AAA Working Group
Internet-Draft
Category: Informational
<draft-calhoun-diameter-impl-guide-05.txt>

Pat R. Calhoun
Sun Microsystems, Inc.
Allan C. Rubens
Tut Systems, Inc.
Haseeb Akhtar
Nortel Networks
William Bulley
Merit Network, Inc.
Jeff Haag
Cisco Systems
February 2001

Diameter Implementation Guidelines

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

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

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

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.

Abstract

The Diameter protocol is used for Authentication, Authorization and Accounting (AAA) for Mobile-IP, ROAMOPS and NASREQ. This document contains implementation guidelines that may be useful to Diameter protocol developers.

Table of Contents

1.0 Introduction

The Diameter protocol is used for Authentication, Authorization and Accounting (AAA) for Mobile-IP, ROAMOPS and NASREQ. This document contains implementation guidelines that may be useful to Diameter protocol developers.

This specification contains implementation guidelines for both the Diameter base protocol [2] and the NASREQ extension [3].

2.0 Base Protocol

This section contains implementation guidelines for the Diameter Base protocol [2].

2.1 Backward Compatibility with RADIUS

The Diameter protocol was designed with RADIUS [1] compatibility in mind. The RADIUS protocol defines a one octet attribute space, and the Diameter protocol reserves the first 255 attribute identifiers to be the same as those defined in RADIUS. This allows Diameter servers to easily perform protocol conversion, since an additional dictionary lookup would not be necessary in order to map a RADIUS attribute to a Diameter AVP.

By re-using the RADIUS attribute space, a Diameter server could easily read a typical RADIUS user profile without any additional conversions. This reduces the need to create duplicate user profiles for both protocols, and also does not require any database conversion while reading the profiles.

2.2 Device-Reboot-Ind Message Flow

The following figure depicts a sample flow of Device-Reboot-Ind between three Diameter peers, one being a proxy or broker server. In this example DIA1 initiates the bootstrap sequence with DIA2, and later DIA3 initiates the bootstrap sequence with DIA2. After some time DIA1 needs to reboot and informs DIA2. The details of each message is provided below.

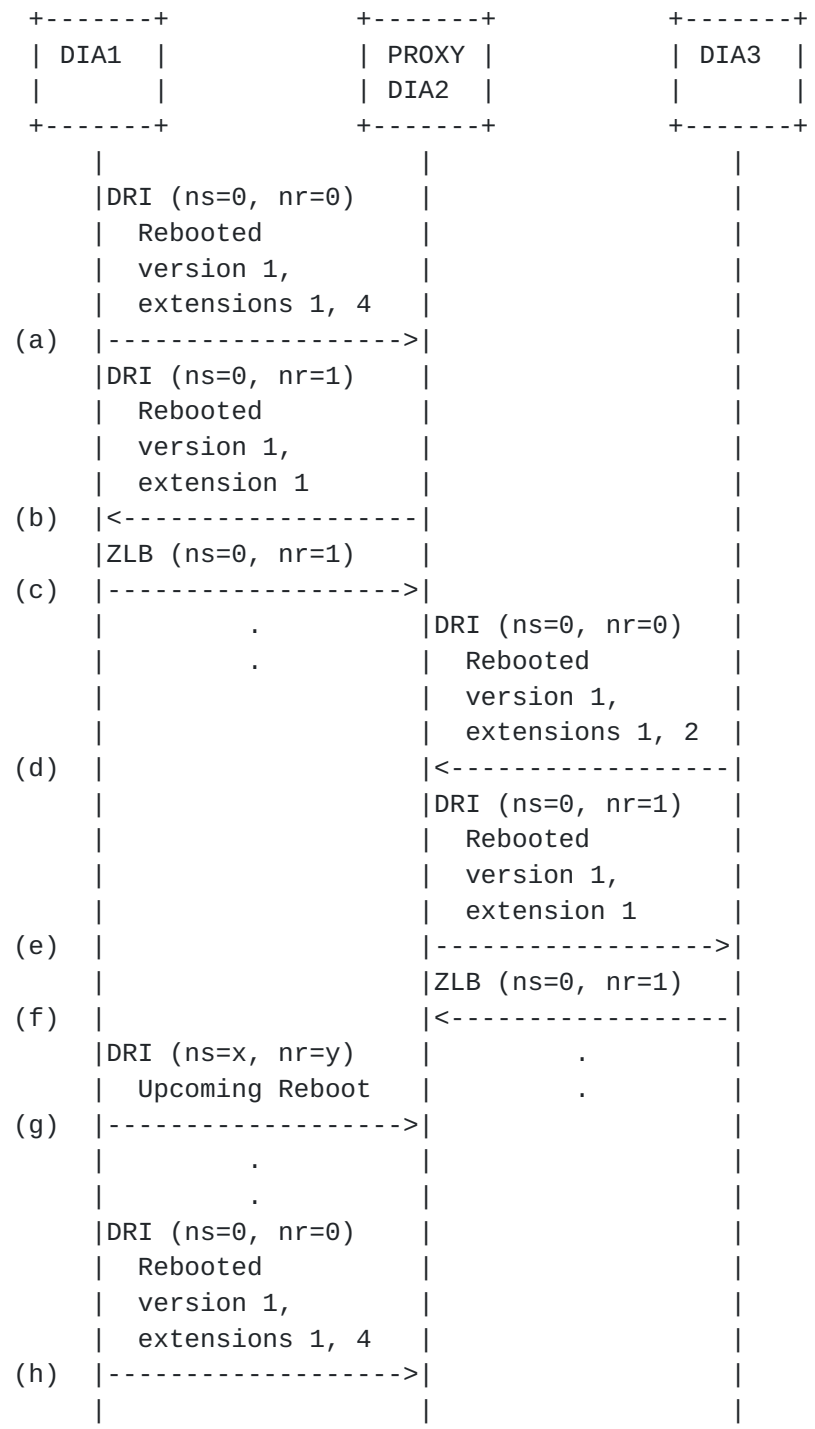


Figure 1: Sample DRI Message Flow in a Proxy Environment

(a) DIA1 sends a DRI message to DIA2 indicating that its version is one (1) and that it supports extensions 1 (NASREQ) and 4 (Mobile-IP).

(b) DIA2 sends a DRI message to DIA1 indicating that its version is one (1) and that it supports extension 1 (NASREQ). This

message also includes a piggy-backed acknowledgement of (a).

(c) DIA1 sends an acknowledgement of (b)

(d) DIA3 sends a DRI message to DIA2 indicating that its version is one (1) and that it supports extension 1 (NASREQ) and 2 (Strong Security).

(e) DIA2 sends a DRI message to DIA3 indicating that its version is one (1) and that it supports extension 1 (NASREQ). This message also includes a piggy-backed acknowledgement of (d).

(f) DIA3 sends an acknowledgement of (e)

(g) after some time DIA1 sends an indication to DIA2 that it is about to reboot. All messages destined to the realm for which DIA1 is responsible for should be redirected to an alternate Diameter Server.

(h) Once the reboot is complete, DIA sends the DRI, which causes steps (a) through (c) to be repeated.

2.3 Message-Reject-Ind Message Flow

The following figure show sample flows of MRI command between two Diameter peers. In this example DIA1 and DIA2 servers generates error messages. The details of the messages are provided below.

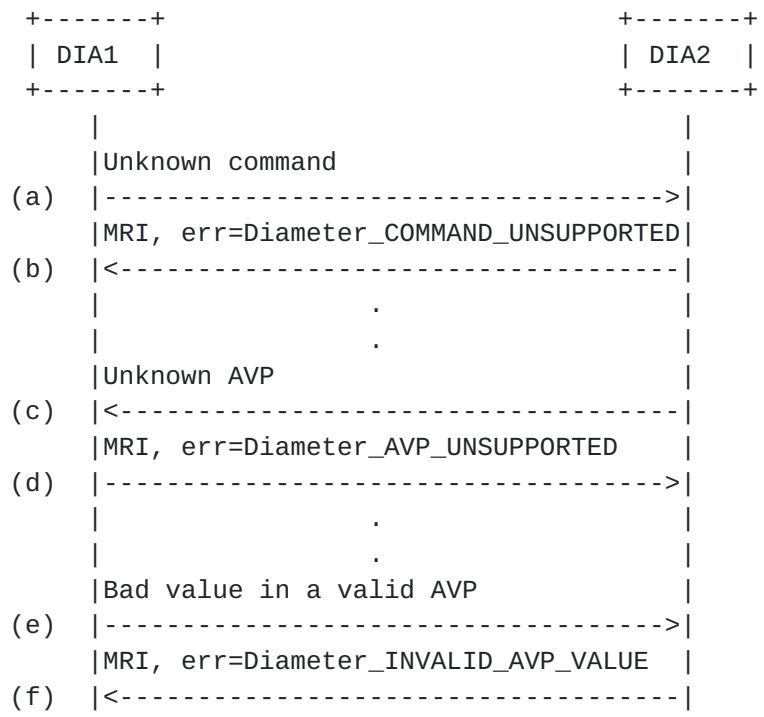


Figure 2: Sample MRI Message Flow

(a) DIA2 receives an unknown command from DIA1.

(b) DIA2 recognizes that it received an unknown command and hence sends an MRI with the Result-Code AVP set to Diameter_COMMAND_UNSUPPORTED and the Command-Code AVP encapsulated within the Failed-AVP AVP.

(c) DIA1 receives an unknown AVP in a message sent by DIA2.

(d) DIA1 recognizes that it received an unknown AVP and returns an MRI with the Result-Code AVP set to Diameter_AVP_UNSUPPORTED and the offending AVP encapsulated within a Failed-AVP AVP.

(e) DIA2 receives a bad parameter within a otherwise valid AVP from DIA1.

(f) As soon as it discovers that it has received a bad parameter, it returns an MRI message to DIA1 with the Result-Code AVP set to Diameter_INVALID_AVP_VALUE and the offending AVP encapsulated within a Failed-AVP AVP.

2.4 Peer Fail-Over and Load Balancing

Although not a function of the Diameter protocol, in some networks it is desirable to ensure resilient service by providing alternate

peers, should communication with a peer fail. Figure 3 provides an example of such a network, where the client communicates with one of two servers providing proxying services. The proxy servers, in turn, communicate with one of two servers in the home administrative domain.

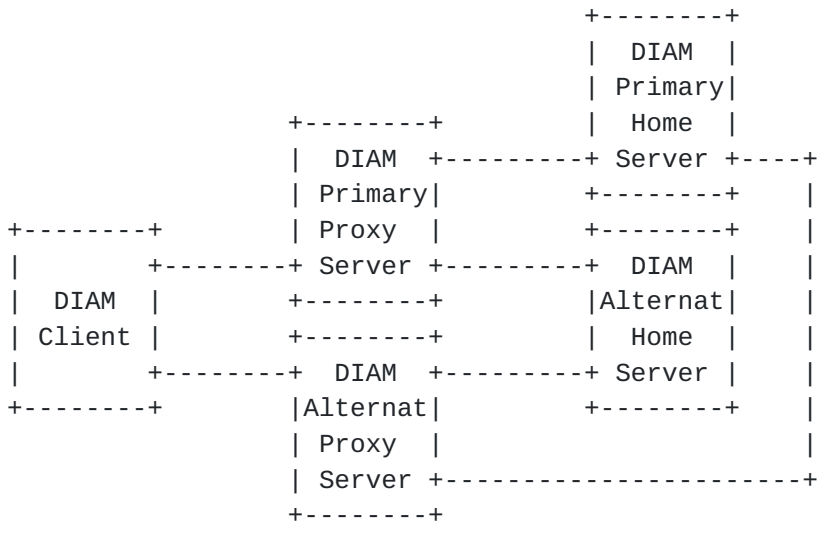


Figure 3: Redundant Diameter Servers

Each node in the network MUST know a priori about its communicating peers, and each peer MAY have a relative priority, forcing all traffic to be sent through a preferred server, if it is available. When a node detects that a communicating peer is no longer available, it MUST attempt to redirect all traffic (including the packets in the retransmission queue destined for the former peer) to the new peer. It is possible that an alternate path not exist, such would be the case if the Diameter Client was no longer reachable. In this case, the Diameter proxy servers SHOULD drop all responses directed to the client, and MUST respond to all requests directed to the client with an appropriate Result Code.

An implementation MAY also make use of the multiple peer arrangement described above to balance the load between a set of peers. A clever implementation MAY also redirect traffic to an alternate peer when it detects that its primary communicating peer's window is full.

2.5 Multiple IP Addresses

SCTP supports multiple IP addresses per Diameter host, and the Host-Name AVP MAY resolve to more than one address. The alternate addresses supplied by the host name resolution SHOULD be used to determine the complete set of addresses indicated by the Host-Name AVP.

2.6 Maintaining Per-Request State

Some applications of Diameter servers require that local state information be maintained for each request, to assist in the processing of the corresponding response. It is important to note that a Diameter server that maintains per-request state information introduces a single point of failure, reducing the reliability of the service. There are two methods that MAY be implemented that allow per-request state information to be maintained:

1. DIA2 MAY maintain a state control block to allow it to match a response with a corresponding request. The state control block MAY include AVPs that need to be added to the response, or any additional policy decisions that will need to be made when the response is received.

2. DIA2 MAY add a Proxy-State AVP (see section 6.2.1) to a request, which may contain any state information that will be needed when the corresponding response is received. When a Diameter node adds its own Proxy-State AVP to a message that already includes such an AVP, it MUST ensure that the original AVP is present in the corresponding response. One suggested method is to "encapsulate" the original Proxy-State AVP in the new Proxy-State AVP.

3.0 NASREQ Extension

This section contains implementation guidelines for the NASREQ Diameter Extension [3].

3.1 RADIUS/Diameter Protocol Interactions

This section describes some basic guidelines that may be used by servers that act as protocol gateways. Note that this document does not restrict implementations from creating other methods, as long as the bridging function doesn't break the RADIUS nor the Diameter protocol.

There are essentially two different situations that must be handled; one where a RADIUS request is received that must be forwarded as a Diameter request, and the inverse. Note that this section uses two different terms; AVP and attribute. The former is used to signify a Diameter AVP, while the latter is used to signify a RADIUS attribute.

3.1.1 RADIUS request forwarded as Diameter request

This section describes the actions that should be followed when a protocol Gateway receives a RADIUS message that is to be translated to a Diameter message.

It is important to note that RADIUS servers are inherently stateless, and this section maintains that assumption. It is quite possible for the RADIUS messages that comprises the session (i.e. authentication and accounting messages) be handled by different protocol gateways in the proxy network.

When a protocol gateway receives a RADIUS message, the following steps should be taken:

- The NAS-IP-Address and/or NAS-Identifier AVPs are included in the Diameter request. These AVPs identify the NAS providing the service to the user.
- The Host-Name AVP is added with the local server's identity. This will ensure that the corresponding response will be returned to the correct gateway server.
- The Gateway Server must maintain state information relevant to the RADIUS request, such as the Identifier field in the RADIUS header, any existing RADIUS Proxy-State attribute as well as the source IP address and port number of the UDP packet. These may be maintained locally in a state table, or may be saved in a Proxy-State AVP.
- If the Acct-Session-Id attribute was found in the request, the contents are inserted in the Acct-Session-Id AVP.
- If the RADIUS request contained a Class or State attribute, the contents of the attribute contain the Diameter Session-Id. If no such attributes are present, and the RADIUS command is an Access-Request, a new Session-Id is created. The Session-Id is included in the Session-Id AVP.

The corresponding Diameter response is always guaranteed to be received by the same protocol gateway that translated the original request, due to the contents of the Host-Name AVP in the Diameter request. The following steps are applied to the response message during the Diameter to RADIUS translation:

- If the Diameter Command-Code is set to AA-Challenge, the Diameter Session Idenfitier is saved in the RADIUS State attribute. This is necessary in order to ensure that the protocol gateway that will receive the subsequent RADIUS Access-Request will have access to the Session Identifier.
- If the Command-Code is set to AA-Answer, the Diameter Session Identifier is saved in a new RADIUS Class attribute, whose format consists of the string "Diameter/" followed by the Diameter Session Identifier. This will ensure that the

subsequent Accounting messages, which could be received by any protocol gateway, would have access to the original Diameter Session Identifier.
- If a Proxy-State attribute was present in the RADIUS request, the same attribute is added in the response. This information may be found in the Proxy-State AVP, or in a local state table.
- If state information regarding the RADIUS request was saved in a Proxy-State AVP, the RADIUS Identifier and UDP IP Address and port number are extracted and used in issuing the RADIUS reply.

3.1.2 Diameter request forwarded as RADIUS request

When a server receives a Diameter request that is to be forwarded to a RADIUS entity, the following steps are an example of the steps that may be followed:

- The Host-Name AVP's value is inserted in the NAS-Identifier attribute. Since the contents of the Host-Name AVP is in an NAI [6] format, and the NAS-Idenfitier follows the Fully Qualified Domain Name (FQDN) syntax rules, the NAI's realm delimited '@' must be replaced by a dot '.'.
- The Host-Name and Session Identifier must be retained in order to ensure that the information is present in the corresponding response. The gateway server may keep this information in a local state table, or may add the information in a RADIUS Proxy-State attribute.

When the corresponding response is received by the gateway server, which is guaranteed in the RADIUS protocol, the following steps may be followed:

- If a Proxy-State AVP is present, extract the Host-Name and Session Identifier information, otherwise find the information in a local state table.
- The Host-Name information is added to the Destination-NAI AVP.
- The Session-Id information is added to the Session-Id AVP.
- If the RADIUS Class or State attributes are present, these attributes must be present in the Diameter response.

3.2 EAP Retransmission and Timers

As noted in [4], the EAP authenticator (NAS) is responsible for retransmission of packets between the authenticating peer (PPP client) 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. Since Diameter operates over SCTP [7], which provides

reliability, all EAP packets sent to a Diameter peer will be retransmitted automatically.

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 the Idle-Timeout in the Diameter-EAP-Answer message.

3.3 Example of an EAP 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 [4]. 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]
```

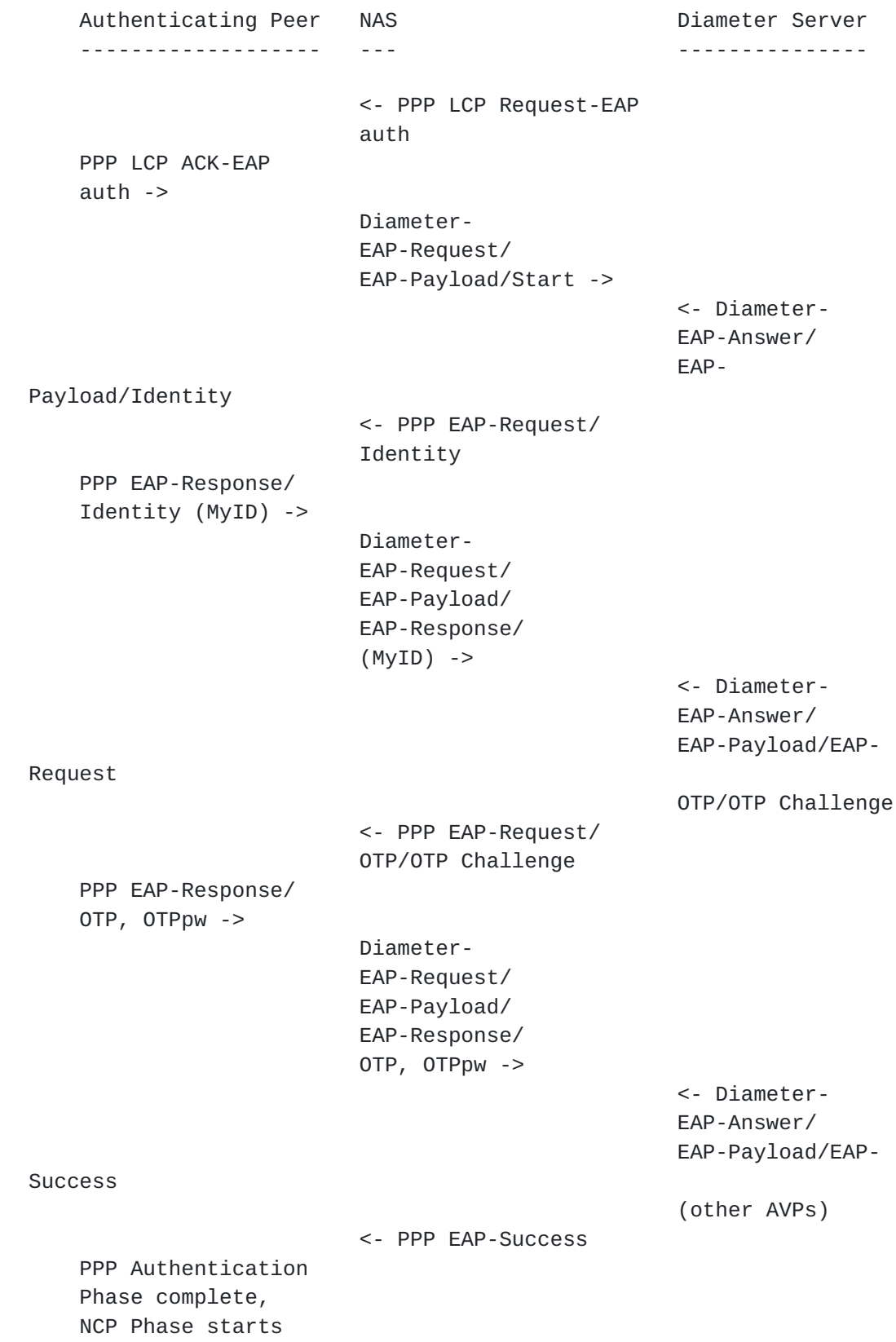
For all Diameter packets, the messages are formatted as:

```
[Diameter Command Code]/[EAP Packet Type]/[EAP Payload]
```

In the example provided below, the PPP client attempts to authenticate using a One-Time-Password [5] encapsulated within EAP [4].

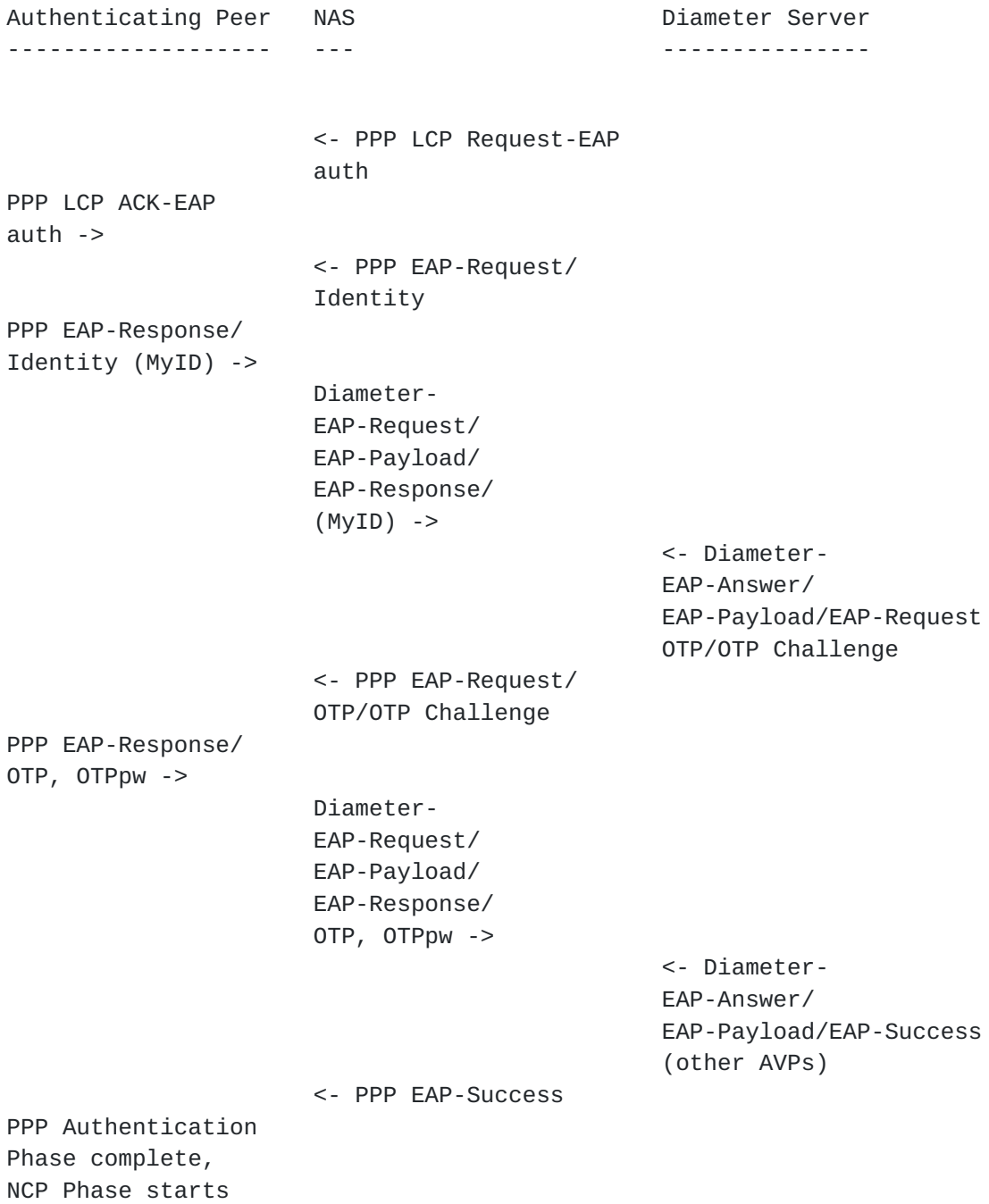
3.3.1 Successful Authentication

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.


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

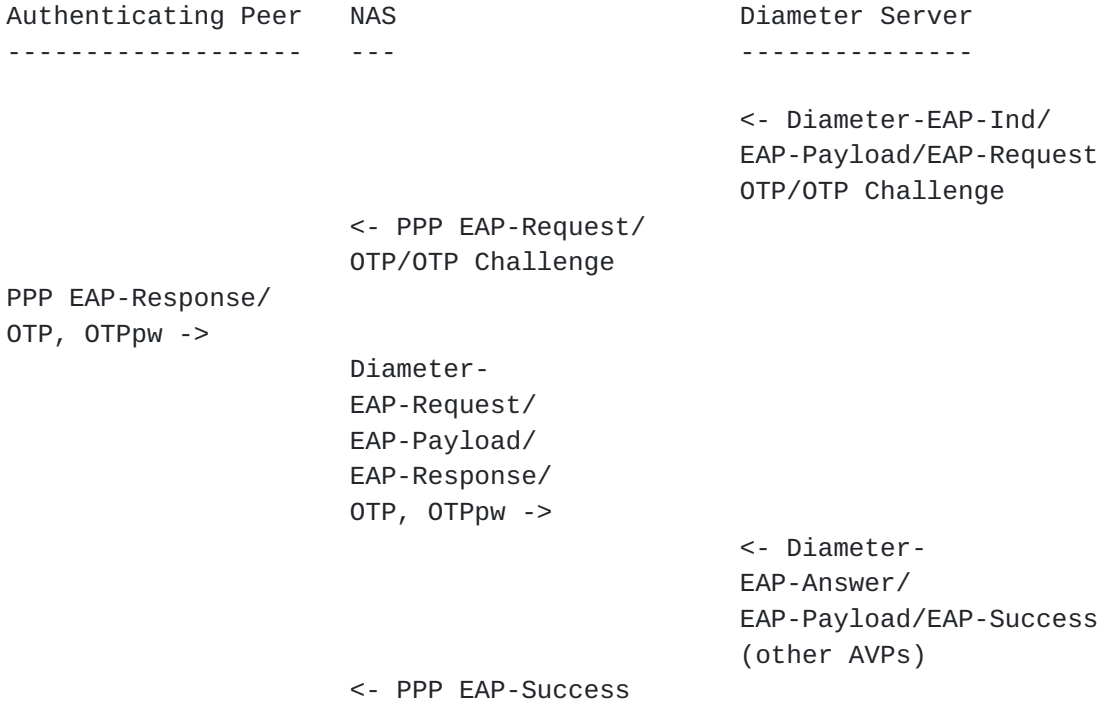
3.3.2: NAS Initiated EAP Authentication

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:



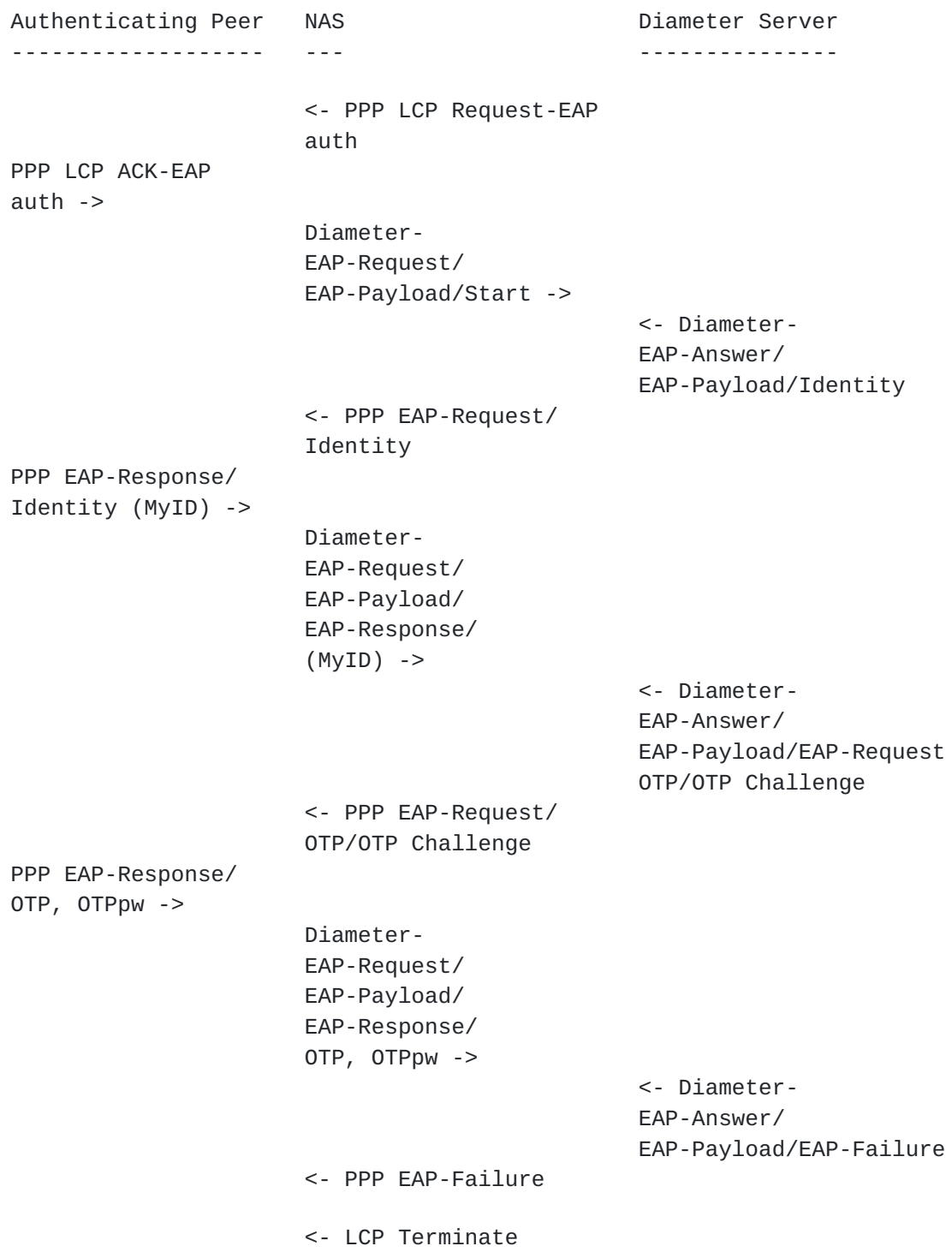
3.3.3: Server-Initiated Authentication

When a server has successfully authenticated and authorized a user, it may include a timeout period to the 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.



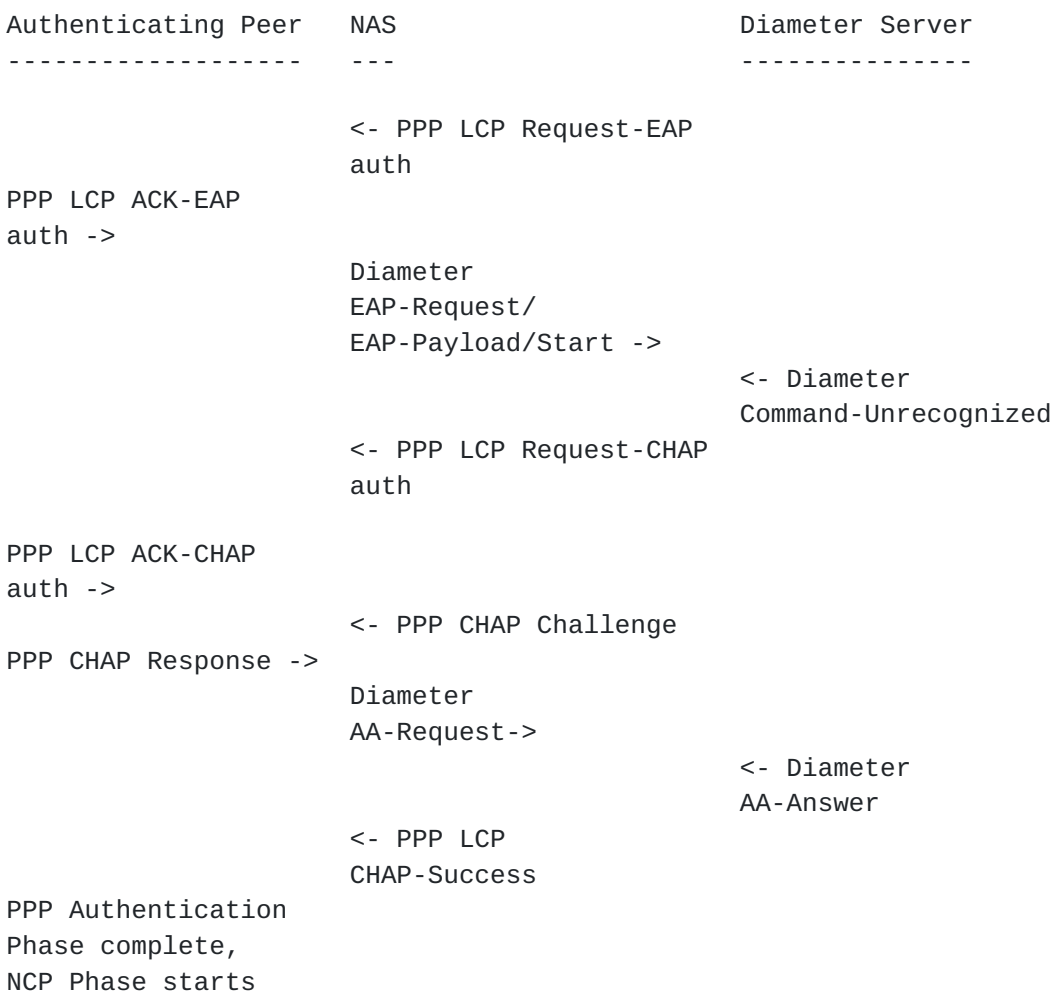
3.3.4: Example of failed EAP Authentication

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



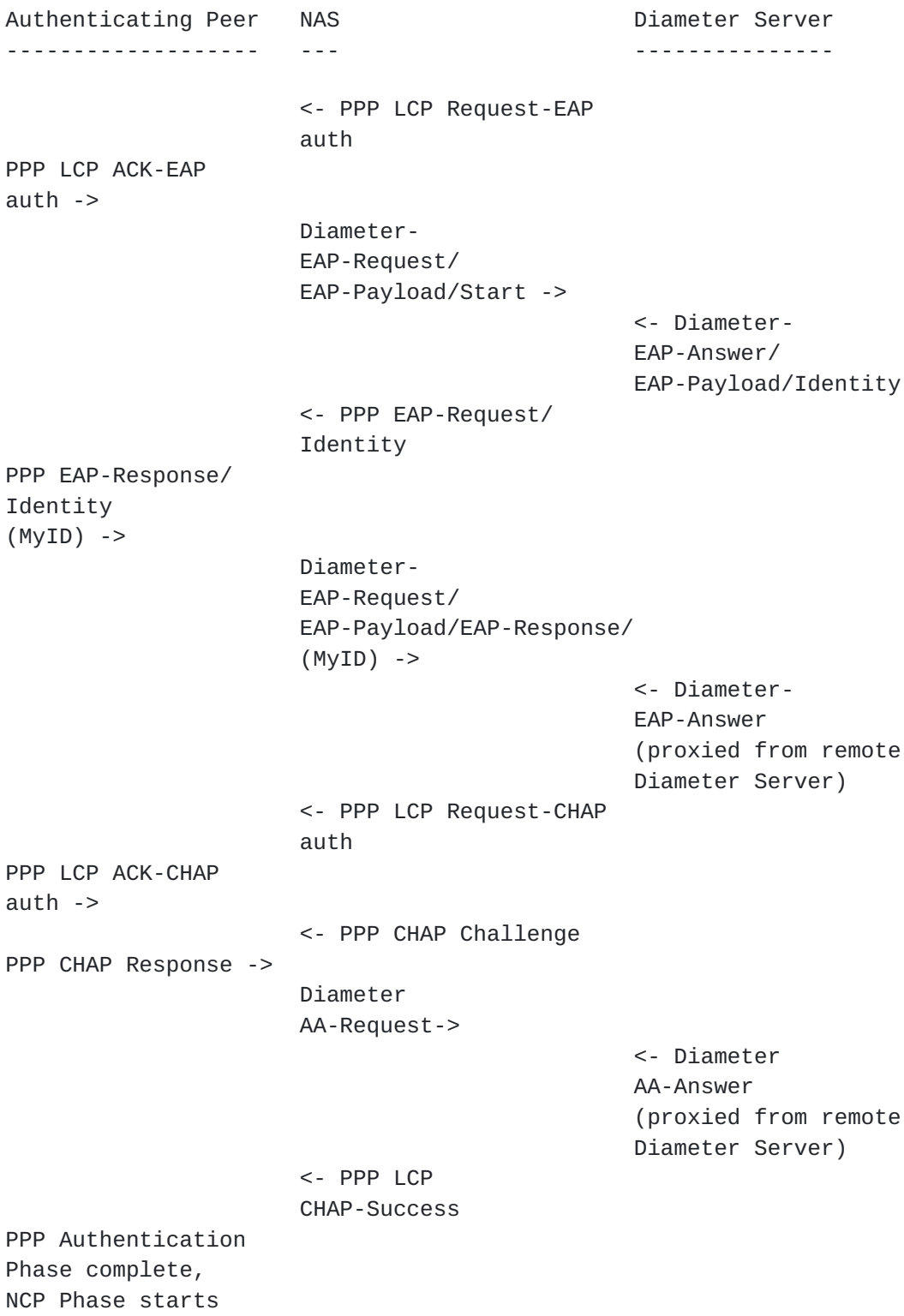
3.3.5: Example of Diameter Server not supporting EAP

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



3.3.6: Example of Diameter Proxy not supporting EAP

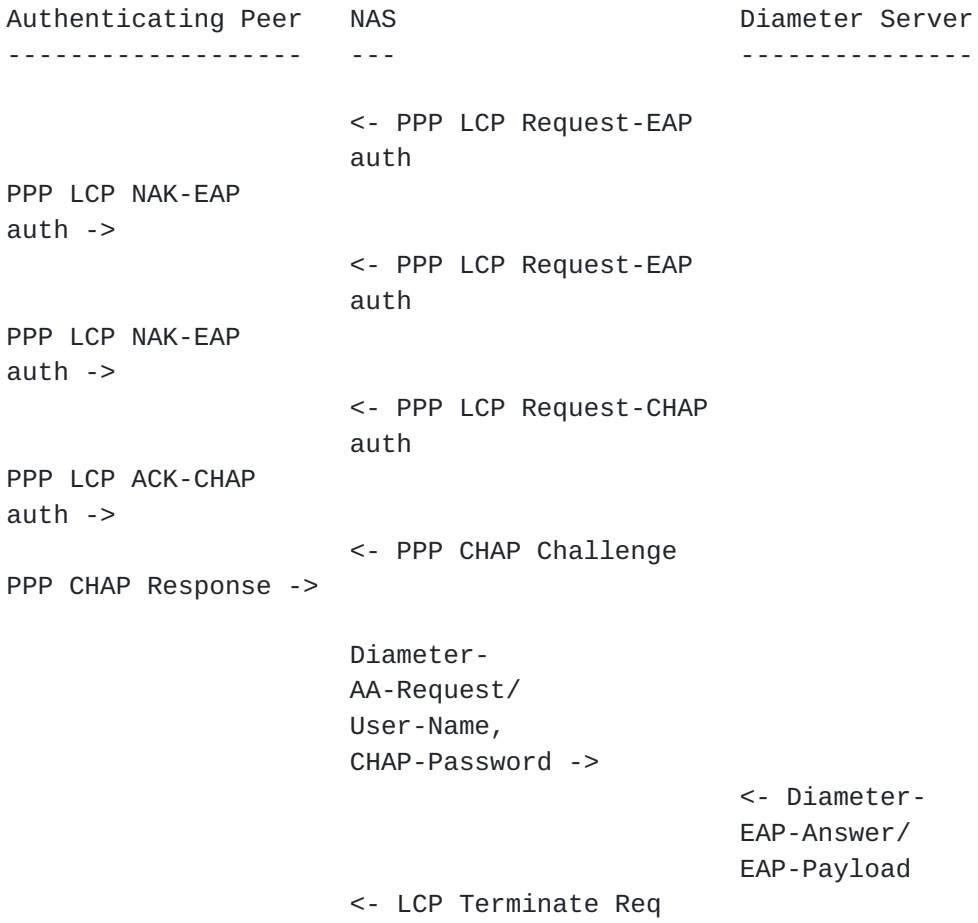
In the case where the local Diameter Server does support the EAP extensions but the remote Diameter Server does not, the conversation would appear as follows:



3.3.7: 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:



4.0 References

[1] Rigney, et alia, "RADIUS", RFC-2138, April 1997

[2] P. Calhoun, A. Rubens, H. Akhtar, E. Guttman, "Diameter Base Protocol", draft-calhoun-diameter-15.txt, IETF work in progress, June 2000.

[3] P. Calhoun, W. Bulley, A. Rubens, J. Haag, "Diameter NASREQ Extension", draft-calhoun-diameter-nasreq-03.txt, IETF work in progress, April 2000.

[4] L. J. Blunk, J. R. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)." RFC 2284, March 1998.

[5] N Haller, C. Metz, P. Nesset, M. Straw, "A One-Time Password

(OTP) System", RFC 2289, February 1998.

[6] Aboba, Beadles "The Network Access Identifier." RFC 2486. January 1999.

[7] R. Stewart et al., "Simple Control Transmission Protocol", draft-ietf-sigtran-sctp-09.txt, IETF Work in Progress, April 2000.

5.0 Acknowledgements

The authors would like to thank Nenad Trifunovic, Tony Johansson and Pankaj Patel for their participation in the Document Reading Party. Also a big thanks to Erik Guttman and David Spence for their invaluable help in cleaning up this document.

The authors would also like to acknowledge the following people for their contribution in the development of the Diameter protocol:

Bernard Aboba, Jari Arkko, William Bulley, Daniel C. Fox, Lol Grant, Ignacio Goyret, Nancy Greene, Peter Heitman, Paul Krumviede, Fergal Ladley, Ryan Moats, Victor Muslin, Kenneth Peirce, Sumit Vakil, John R. Vollbrecht and Jeff Weisberg and Glen Zorn.

6.0 Authors' Addresses

Questions about this memo can be directed to:

Pat R. Calhoun
Network and Security Research Center, Sun Laboratories
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
Tut Systems, Inc.
220 E. Huron, Suite 260
Ann Arbor, MI 48104
USA

Phone: 1-734-995-1697
E-Mail: arubens@tutsys.com

Haseeb Akhtar
Wireless Technology Labs
Nortel Networks
2221 Lakeside Blvd.
Richardson, TX 75082-4399
USA

Phone: 1-972-684-8850
E-Mail: haseeb@nortelnetworks.com

William Bulley
Merit Network, Inc.
Building One, Suite 2000
4251 Plymouth Road
Ann Arbor, Michigan 48105-2785
USA

Phone: 1-734-764-9993
Fax: 1-734-647-3185
E-mail: web@merit.edu

Jeff Haag
Cisco Systems
7025 Kit Creek Road
PO Box 14987
Research Triangle Park, NC 27709

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

7.0 Full Copyright Statement

8.0 Expiration Date

This memo is filed as <draft-calhoun-diameter-impl-guide-05.txt> and expires in July 2001.