protocol (EAP) Extensions

Status of this Memo

This document is an individual contribution for consideration by the AAA Working Group of the Internet Engineering Task Force. Comments should be submitted to the diameter@ipass.com mailing list.

Distribution of this memo is unlimited.

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>

The list of Internet-Draft Shadow Directories can be accessed at:

<http://www.ietf.org/shadow.html>.

Abstract

The Extensible Authentication Protocol (EAP) is a PPP extension that provides support for additional authentication methods within PPP. This document describes how EAP can be carried within the DIAMETER protocol to provide end to end authentication.

INTERNET DRAFT

August 1999

Table of Contents

- 1.0 Introduction
 - 1.1 Copyright Statement
 - 1.2 Requirements language
 - 1.3 Changes in version -02
- 2.0 Command Codes
 - 2.1 DIAMETER-EAP-Request
 - 2.2 DIAMETER-EAP-Answer
 - 2.3 DIAMETER-EAP-Ind
- 3.0 DIAMETER AVPs
 - 3.1 EAP-Packet
- 4.0 Protocol overview
 - 4.1 Retransmission and Timers
 - 4.2 Example of an OTP Authentication
 - 4.2.1 Successful Authentication
 - 4.2.2 NAS Initiated EAP Authentication
 - 4.2.3 Server-Initiated Authentication
 - 4.2.4 Example of failed EAP Authentication
 - 4.2.5 Example of DIAMETER not supporting EAP
 - 4.2.6 Example of DIAMETER Proxy not supporting EAP
 - 4.2.7 Example of PPP Client not supporting EAP
 - 4.3 Feature Advertisement/Discovery
- 5.0 Alternative uses
- 6.0 IANA Considerations
- 7.0 Acknowledgments
- 8.0 References
- 9.0 Authors' Addresses
- 10.0 Full Copyright Statement

[1.0](#) Introduction

The Extensible Authentication Protocol (EAP), described in [1], provides a standard mechanism for support of additional authentication methods within PPP. Through the use of EAP, support for a number of authentication schemes may be added, including token cards, Kerberos, Public Key, One Time Passwords, and others. In order to provide for support of EAP within DIAMETER, two new attributes, EAP-Message and Signature, were introduced as DIAMETER extensions in [5]. This document describes how these new attributes may be used for providing EAP support within DIAMETER.

The scheme described here is similar to that proposed in [2], in that the DIAMETER server is used to shuttle DIAMETER-encapsulated EAP Packets between the NAS and a backend security server. While the conversation between the DIAMETER server and the backend security server will typically occur using a proprietary protocol developed by

the backend security server vendor, it is also possible to use DIAMETER-encapsulated EAP via the EAP-Packet AVP. This has the advantage of allowing the DIAMETER server to support EAP without the need for authentication-specific code, which can instead reside on a backend security server.

This proposal serves three purposes:

1. It provides for end-to-end authentication, between the user and his/her home DIAMETER server. End-to-End authentication, as described in this specification, greatly reduces the possibility for fraudulent authentication, such as replay attacks.
2. It allows for mutual (bi-directional) authentication. When PPP or CHAP are used as the PPP authentication mechanism, it is not possible to perform bi-directional authentication since the authenticator (e.g. the NAS) does not have access to the DIAMETER Server's authentication information. Although it would be possible for the DIAMETER server to "download" the authentication information to the NAS, even encrypted, it would be quite unwise to do so in roaming environments where the NAS and the authenticating DIAMETER server are not owned by the same Administrative Domain.
3. It allows for home DIAMETER server initiated authentication. Since the Home DIAMETER server may initially authenticate and authorize the user for a finite period, it may periodically send an authentication request to the user to ensure that the user is still active. Furthermore, this will allow the Home DIAMETER server to re-authorize the user for access for a finite amount of time. See [8] for more information.

The Extension number for this draft is three (3). This value is used in the Extension-Id Attribute value Pair (AVP) as defined in [7].

[1.1](#) Copyright Statement

Copyright (C) The Internet Society 1999. All Rights Reserved.

[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].

Calhoun, Rubens, Haag expires January 2000

[Page 3]

INTERNET DRAFT

August 1999

[1.3](#) Changes in version -03

The following changes were made in this revision of the document:

- The document introduces the DIAMETER-EAP-Ind to allow the server to initiate an unsolicited authentication session with the PPP client as described in [8].
- The AVP Header formats have changed since the last version of this draft.
- IANA considerations were added, as well as many new useful references.
- Well, to be honest, the list of changes are just too great list. This document needed a good re-write. Here it is.

[2.0](#) Command Codes

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

Command Name	Command Code
-----	-----
DIAMETER-EAP-Request	???
DIAMETER-EAP-Answer	???
DIAMETER-EAP-Ind	???

[2.1](#) DIAMETER-EAP-Request

Description

The DIAMETER-EAP-Request command is sent by a DIAMETER Client to a DIAMETER Server and conveys an EAP-Response [[1](#)] from the dial-up PPP Client. The DIAMETER-EAP-Request MUST contain one EAP-Packet AVP, which contains the actual EAP payload. A EAP-Packet AVP with no data MAY be sent to the DIAMETER Server to initiate an EAP authentication session.

Upon receipt of a DIAMETER-EAP-Request, A DIAMETER Server MUST issue a reply. The reply may be either:

- 1) a DIAMETER-EAP-Answer containing an EAP-Request in at least one EAP-Packet attribute
- 2) a DIAMETER-EAP-Answer containing an EAP-Packet of type

Calhoun, Rubens, Haag

expires January 2000

[Page 4]

INTERNET DRAFT

August 1999

"success" and a Result Code AVP indicating success

3) a DIAMETER-EAP-Answer containing an EAP-Packet of type "failure" and a Result-Code AVP indicating failure.

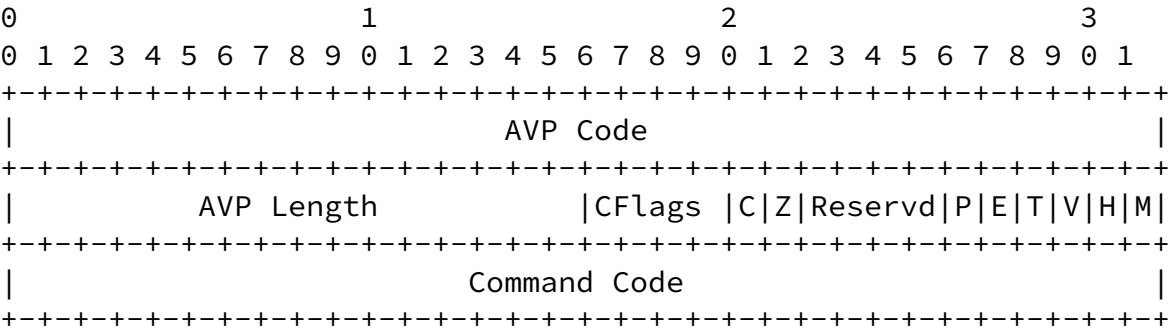
4) A Message-Reject-Ind packet is returned if the server does not support the EAP extensions.

Message Format

```
<DIAMETER-EAP-Request> ::= <DIAMETER Header>
                             <DIAMETER-EAP-Request Command AVP>
                             <Host-IP-Address AVP>
                             [<Host-Name AVP>]
                             <EAP-Packet AVP>
                             <User-Name AVP>
                             <Timestamp AVP>
                             <Initialization-Vector AVP>
                             {<Integrity-Check-Vector AVP> ||
                              <Digital-Signature AVP> }
```

AVP Format

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



AVP Code

256 DIAMETER Command

AVP Length

The length of this attribute MUST be 12.

Command Flags

The following Command-specific flag bits may be set in the DIAMETER-EAP-Request command:

The 'C' (Authentication-only) bit may be set to indicate that only authentication of the user is required, and that no authorization should be performed. Additionally, no authorization AVPs are expected in the DIAMETER-EAP-Answer command.

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-

Request).

[2.2](#) DIAMETER-EAP-Answer

Description

The DIAMETER-EAP-Answer packets are sent by the DIAMETER Server to the client in response to a DIAMETER-EAP-Request, and they contain the next EAP-Request packet to be transmitted to the PPP client. The DIAMETER-EAP-Answer message MUST include an EAP payload of type EAP-Request [[1](#)] encapsulated within an EAP-Packet AVP.

If the Result-Code AVP is present in the message, it indicates that the authentication is complete. Otherwise, after transmitting the contents of the EAP-Packet AVP to the PPP client, the NAS remains in a state where it awaits an EAP-Response [[1](#)] from the PPP client. When the Result-Code AVP indicates success, it MUST have an accompanying EAP-Success [[1](#)] message encapsulated within the EAP-Packet AVP. If the Result-Code AVP indicates failure, an accompanying EAP-Failure [[1](#)] message SHOULD be present in the EAP-Packet AVP.

A DIAMETER-EAP-Answer with a successful Result-Code AVP and the 'C' bit NOT set MUST include the normal authorization AVPs that one would find in an AA-Answer, as defined in [[2](#)].

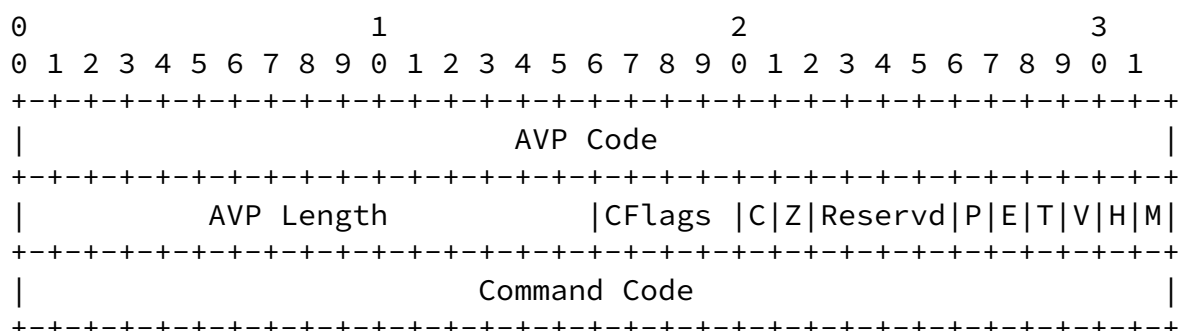
Message Format

```
<DIAMETER-EAP-Answer> ::= <DIAMETER Header>
                             <DIAMETER-EAP-Answer Command AVP>
                             <Result-Code AVP>
                             <Host-IP-Address AVP>
```

```
[<Host-Name AVP>]
<EAP-Packet AVP>
<User-Name AVP>
<misc. AVPs [2]>
<Timestamp AVP>
<Initialization-Vector AVP>
{<Integrity-Check-Vector AVP> ||
 <Digital-Signature AVP> }
```

AVP Format

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



AVP Code

256 DIAMETER Command

AVP Length

The length of this attribute MUST be 12.

Command Flags

The Command Specific flags MUST be set to the same value that was found in the DIAMETER-EAP-Request. The following values are supported:

The 'C' (Authentication-only) bit may be set to indicate that only authentication of the user is required, and that no authorization should be performed. Additionally, no authorization AVPs are expected in the DIAMETER-EAP-Answer command.

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).

[2.3](#) DIAMETER-EAP-Ind

Description

The DIAMETER-EAP-Ind command is sent as an unsolicited message from the DIAMETER Server to a client, and is used to request a re-authentication of the PPP client. The message MUST contain an EAP-Packet AVP, which MAY contain either an identity request, or a challenge request. It is recommended that the Identity Request be bypassed since the user's identity is already known, and by issuing the challenge directly, the number of round trips required for re-authentication is greatly diminished.

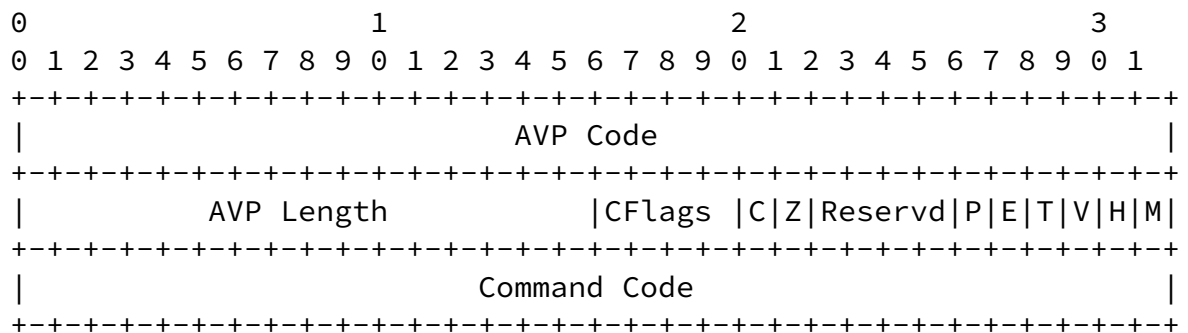
Upon receipt of the message, the NAS MUST issue the EAP payload to the PPP Client, and SHOULD respond with a DIAMETER-EAP-Request containing the EAP-Response [[1](#)] packet.

Message Format

```
<DIAMETER-EAP-Ind> ::= <DIAMETER Header>
                        <DIAMETER-EAP-Ind Command AVP>
                        <Host-IP-Address AVP>
                        [<Host-Name AVP>]
                        <EAP-Packet AVP>
                        <User-Name AVP>
                        <Timestamp AVP>
                        <Initialization-Vector AVP>
                        {<Integrity-Check-Vector AVP> ||
                        <Digital-Signature AVP> }
```

AVP Format

A summary of the DIAMETER-EAP-Ind packet format is shown below. The fields are transmitted from left to right.



AVP Code

256 DIAMETER Command

AVP Length

The length of this attribute MUST be 12.

Command Flags

The following Command-specific flag bits may be set in the DIAMETER-EAP-Request command:

The 'C' (Authentication-only) bit may be set to indicate that only authentication of the user is required, and that no authorization should be performed. Additionally, no authorization AVPs are expected in the DIAMETER-EAP-Answer command.

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-Ind).

[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:

INTERNET DRAFT

August 1999

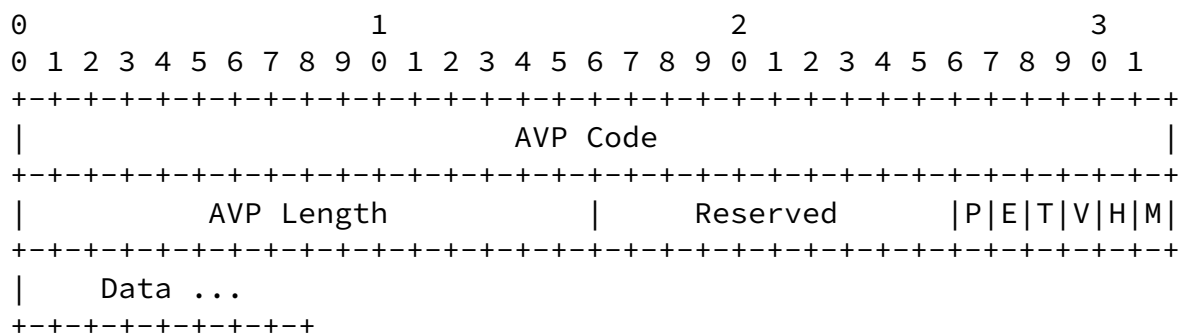
EAP-Packet ???

[3.1](#) EAP-Packet

Description

This attribute is used to contain the actual EAP payload [\[1\]](#) to be that is being exchanged between the dial-up PPP client and the home authentication server.

AVP Format



AVP Code

??? EAP-Packet

AVP Length

The length of this attribute MUST be at least 8.

AVP Flags

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

Data

The Data field contains an EAP Packet as defined in [1].

[4.0](#) Protocol overview

The EAP conversation between the authenticating peer and the NAS begins with the negotiation of EAP within LCP. Once EAP has been negotiated, the NAS will typically send to the DIAMETER server a

DIAMETER Message packet containing the DIAMETER-EAP-Request Command signifying an EAP-Start. EAP-Start is indicated by sending an DIAMETER-EAP-Request Command with an EAP-Packet attribute with a length of 8 (no data). The Port number and NAS Identifier MUST be included in the attributes issued by the NAS in the DIAMETER-EAP-Request packet.

If the DIAMETER server supports EAP, it MUST respond with an DIAMETER- EAP-Answer packet containing an EAP-Packet AVP. The EAP-Packet AVP includes an encapsulated EAP payload [1] which is then passed on to the authenticating PPP client. The DIAMETER-EAP-Answer typically will contain an EAP-Packet AVP encapsulating an EAP-Request/Identity message, requesting the authenticating PPP client to identify itself. The NAS will then respond with a DIAMETER-EAP-Request packet containing an EAP-Packet AVP encapsulating an EAP-Response [1], etc. The conversation continues until the DIAMETER server sends a DIAMETER-EAP-Answer with a Result-Code AVP is received. If the Result-Code AVP indicates an error, the EAP-Packet AVP SHOULD encapsulate an EAP-Failure [1] and the NAS SHOULD disconnect the user by issuing an LCP Terminate Request. If the Result-Code AVP indicates success, the EAP-Packet AVP MUST encapsulate an EAP-Success [1] and the NAS MUST successfully terminate the PPP authentication phase.

The above scenario creates a situation in which the NAS never needs to manipulate an EAP packet. An alternative may be used in situations where an EAP-Request/Identity message will always be sent by the NAS to the authenticating peer. This involves having the NAS send an EAP-Request/Identity message to the authenticating peer, and forwarding the EAP-Response/Identity packet to the DIAMETER server in the EAP-Packet attribute of a DIAMETER-EAP-Request packet. While this approach will save a round-trip, it cannot be universally employed.

There are circumstances in which the user's identity may not be needed (such as when authentication and accounting is handled based on the calling or called phone number), and therefore an EAP-Request/Identity packet may not necessarily be issued by the NAS to the authenticating peer.

Unless the NAS interprets the EAP-Response/Identity packet returned by the authenticating peer, it will not have access to the user's identity. Therefore, the DIAMETER Server SHOULD return the user's identity by inserting it in the User-Name attribute of subsequent DIAMETER-EAP-Answer packets. Without the user's identity, accounting and billing becomes very difficult to manage.

This document also describes the DIAMETER-EAP-Ind, which may be sent by DIAMETER Servers in order to initiate an unsolicited EAP authentication with the dial-up EAP Client. The document [8]

describes a situation where this is advantageous. By allowing the server to initiate the request, and to simply send an EAP challenge (assuming that the actual authentication protocol does have the concept of a challenge) the number of round trips required is significantly diminished. Upon receipt of such a message, the DIAMETER client is expected to send a DIAMETER-EAP-Request containing an EAP-Response [1] payload.

In cases where a backup DIAMETER servers is available, were the primary server to fail at any time during the EAP conversation, it would be desirable for the NAS to be able to redirect the conversation to an alternate DIAMETER server. In the event that this should occur, the EAP transaction will have to start from the beginning.

The DIAMETER-EAP-Answer with a successful Result-Code AVP MUST contain an encapsulated EAP-Success [1]. If the Authenticate-Only bit is NOT set, the packet MUST contain all of the expected AVPs that are currently returned in a DIAMETER AA-Answer [2].

For proxied DIAMETER requests there are two methods of processing. If the domain is determined based on the DNIS the DIAMETER Server may proxy the initial DIAMETER-EAP-Request/EAP-Start. If the domain is determined based on the user's identity, the local DIAMETER Server MUST respond with a DIAMETER-EAP-Answer/EAP-Identity packet. The

response from the authenticating peer MUST be proxied to the final authentication server.

For proxied DIAMETER requests, the NAS may receive an Command Unrecognized packet in response to its DIAMETER-EAP-Request/EAP-Identity packet. This would occur if the message was proxied to a DIAMETER Server which does not support the DIAMETER EAP extensions. At this point, the NAS MUST re-open LCP with the authenticating peer and request either CHAP or PAP as the authentication protocol. See [section 4.2](#) for additional packet exchange information.

If the NAS is unable to negotiate EAP with the authenticating peer, what happens next is a matter of policy. In circumstances where EAP is required of all users accessing the NAS, the NAS MUST disconnect the user. However, in circumstances where EAP is mandatory for some users, and optional or not required for others, the decision cannot be made until the user's identity is ascertained. In this case, the NAS will negotiate another authentication method, such as CHAP, and will pass the User-Name and CHAP-Password attributes to the DIAMETER Server in an Authentication-Request message. If the user is not required to use EAP, then the DIAMETER Server will respond with an AA-Answer [2]. However, should the user require EAP, then the DIAMETER Server will respond with an DIAMETER-EAP-Answer packet

containing an EAP-Packet attribute. The EAP-Packet attribute will either encapsulate an EAP- Request/Identity packet, or if the DIAMETER Server makes use of the User-Name attribute in the AA-Request [2], it may encapsulate an EAP challenge. On receiving the EAP-Packet attribute, the NAS will either attempt to negotiate EAP if it had not done so previously, or if negotiation had previously been attempted and failed, it MUST disconnect the user.

[4.1](#) Retransmission and Timers

As noted in [\[1\]](#), the EAP authenticator (NAS) is responsible for retransmission of packets between the authenticating peer and the NAS. Thus if an EAP packet is lost in transit between the authenticating peer and the NAS (or vice versa), the NAS will retransmit. As in DIAMETER [2], the DIAMETER client is responsible for retransmission of packets between the DIAMETER client and the DIAMETER server.

Note that it may be necessary to adjust authentication timeouts in certain cases. For example, when a token card is used additional time may be required to allow the user to find the card and enter the token. Since the NAS will typically not have knowledge of the required parameters, these need to be provided by the DIAMETER server. This can be accomplished by inclusion of EAP-Timeout and Password-Retry attributes within the EAP-Response packet.

[4.2](#) Example of an OTP Authentication

This section provides sample messages exchanges between an Authenticating Peer, which is typically a dial-up PPP client, a NAS and a DIAMETER server. The protocol used between the Dial-up PPP client and the NAS is EAP over PPP as defined in [\[1\]](#). The protocol between the NAS and the DIAMETER Server is EAP encapsulated within DIAMETER, as described in this specification.

For all PPP packets, the messages are formatted as:

[LCP Packet Type]
[EAP Packet Type]/[EAP Payload]

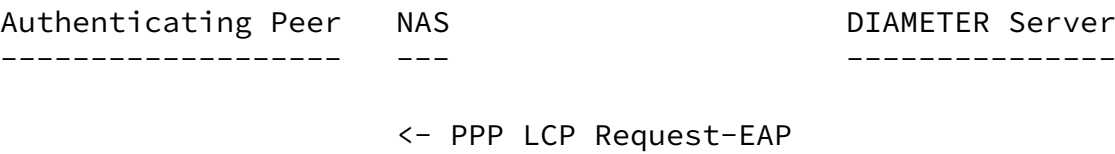
For all DIAMETER packets, the messages are formatted as:

[DIAMETER Command Code]/[EAP Packet Type]/[EAP Payload]

In the example provided below, the PPP client attempts to authenticate using a One-Time-Password [\[12\]](#) encapsulated within EAP [\[1\]](#).

[4.2.1](#) Successful Authentication

The example below shows the conversation between the authenticating peer, NAS, and server, for the case of a One Time Password (OTP) authentication. OTP is used only for illustrative purposes; other authentication protocols could also have been used, although they would show somewhat different behavior.



	auth	
PPP LCP ACK-EAP auth ->	DIAMETER- EAP-Request/ EAP-Packet/Start ->	<- DIAMETER- EAP-Answer/ EAP-Packet/Identity
	<- PPP EAP-Request/ Identity	
PPP EAP-Response/ Identity (MyID) ->	DIAMETER- EAP-Request/ EAP-Packet/ EAP-Response/ (MyID) ->	<- DIAMETER- EAP-Answer/ EAP-Packet/EAP-Request OTP/OTP Challenge
	<- PPP EAP-Request/ OTP/OTP Challenge	
PPP EAP-Response/ OTP, OTPpw ->	DIAMETER- EAP-Request/ EAP-Packet/ EAP-Response/ OTP, OTPpw ->	<- DIAMETER- EAP-Answer/ EAP-Packet/EAP-Success (other attributes)
	<- PPP EAP-Success	
PPP Authentication Phase complete, NCP Phase starts		

[4.2.2](#) NAS Initiated EAP Authentication

In the case where the NAS sends the authenticating peer an

EAP- Request/Identity packet without first sending an EAP-Start packet to the DIAMETER server, the conversation would appear as follows:

Authenticating Peer -----	NAS ---	DIAMETER Server -----
	<- PPP LCP Request-EAP auth	
PPP LCP ACK-EAP auth ->		
	<- PPP EAP-Request/ Identity	
PPP EAP-Response/ Identity (MyID) ->		
	DIAMETER- EAP-Request/ EAP-Packet/ EAP-Response/ (MyID) ->	
		<- DIAMETER- EAP-Answer/ EAP-Packet/EAP-Request OTP/OTP Challenge
	<- PPP EAP-Request/ OTP/OTP Challenge	
PPP EAP-Response/ OTP, OTPpw ->		
	DIAMETER- EAP-Request/ EAP-Packet/ EAP-Response/ OTP, OTPpw ->	
		<- DIAMETER- EAP-Answer/ EAP-Packet/EAP-Success (other attributes)
	<- PPP EAP-Success	
PPP Authentication Phase complete, NCP Phase starts		

4.2.3 Server-Initiated Authentication

As described in [8], when a server has successfully authenticated and

authorized a user, it may include a timeout period to the

INTERNET DRAFT

August 1999

authorization. The server can later initiate an unsolicited re-authentication request to the user, through the NAS. This method has the advantage of reducing the number of round trips required for re-authentication/authorization.

Authenticating Peer -----	NAS ---	DIAMETER Server -----
		<- DIAMETER-EAP-Ind/ EAP-Packet/EAP-Request OTP/OTP Challenge
	<- PPP EAP-Request/ OTP/OTP Challenge	
PPP EAP-Response/ OTP, OTPpw ->	DIAMETER- EAP-Request/ EAP-Packet/ EAP-Response/ OTP, OTPpw ->	
		<- DIAMETER- EAP-Answer/ EAP-Packet/EAP-Success (other attributes)
	<- PPP EAP-Success	

[4.2.4](#) Example of failed EAP Authentication

In the case where the client fails EAP authentication, the conversation would appear as follows:

INTERNET DRAFT

August 1999

Authenticating Peer -----	NAS ---	DIAMETER Server -----
	<- PPP LCP Request-EAP auth	
PPP LCP ACK-EAP auth ->	DIAMETER- EAP-Request/ EAP-Packet/Start ->	
	<- PPP EAP-Request/ Identity	<- DIAMETER- EAP-Answer/ EAP-Packet/Identity
PPP EAP-Response/ Identity (MyID) ->	DIAMETER- EAP-Request/ EAP-Packet/ EAP-Response/ (MyID) ->	
	<- PPP EAP-Request/ OTP/OTP Challenge	<- DIAMETER- EAP-Answer/ EAP-Packet/EAP-Request OTP/OTP Challenge
PPP EAP-Response/ OTP, OTPpw ->	DIAMETER- EAP-Request/ EAP-Packet/	

EAP-Response/
OTP, OTPpw ->

<- DIAMETER-
EAP-Answer/
EAP-Packet/EAP-Failure

<- PPP EAP-Failure

<- LCP Terminate

[4.2.5](#) Example of DIAMETER not supporting EAP

In the case that the DIAMETER server or proxy does not support EAP extensions the conversation would appear as follows:

Calhoun, Rubens, Haag

expires January 2000

[Page 18]

INTERNET DRAFT

August 1999

Authenticating Peer

NAS

DIAMETER Server

PPP LCP ACK-EAP
auth ->

<- PPP LCP Request-EAP
auth

DIAMETER
EAP-Request/
EAP-Packet/Start ->

<- DIAMETER
Command-Unrecognized

<- PPP LCP Request-CHAP
auth

PPP LCP ACK-CHAP
auth ->

<- PPP CHAP Challenge

PPP CHAP Response ->

DIAMETER
AA-Request->

<- DIAMETER
AA-Answer

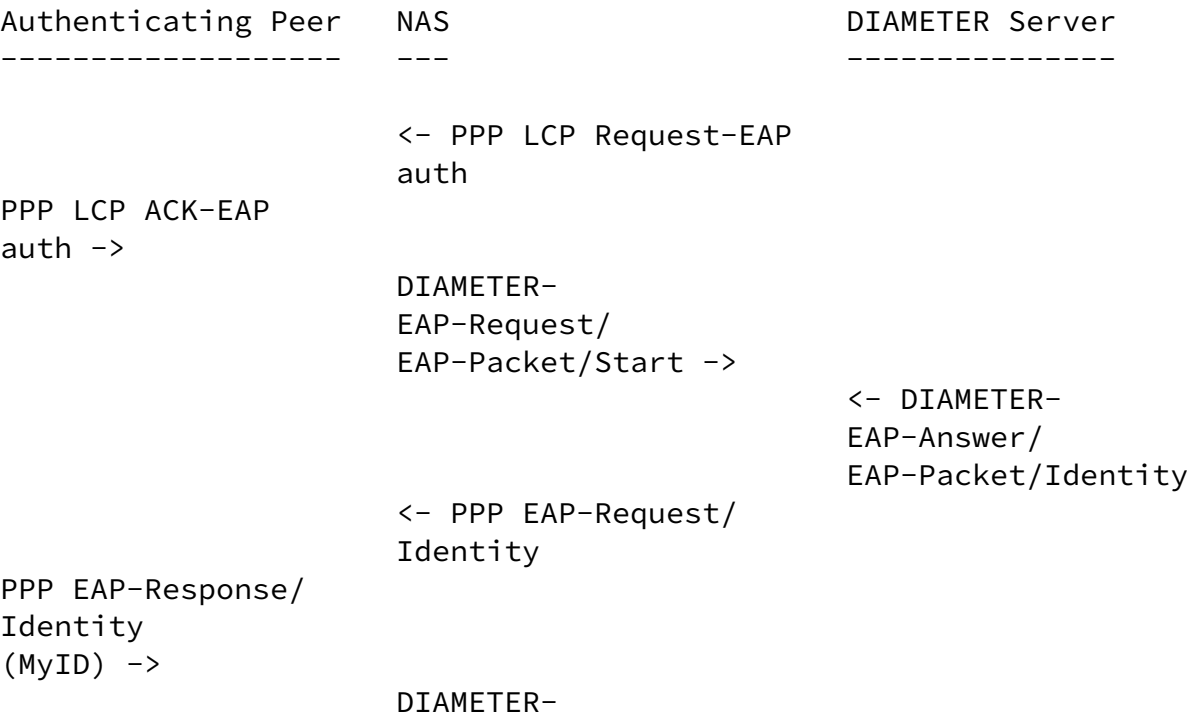
<- PPP LCP
CHAP-Success

PPP Authentication

Phase complete,
NCP Phase starts

4.2.6 Example of DIAMETER Proxy not supporting EAP

In the case where the local DIAMETER Server does support the EAP extensions but the remote DIAMETER Server does not, the conversation would appear as follows:



	EAP-Request/ EAP-Packet/EAP-Response/ (MyID) ->	<- DIAMETER- EAP-Answer (proxied from remote DIAMETER Server)
	<- PPP LCP Request-CHAP auth	
PPP LCP ACK-CHAP auth ->		
	<- PPP CHAP Challenge	
PPP CHAP Response ->		
	DIAMETER AA-Request->	<- DIAMETER AA-Answer (proxied from remote DIAMETER Server)
	<- PPP LCP CHAP-Success	
PPP Authentication Phase complete, NCP Phase starts		

[4.2.7](#) Example of PPP Client not supporting EAP

In the case where the authenticating peer does not support EAP, but

where EAP is required for that user, the conversation would appear as follows:

Authenticating Peer -----	NAS ---	DIAMETER Server -----
	<- PPP LCP Request-EAP auth	
PPP LCP NAK-EAP auth ->		
	<- PPP LCP Request-EAP auth	

```

PPP LCP NAK-EAP
auth ->

                                <- PPP LCP Request-CHAP
                                auth

PPP LCP ACK-CHAP
auth ->

                                <- PPP CHAP Challenge

PPP CHAP Response ->

                                DIAMETER-
                                AA-Request/
                                User-Name,
                                CHAP-Password ->

                                <- DIAMETER-
                                EAP-Answer/
                                EAP-Packet

                                <- LCP Terminate Req

```

[4.3](#) Feature Advertisement/Discovery

As defined in [8], the Reboot-Ind and Device-Feature-Query messages can be used to inform a peer about locally supported DIAMETER Extensions. In order to advertise support of this extension, the Extension-Id AVP must be transmitted with a value of three (3).

[5.0](#) Alternative uses

Currently the conversation between the backend security server and the DIAMETER server is proprietary because of lack of standardization. In order to increase standardization and provide interoperability between DIAMETER vendors and backend security vendors, it is recommended that DIAMETER-encapsulated EAP be used for this conversation.

This has the advantage of allowing the DIAMETER server to support EAP without the need for authentication-specific code within the DIAMETER server. Authentication-specific code can then reside on a backend security server instead.

In the case where DIAMETER-encapsulated EAP is used in a conversation between a DIAMETER server and a backend security server, the Security Server will typically return an DIAMETER-EAP-Answer/EAP-Packet/EAP-Success message without inclusion of the expected attributes currently returned in a successful AA-Answer [2]. This means that the DIAMETER server MUST add these attributes prior to sending an DIAMETER-EAP- Answer/EAP-Packet/EAP-Success message to the NAS.

[6.0](#) IANA Considerations

The numbers for the Command Code AVPs ([section 3](#)) is taken from the numbering space defined for Command Codes in [2]. The numbers for the various AVPs defined in [section 4](#) were taken from the AVP numbering space defined in [2]. The numbering for the AVP and Command Codes MUST NOT conflict with values specified in [2] and other DIAMETER related Internet Drafts.

This document also introduces two new bits to the AVP Header, which MUST NOT conflict with the base protocol [2] and any other DIAMETER extension.

[7.0](#) Acknowledgments

Thanks for Bernard Aboba for his contribution to [9]. Much of the text found in this draft was taken directly from the said draft.

[8.0](#) References

- [1] L. J. Blunk, J. R. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)." [RFC 2284](#), March 1998.
- [2] P. R. Calhoun, "DIAMETER Authentication Extension", [draft-calhoun-diameter-auth-06.txt](#), August 1999.
- [3] C. Rigney, A. Rubens, W. Simpson, S. Willens, "Remote Authentication DialIn User Service (RADIUS)." [RFC 2138](#), April 1997.
- [4] C. Rigney, "RADIUS Accounting." [RFC 2139](#), April 1997.
- [5] R. Rivest, S. Dusse, "The MD5 Message-Digest Algorithm", [RFC 1321](#), April 1992
- [6] S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.

- [7] P. R. Calhoun, A. Rubens, "DIAMETER Base Protocol", [draft-calhoun-diameter-08.txt](#), August 1999.
- [8] G. Zorn, P. R. Calhoun, "Limiting Fraud in Roaming", [draft-ietf-roamops-fraud-limit-00.txt](#), May 1999.
- [9] P. R. Calhoun, A. Rubens, B. Aboba, "Extensible Authentication Protocol Support in RADIUS", [draft-ietf-radius-eap-05.txt](#), Work in Progress, May 1998.
- [10] Narten, Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", [BCP 26](#), [RFC 2434](#), October 1998
- [11] W. Simpson, "The Point-to-Point Protocol (PPP)", [RFC 1661](#), July 1994.
- [12] N Haller, C. Metz, P. Nessel, M. Straw, "A One-Time Password (OTP) System", [RFC 2289](#), February 1998.
- [13] P. Calhoun, W. Bulley, "DIAMETER Proxy Server Extensions", [draft-calhoun-diameter-proxy-02.txt](#), Work in Progress, August 1999.

[9.0](#) Authors' Addresses

Questions about this memo can be directed to:

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

Allan C. Rubens
Ascend Communications
1678 Broadway
Ann Arbor, MI 48105-1812
USA

Phone: 1-734-761-6025
E-Mail: acr@del.com

Jeff Haag
Cisco Systems
7025 Kit Creek Road

INTERNET DRAFT

August 1999

PO Box 14987
Research Triangle Park, NC 27709

Phone: 1-919-392-2353
E-Mail: haag@cisco.com

10.0 Full Copyright Statement

Copyright (C) The Internet Society (1999). 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."

Calhoun, Rubens, Haag expires January 2000