Network Working Group
Internet-Draft
Expires: December 29, 2003

P. Eronen, Ed.
Nokia
T. Hiller
Lucent Technologies
G. Zorn
Cisco Systems
June 30, 2003

Diameter Extensible Authentication Protocol (EAP) Application
draft-ietf-aaa-eap-02.txt

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 Internet-Draft will expire on December 29, 2003.

Copyright Notice

Abstract

The Extensible Authentication Protocol (EAP) provides a standard mechanism for support of various authentication methods. This document defines the Command-Codes and AVPs necessary to carry EAP packets between a Network Access Server (NAS) and a back-end authentication server.

Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",

"SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

Table of Contents

1. Introduction

The Extensible Authentication Protocol (EAP), defined in [RFC2284bis], is an authentication framework which supports multiple authentication mechanisms. EAP may be used on dedicated links as well as switched circuits, and wired as well as wireless links.

To date, EAP has been implemented with hosts and routers that connect via switched circuits or dial-up lines using PPP [RFC1661], IEEE 802 wired switches [IEEE-802.1X], and IEEE 802.11 wireless access points [IEEE-802.11i]. EAP has also been adopted for IPsec remote access in IKEv2 [IKEv2].

This document specifies the Diameter EAP application that carries EAP packets between a Network Access Server (NAS) working as an EAP Authenticator and a back-end authentication server. The Diameter EAP application is based on NASREQ and is intended for similar environments as NASREQ.

In Diameter EAP application, authentication occurs between the EAP client and its home Diameter server. This end-to-end authentication reduces the possibility for fraudulent authentication, such as replay and man-in-the-middle attacks. End-to-end authentication also provides a possibility for mutual authentication, which is not possible with PAP and CHAP in a roaming PPP environment.

Diameter EAP application relies heavily on [NASREQ], and in earlier drafts was part of the Diameter NASREQ application. It can also be used in conjunction with NASREQ, selecting the application based on the used authentication mechanism (EAP or PAP/CHAP). Diameter EAP application defines new Command-Codes and new AVPs, and can work together with RADIUS EAP support [RFC2869bis].

2. Extensible Authentication Protocol Support in Diameter

2.1 Advertising application support

Diameter nodes conforming to this specification MAY advertise support by including the value of TBD in the Auth-Application-Id AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer command [BASE].

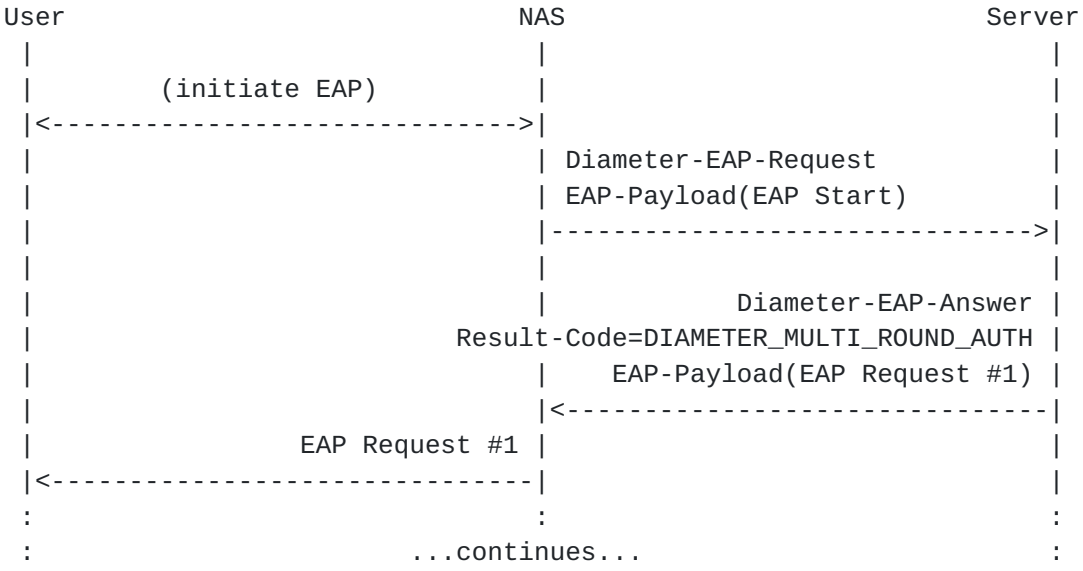
If the NAS receives a response with the Result-Code set to DIAMETER_APPLICATION_UNSUPPORTED [BASE], it is an indication that the Diameter server in the home realm does not support EAP. If possible, the access device MAY attempt to negotiate another authentication protocol, such as PAP or CHAP. An access device SHOULD be cautious when determining whether a less secure authentication protocol will

be used, since this could be a result of a bidding down attack (see Section 8.2.6).

2.2 Protocol Overview

The EAP conversation between the authenticating peer and the access device begins with the initiation of EAP within a link layer, such as PPP [RFC1661] or IEEE 802.1X [IEEE-802.1X]. Once EAP has been initiated, the access device will typically send to the Diameter server a Diameter-EAP-Request message with an empty EAP-Payload AVP, signifying an EAP-Start.

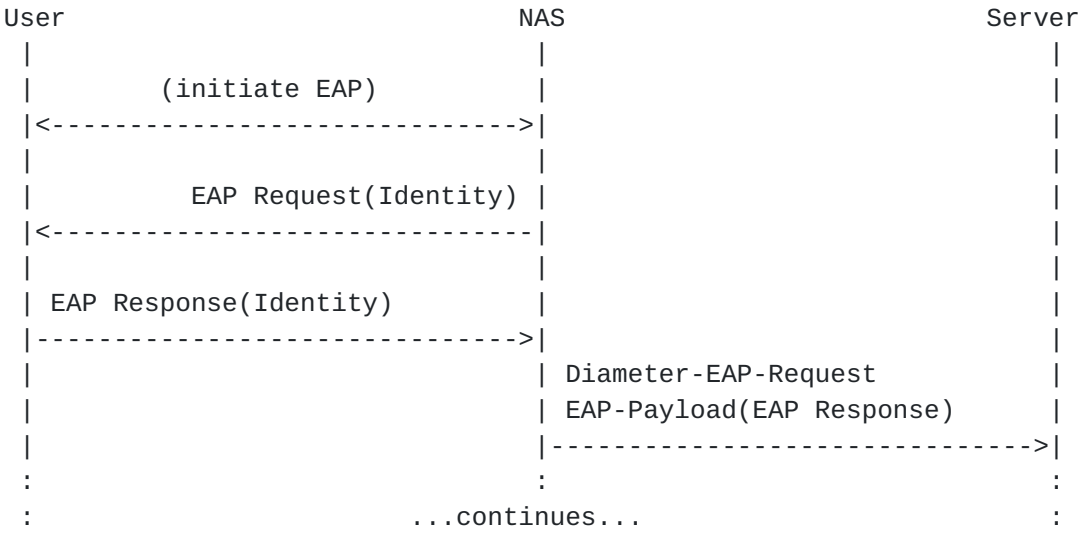
If the Diameter home server is willing to do EAP authentication, it respons with a Diameter-EAP-Answer message containing an EAP-Payload AVP that includes an encapsulated EAP packet. The Result-Code AVP set to DIAMETER_MULTI_ROUND_AUTH, signifying that a subsequent request is expected. The EAP payload is forwarded by the access device to the EAP client. This is illustrated in the diagram below.



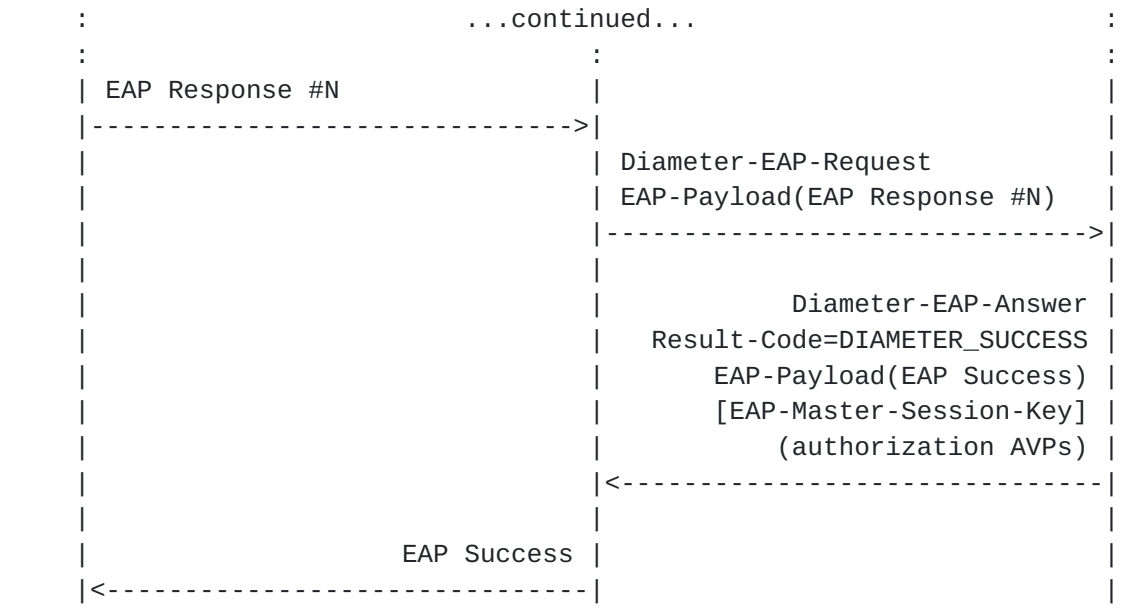
The initial Diameter-EAP-Answer in a multi-round exchange normally includes an EAP-Request/Identity, requesting the EAP client to identify itself. Upon receipt of the EAP client's EAP-Response, the access device will then issue a second Diameter-EAP-Request message, with the client's EAP payload encapsulated within the EAP-Payload AVP.

A preferred approach is for the access device to issue the EAP-Request/Identity message to the EAP client, and forward the EAP-Response/Identity packet, encapsulated within the EAP-Payload AVP, as a Diameter-EAP-Request to the Diameter server (see the diagram below). This alternative reduces the number of Diameter

message round trips. When the EAP-Request/Identity message is issued by the access device, it SHOULD interpret the EAP-Response/Identity packet returned by the authenticating peer, and copy its value to a User-Name AVP in Diameter-EAP-Request. This is useful in roaming environments, since the Destination-Realm is needed for routing purposes. Note that this alternative cannot be universally employed, as there are circumstances where a user's identity is not needed (such as when authorization occurs based on a calling or called phone number).



The conversation continues until the Diameter server sends a Diameter-EAP-Answer with a Result-Code AVP indicating success or failure, and an optional EAP-Payload. The Result-Code AVP is used by the access device to determine whether service is to be provided to the EAP client. The access device MUST NOT rely on the contents of the optional EAP-Payload to determine whether service is to be provided.



If authorization was requested, a Diameter-EAP-Answer with Result-Code set to DIAMETER_SUCCESS MUST also include the appropriate authorization AVPs required for the service requested (see Section 5 and [NASREQ]). If the Result-Code DIAMETER_LIMITED_SUCCESS is returned, this means that the NAS has to get additional authorization AVPs using a separate NASREQ request. This case is described in Section TBD below. Diameter-EAP-Answer messages whose Result-Code AVP is set to DIAMETER_MULTI_ROUND_AUTH MAY include authorization AVPs.

A Diameter-EAP-Answer with succesful Result-Code MAY also include an EAP-Master-Session-Key AVP that contains keying material for protecting the communication between the user and the NAS. Exactly how this keying material is used depends on the link layer in question, is beyond the scope of this document.

A home Diameter server MAY request EAP re-authentication by issuing the Re-Auth-Request [BASE] message to the Diameter client.

Should an EAP authentication session be interrupted due to a home server failure, the session MAY be directed to an alternate server, but the authentication session will have to be restarted from the beginning.

2.3 Sessions and NASREQ interaction

(NOTE: This section has not received sufficient WG discussion yet, and is likely to be changed in the future.)

The previous section introduced the basic protocol between the NAS

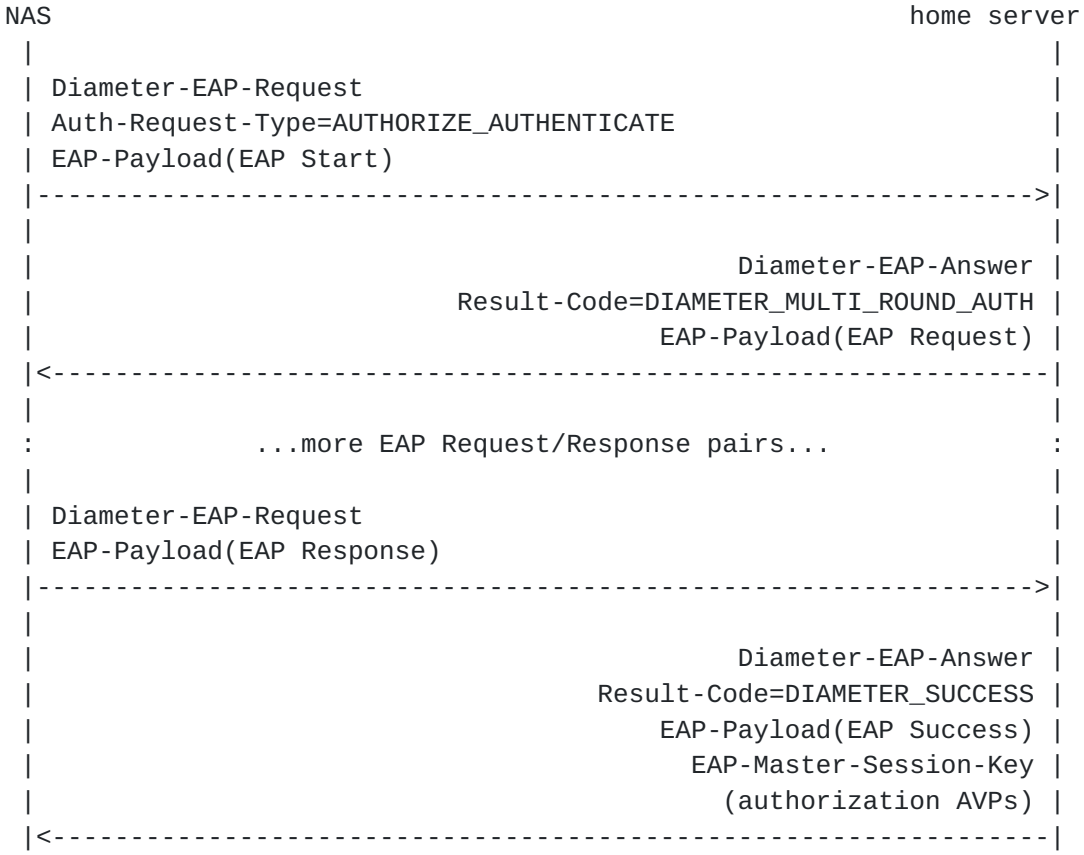
and the home server. Since the Diameter-EAP-Answer message may include a Master Session Key (MSK) for protecting the communication between the user and the NAS, care must be taken to ensure that this key does not fall into wrong hands.

Basic Diameter security mechanisms (IPsec and TLS) protect Diameter messages hop-by-hop. Since there are currently no end-to-end (NAS-to-home server) security mechanisms defined for Diameter, this section describes some possible scenarios how the messages could be transported protected using these hop-by-hop mechanisms.

The list of scenarios is not intended to be exhaustive, and it is possible to combine them. For instance, the first proxy agent after the NAS could use redirects as in scenario 2 to bypass any additional proxy agents.

2.3.1 Scenario 1: Direct connection

The simplest case is when the NAS contacts the home server directly. All the authorization AVPs are delivered by the home server, as is EAP keying material.

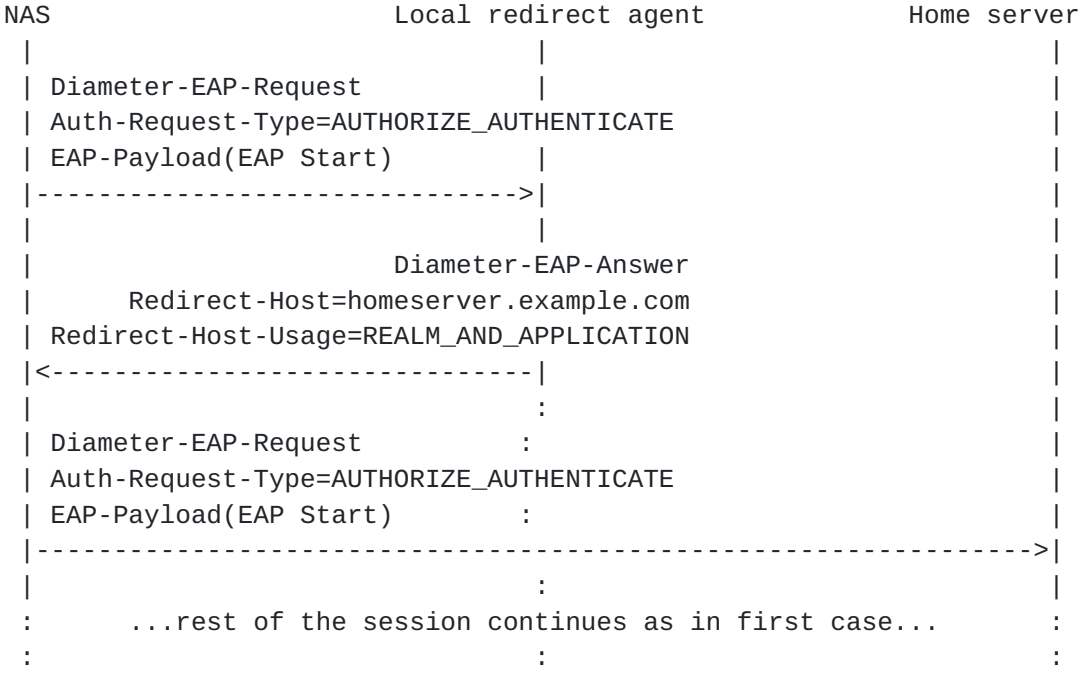


This scenario is the most likely to be used in small networks, or in

cases where Diameter agents are not needed to provide routing or additional authorization AVPs.

2.3.2 Scenario 2: Direct connection with redirects

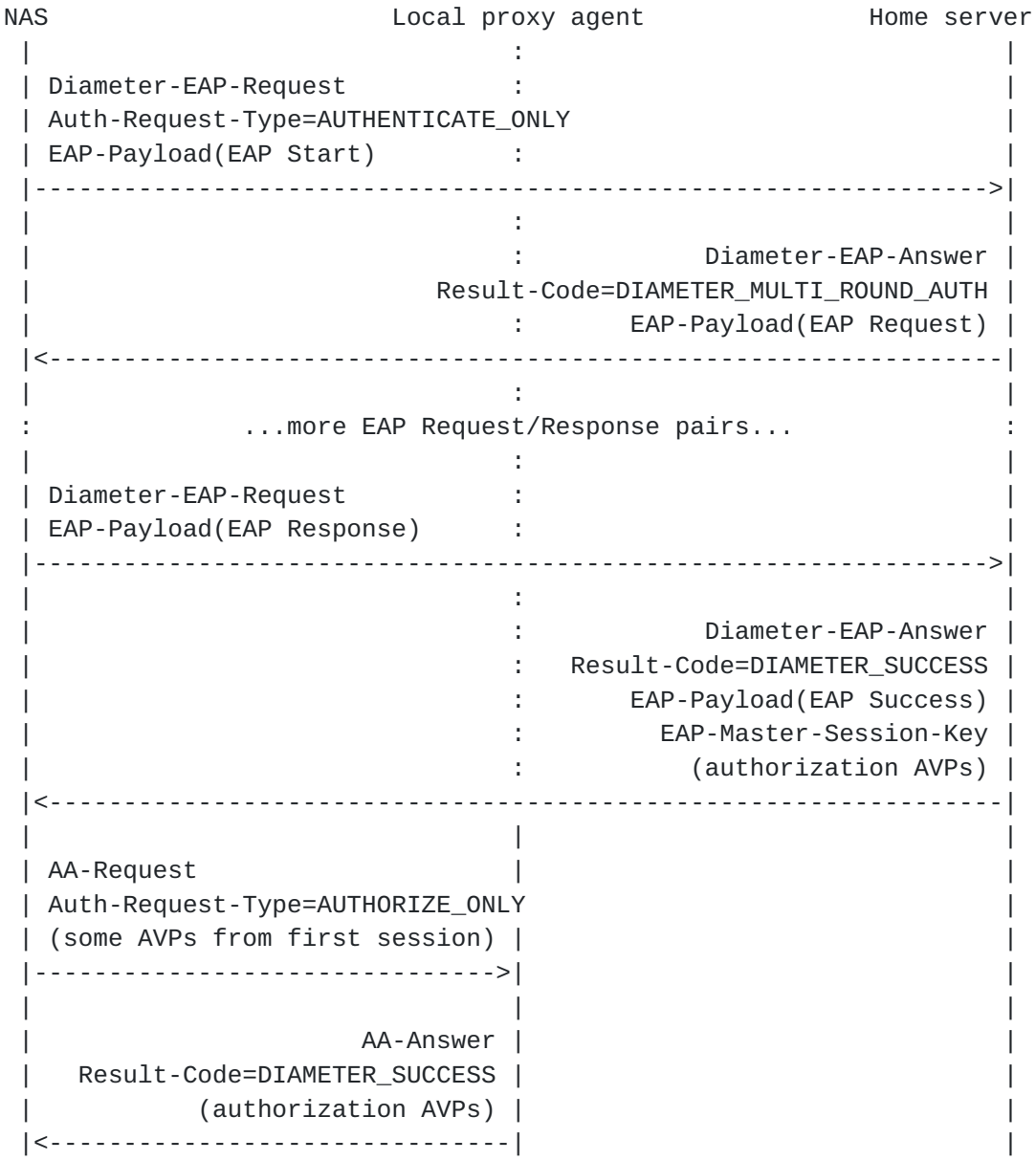
In this scenario the NAS uses a redirect agent to locate the home server, and the rest of the session proceeds as before.



The advantage of this scenario is that knowledge of realms and home servers is centralized to a redirect agent, and it is not necessary to modify the NAS configuration when, e.g., a new roaming agreement is done.

2.3.3 Scenario 3: Direct EAP, authorization via agents

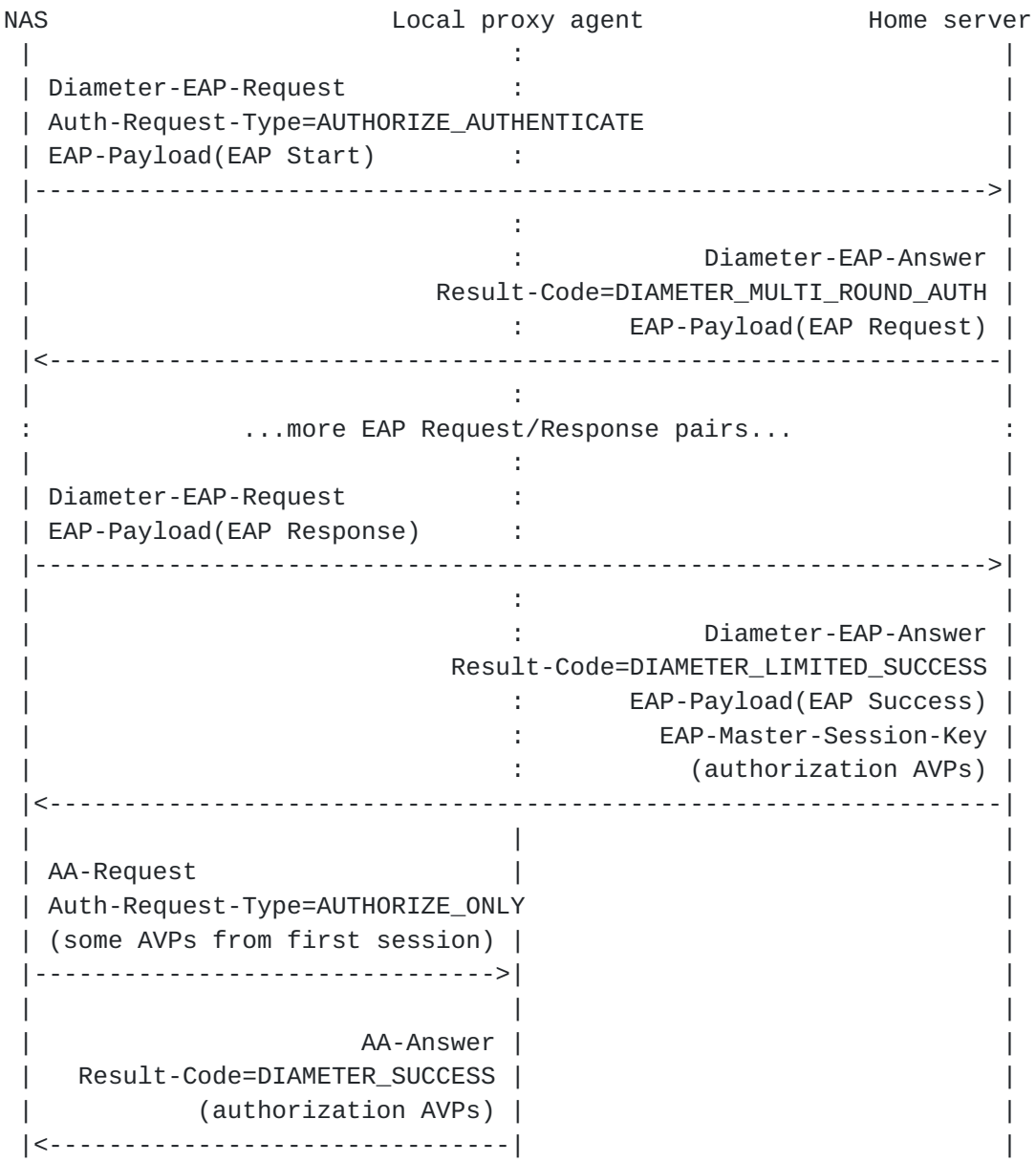
In this scenario the EAP authentication is done directly with the home server (with Auth-Request-Type set to AUTHENTICATE_ONLY), and the authorization AVPs are retrieved from the local proxy agents. This scenario is intended for environments where the home server cannot provide all the necessary authorization AVPs to the NAS.



The NASREQ application is used here for authorization because the realm-specific routing table does support routing based on application, but not more...TO BE CLARIFIED.

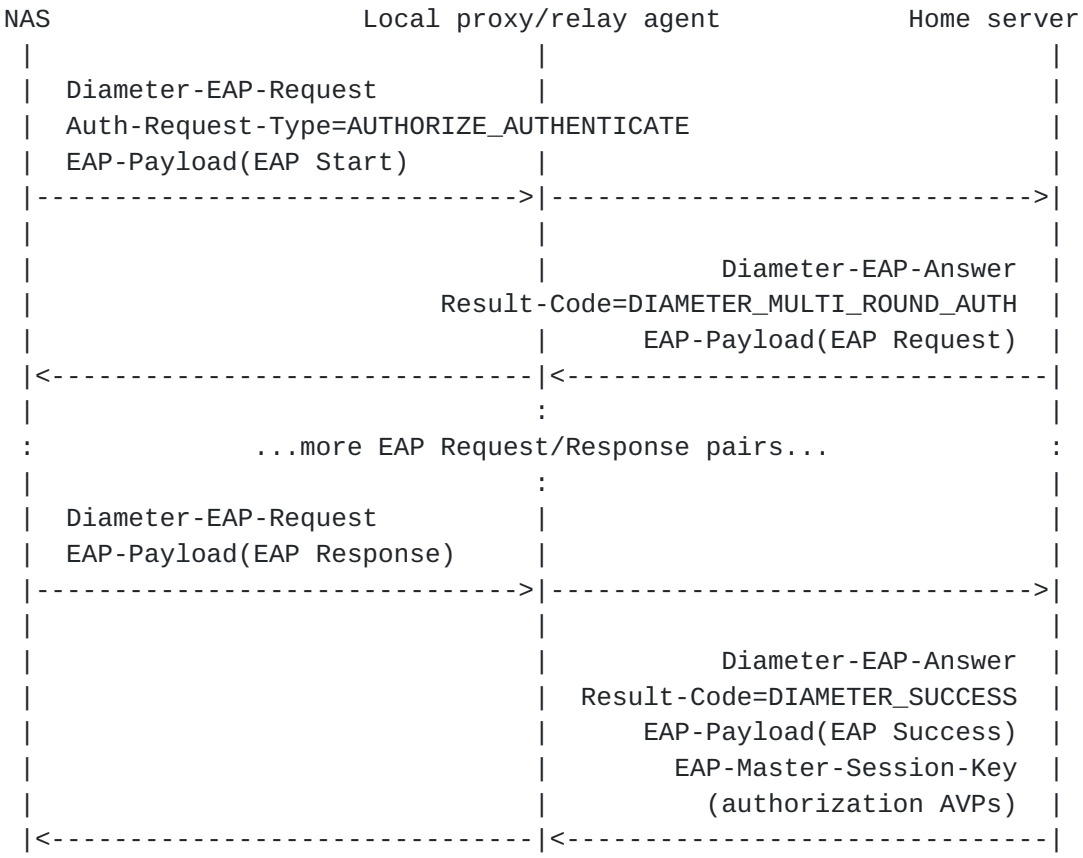
A second possibility is that the home server signals the NAS to

perform a separate authorization step. In this case, the NAS begins the Diameter EAP session with Auth-Request-Type=AUTHORIZE_AUTHENTICATE. The last Diameter-EAP-Answer from the home server contains Result-Code=DIAMETER_LIMITED_SUCCESS, so the NAS does additional AUTHORIZE_ONLY NASREQ step.



2.3.4 Scenario 4: Proxy agents

Same as scenario 1, but through proxies. Note that in this case the proxies can see the EAP session keys, so this is not suitable for environments where proxies can't be trusted for this.



2.4 Invalid packets

While acting as a pass-through, the NAS MUST validate the EAP header fields (Code, Identifier, Length) prior to forwarding an EAP packet to or from the Diameter server. On receiving an EAP packet from the peer, the NAS checks the Code (2) and Length fields, and matches the Identifier value against the current Identifier, supplied by the Diameter server in the most recently validated EAP Request. On receiving an EAP packet from the Diameter server (encapsulated within a Diameter-EAP-Answer), the NAS checks the Code (1) and Length fields, then updates the current Identifier value. Pending EAP Responses that do not match the current Identifier value are silently discarded by the NAS.

Since EAP method fields (Type, Type-Data) are typically not validated by a NAS operating as a pass-through, despite these checks it is

possible for a NAS to forward an invalid EAP packet to or from the Diameter server.

A Diameter server receiving an EAP-Payload AVP it does not understand SHOULD make the determination of whether the error is fatal or non-fatal based on the EAP Type. A Diameter server determining that a fatal error has occurred MUST send an a Diameter-EAP-Answer with a failure Result-Code and an EAP-Payload AVP encapsulating an EAP Failure packet. A Diameter server determining that a non-fatal error has occurred MUST send a Diameter-EAP-Answer with an EAP-Reissued-Payload AVP encapsulating the previous EAP Request sent by the server.

When receiving a Diameter-EAP-Answer with an EAP-Reissued-Payload AVP, the NAS SHOULD discard the EAP-Response packet most recently transmitted to the Diameter server and check whether additional EAP Response packets have been received matching the current Identifier value. If so, a new EAP Response packet, if available, MUST be sent to the Diameter server within an Diameter-EAP-Request. If no EAP Response packet is available, then the EAP Request encapsulated within the EAP-Reissued-Payload AVP is sent to the peer, and the retransmission timer is reset.

In order to provide protection against Denial of Service (DoS) attacks, it is advisable for the NAS to allocate a finite buffer for EAP packets received from the peer, and to discard packets according to an appropriate policy once that buffer has been exceeded. Also, the Diameter server is advised to permit only a modest number of invalid EAP packets within a single session, prior to terminating the session with TBD. By default a value of 5 invalid EAP packets is recommended.

2.5 Retransmission

As noted in [RFC2284bis], if an EAP packet is lost in transit between the authenticating peer and the NAS (or vice versa), the NAS will retransmit.

It may be necessary to adjust retransmission strategies and 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.

If a Multi-Round-Time-Out AVP [BASE] is present in an Diameter-EAP-Answer message that also contains an EAP-Payload AVP, that value is used to set the EAP retransmission timer for that EAP

Request, and that Request alone.

2.6 Fragmentation

Using the EAP-Payload AVP, it is possible for the Diameter server to encapsulate an EAP packet that is larger than the MTU on the link between the NAS and the peer. Since it is not possible for the Diameter server to use MTU discovery to ascertain the link MTU, an EAP-MTU attribute may be included in a Diameter-EAP-Request message so as to provide the Diameter server with this information.

A Diameter server having received an EAP-MTU attribute in a Diameter-EAP-Request message MUST NOT send any subsequent packet in this EAP conversation containing EAP-Payload attribute whose length exceeds the length specified by the EAP-MTU value.

2.7 Accounting

This document specifies one additional AVP for accounting messages. One or more Accounting-EAP-Auth-Method AVPs (see Section 4.1.5) MAY be included in Accounting-Request messages to indicate the EAP method(s) used to authenticate the user.

If the NAS has authenticated the user with a locally implemented EAP method, it knows the method used and SHOULD include it in an Accounting-EAP-Auth-Method AVP.

If the authentication was done using Diameter-EAP-Request/Answer messages, the Diameter server SHOULD include one more more Accounting-EAP-Auth-Method AVPs in Diameter-EAP-Answer packets with a successful result code. In this case, the NAS SHOULD include these AVPs in Accounting-Request messages.

2.8 Usage guidelines

2.8.1 User-Name AVP

Unless the access device interprets the EAP-Response/Identity packet returned by the authenticating peer, it will not have access to the user's identity. Furthermore, some EAP methods support identity protection where the user's real identity is not included in EAP-Response/Identity. Therefore, the Diameter Server SHOULD return the user's identity by inserting it in the User-Name AVP of subsequent Diameter-EAP-Answer packets. Without the user's identity, the Session-Id AVP MAY be used for accounting and billing, however operationally this could be very difficult to manage.

2.8.2 Conflicting AVPs

A Diameter-EAP-Answer message containing an EAP-Payload of type EAP-Success or EAP-Failure MUST NOT have the Result-Code AVP set to DIAMETER_MULTI_ROUND_AUTH. Also, the Result-Code SHOULD match the contained EAP packet (successful Result-Code if EAP-Success, and a failure Result-Code for EAP-Failure). TO BE WRITTEN: clarify this.

2.8.3 Displayable messages

The Reply-Message AVP [NASREQ] contains text which may be displayed to the user. Note that the NAS does not necessarily have any facility for actually sending these messages to the user. In any case, the NAS MUST NOT manufacture any EAP packets (such as EAP-Request/Notification) from Reply-Message AVPs.

2.8.4 Role reversal

Some environments where EAP is used, such as PPP, support peer-to-peer operation. That is, both parties act as authenticators and authenticatees at the same time, in two simultaneous and independent EAP conversations.

This specification is intended for communication between EAP (passthrough) authenticator and backend authentication server. A Diameter client MUST NOT send a Diameter-EAP-Request encapsulating an EAP Request packet, and a Diameter server receiving such packet MUST respond with a failure Result-Code..

2.8.5 Alternative Uses

Currently the conversation between the backend authentication 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 back-end authentication server instead.

In the case where Diameter-encapsulated EAP is used in a conversation between a Diameter server and a backend authentication server, the latter will typically return an Diameter-EAP-Answer/EAP-Payload/ EAP-Success message without inclusion of the expected authorization AVPs required in a successful response. This means that the Diameter

server MUST add these attributes prior to sending an Diameter-EAP-Answer/EAP-Payload/EAP-Success message to the access device.

3. Command-Codes

This section defines new Command-Code values that MUST be supported by all Diameter implementations conforming to this specification. The following Command Codes are defined in this section:

Command-Name	Abbrev.	Code	Reference
Diameter-EAP-Request	DER	268	3.1
Diameter-EAP-Answer	DEA	268	3.2

3.1 Diameter-EAP-Request (DER) Command

The Diameter-EAP-Request (DER) command, indicated by the Command-Code field set to 268 and the 'R' bit set in the Command Flags field, is sent by a Diameter client to a Diameter server and conveys an EAP-Response from the EAP client. The Diameter-EAP-Request MUST contain one EAP-Payload AVP, which contains the actual EAP payload. An EAP-Payload AVP with no data MAY be sent to the Diameter server to initiate an EAP authentication session.

The DER message MAY be the result of a multi-round authentication exchange, which occurs when the DEA is received with the Result-Code AVP set to DIAMETER_MULTI_ROUND_AUTH [BASE]. A subsequent DER message MUST include any State AVPs [NASREQ] that were present in the DEA. For re-authentication, it is recommended that the Identity request be skipped in order to reduce the number of authentication round trips. This is only possible when the user's identity is already known by the home Diameter server.

Message format

```
<Diameter-EAP-Request> ::= < Diameter Header: 268, REQ, PXY >
                           < Session-Id >
                           { Auth-Application-Id }
                           { Origin-Host }
                           { Origin-Realm }
                           { Destination-Realm }
                           { Auth-Request-Type }
                           [ NAS-Port ]
                           [ NAS-Port-Id ]
                           [ Origin-State-Id ]
                           [ Destination-Host ]
```

```
                                 [ NAS-Identifier ]
                                 [ NAS-IP-Address ]
                                 [ NAS-IPv6-Address ]
                                 [ NAS-Port-Type ]
                                 [ Port-Limit ]
                                 [ User-Name ]
                                 { EAP-Payload }
                                 { EAP-MTU }
                                 [ Service-Type ]
                                 [ Idle-Timeout ]
                                 [ State ]
                                 [ Authorization-Lifetime ]
                                 [ Auth-Grace-Period ]
                                 [ Auth-Session-State ]
                                 [ Session-Timeout ]
                                 [ Callback-Number ]
                                 [ Called-Station-Id ]
                                 [ Calling-Station-Id ]
                               * [ Class ]
                                 [ Originating-Line-Info ]
                                 [ Connect-Info ]
                               * [ Framed-Compression ]
                                 [ Framed-Interface-Id ]
                                 [ Framed-IP-Address ]
                               * [ Framed-IPv6-Prefix ]
                                 [ Framed-IP-Netmask ]
                                 [ Framed-MTU ]
                                 [ Framed-Protocol ]
                               * [ Tunneling ]
                               * [ Proxy-Info ]
                               * [ Route-Record ]
                               * [ AVP ]
```

3.2 Diameter-EAP-Answer (DEA) Command

The Diameter-EAP-Answer (DEA) message, indicated by the Command-Code field set to 268 and the 'R' bit cleared in the Command Flags field, is sent by the Diameter server to the client for one of the following reasons:

1. The message is part of a multi-round authentication exchange, and the server is expecting a subsequent Diameter-EAP-Request. This is indicated by setting the Result-Code to DIAMETER_MULTI_ROUND_AUTH, and MAY include zero or more State AVPs.

2. the EAP client has been successfully authenticated and

authorized, in which case the message MUST include the Result-Code AVP indicating success, and SHOULD include an EAP-Payload of type EAP-Success. This event MUST cause the access device to provide service to the EAP client.

3. The EAP client has not been successfully authenticated and/or authorized, and the Result-Code AVP is set to indicate failure. This message SHOULD include an EAP-Payload, but this AVP is not used to determine whether service is to be provided.

If the message from the Diameter client included a request for authorization, a successful response MUST include the authorization AVPs that are relevant to the service being provided.

Message format

```
<Diameter-EAP-Answer> ::= < Diameter Header: 268, PXY >
                          < Session-Id >
                          { Auth-Application-Id }
                          { Auth-Request-Type }
                          { Result-Code }
                          { Origin-Host }
                          { Origin-Realm }
                          [ User-Name ]
                          [ EAP-Payload ]
                          [ Multi-Round-Time-Out ]
                          [ Service-Type ]
                        * [ Class ]
                        * [ Configuration-Token ]
                          [ Acct-Interim-Interval ]
                          [ Error-Message ]
                          [ Error-Reporting-Host ]
                          [ Idle-Timeout ]
                          [ Authorization-Lifetime ]
                          [ Auth-Grace-Period ]
                          [ Auth-Session-State ]
                          [ Re-Auth-Request-Type ]
                          [ Session-Timeout ]
                          [ State ]
                        * [ Reply-Message ]
                          [ Termination-Action ]
                          [ Origin-State-Id ]
                        * [ Filter-Id ]
                          [ Port-Limit ]
                          [ Callback-Id ]
                          [ Callback-Number ]
                          [ Framed-Appletalk-Link ]
```

```
                    * [ Framed-Appletalk-Network ]
                      [ Framed-Appletalk-Zone ]
                    * [ Framed-Compression ]
                      [ Framed-Interface-Id ]
                      [ Framed-IP-Address ]
                    * [ Framed-IPv6-Prefix ]
                      [ Framed-IPv6-Pool ]
                    * [ Framed-IPv6-Route ]
                      [ Framed-IP-Netmask ]
                    * [ Framed-Route ]
                      [ Framed-Pool ]
                      [ Framed-IPX-Network ]
                      [ Framed-MTU ]
                      [ Framed-Protocol ]
                      [ Framed-Routing ]
                    * [ NAS-Filter-Rule ]
                    * [ Tunneling ]
                    * [ Redirect-Host ]
                      [ Redirect-Host-Usage ]
                      [ Redirect-Max-Cache-Time ]
                    * [ Proxy-Info ]
                    * [ AVP ]
```

4. Attribute-Value Pairs

This section both defines new AVPs, unique to the EAP Diameter application and describes the usage of AVPs defined elsewhere if that usage in the EAP application is noteworthy.

4.1 New AVPs

4.1.1 EAP-Payload AVP

The EAP-Payload AVP (AVP Code 402) is of type OctetString and is used to encapsulate the actual EAP packet that is being exchanged between the EAP client and the home Diameter server.

4.1.2 EAP-Reissued-Payload AVP

The EAP-Reissued-Payload AVP (AVP Code TBD) is of type OctetString. This AVP MAY be included in Diameter-EAP-Answer messages to signal the NAS that the EAP packet in it sent was not a satisfactory response (see Section 2.4 for discussion). To ease RADIUS translation, this AVP contains the previous EAP packet sent by the Diameter server.

4.1.3 EAP-MTU AVP

The EAP-MTU AVP (AVP Code TBD) is of type Unsigned32. Its use is described in Section 2.6.

4.1.4 EAP-Master-Session-Key AVP

The EAP-Master-Session-Key AVP (AVP Code TBD) is of type OctetString. It is used by the Diameter server...TBD

4.1.5 Accounting-EAP-Auth-Method AVP

The Accounting-EAP-Auth-Method AVP (AVP Code 401) is of type Unsigned64. In case of expanded types [RFC2284bis, Section 5.7], the least significant 32 bits contain the Vendor-Type field, and the next 24 bits contain the Vendor-Id field.

The use of this AVP is described in Section 2.7.

5. AVP Occurrence Tables

The following tables use these symbols:

0	The AVP MUST NOT be present in the message
0+	Zero or more instances of the AVP MAY be present in the message
0-1	Zero or one instance of the AVP MAY be present in the message
1	One instance of the AVP MUST be present in the message

Note that AVPs that can only be present within a Grouped AVP are not represented in these tables.

5.1 EAP Command AVP Table

The following table lists the AVPs that may be present in the DER and DEA Commands, defined in this document; however, the AVPs listed are defined both here and in [NASREQ].

	Command-Code	
Attribute Name	DER	DEA
Accounting-EAP-Auth-Method	0	0+
Acct-Interim-Interval [BASE]	0	0-1
Auth-Application-Id [BASE]	1	1
Auth-Grace-Period [BASE]	0-1	0-1

Auth-Request-Type [BASE]	1	1
Auth-Session-State [BASE]	0-1	0-1
Authorization-Lifetime [BASE]	0-1	0-1
Callback-Id [NASREQ]	0	0-1
Callback-Number [NASREQ]	0-1	0-1
Called-Station-Id [NASREQ]	0-1	0
Calling-Station-Id [NASREQ]	0-1	0
Class [BASE]	0+	0+
Configuration-Token [NASREQ]	0	0+
Connect-Info [NASREQ]	0-1	0
Destination-Host [BASE]	0-1	0
Destination-Realm [BASE]	1	0
EAP-Payload	1	0-1
EAP-MTU	0-1	0
Error-Message [BASE]	0	0-1
Error-Reporting-Host [BASE]	0	0-1
Failed-AVP [BASE]	0+	0+
Filter-Id [NASREQ]	0	0+
Framed-Appletalk-Link [NASREQ]	0	0-1
Framed-Appletalk-Network [NASREQ]	0	0+
Framed-Appletalk-Zone [NASREQ]	0	0-1
Framed-Compression [NASREQ]	0+	0+
Framed-Interface-Id [NASREQ]	0-1	0-1
Framed-IP-Address [NASREQ]	0-1	0-1
Framed-IP-Netmask [NASREQ]	0-1	0-1
Framed-IPv6-Prefix [NASREQ]	0+	0+
Framed-IPv6-Pool [NASREQ]	0	0-1
Framed-IPv6-Route [NASREQ]	0	0+
Framed-IPX-Network [NASREQ]	0	0-1
Framed-MTU [NASREQ]	0-1	0-1
Framed-Pool [NASREQ]	0	0-1
Framed-Protocol [NASREQ]	0-1	0-1
Framed-Route [NASREQ]	0	0+
Framed-Routing [NASREQ]	0	0-1
Idle-Timeout [NASREQ]	0-1	0-1
Multi-Round-Time-Out [BASE]	0	0-1
NAS-Filter-Rule [NASREQ]	0	0+
NAS-Identifier [NASREQ]	0-1	0
NAS-IP-Address [NASREQ]	0-1	0
NAS-IPv6-Address [NASREQ]	0-1	0
NAS-Port [NASREQ]	0-1	0
NAS-Port-Id [NASREQ]	0-1	0
NAS-Port-Type [NASREQ]	0-1	0
NAS-Session-Key [NASREQ]	0	0+
Originating-Line-Info [NASREQ]	0-1	0
Origin-Host [BASE]	1	1
Origin-Realm [BASE]	1	1
Origin-State-Id [BASE]	0-1	0-1

Port-Limit [NASREQ]	0-1	0-1
Proxy-Info [BASE]	0+	0+
Re-Auth-Request-Type [BASE]	0	0-1
Redirect-Host [BASE]	0	0+
Redirect-Host-Usage [BASE]	0	0-1
Redirect-Max-Cache-Time [BASE]	0	0-1
Reply-Message [NASREQ]	0	0+
Result-Code [BASE]	0	1
Route-Record [BASE]	0+	0
Service-Type [NASREQ]	0-1	0-1
Session-Id [BASE]	1	1
Session-Timeout [BASE]	0-1	0-1
State [NASREQ]	0-1	0-1
Termination-Action [NASREQ]	0	0-1
Termination-Cause [BASE]	0	0-1
Tunneling [NASREQ]	0+	0+
User-Name [BASE]	0-1	0-1

5.2 Accounting AVP Table

The table in this section is used to represent which AVPs defined in this document are to be present in the Accounting messages, defined in [BASE].

	Command Code	
Attribute Name	ACR	ACA
Accounting-EAP-Auth-Method	0+	0

6. RADIUS/Diameter interactions

Section 9 of [NASREQ] describes basic guidelines that translation agents may follow when translating between RADIUS and Diameter protocols. This section gives additional guidelines for the Diameter EAP application. Note that this document does not restrict implementations from creating additional methods, as long as the translation function doesn't violate the RADIUS or the Diameter protocols.

6.1 RADIUS Request forwarded as Diameter Request

RADIUS Access-Request to Diameter-EAP-Request:

- RADIUS EAP-Message attribute(s) are translated to a Diameter EAP-Payload AVP. If multiple RADIUS EAP-Message attributes are present, they are concatenated and translated to a single Diameter EAP-Payload AVP.

- An empty RADIUS EAP-Message attribute (with length 2) signifies EAP-Start, and it is translated to an empty EAP-Payload AVP.

- If the RADIUS Framed-MTU attribute is present, it is translated to the Diameter EAP-MTU AVP.

Diameter-EAP-Answer to RADIUS Access-Accept/Reject/Challenge:

- Diameter EAP-Payload AVP is translated to RADIUS EAP-Message attribute(s). If necessary, the value is split into multiple RADIUS EAP-Message attributes.

- Diameter EAP-Reissued-Payload AVP is translated to a message that contains RADIUS EAP-Message attribute(s), and a RADIUS Error-Cause attribute [DynAuth] with value 202 (decimal), "Invalid EAP Packet (Ignored)" [RFC2869bis].

- As described in [NASREQ], if the Result-Code AVP set to DIAMETER_MULTI_ROUND_AUTH and the Multi-Round-Time-Out AVP is present, it is translated to the RADIUS Session-Timeout attribute.

- Diameter EAP-Master-Session-Key AVP can be translated to the vendor-specific RADIUS MS-MPPE-Recv-Key and MS-MPPE-Send-Key attributes [RFC2548]. The first up to 32 octets of the key is stored into MS-MPPE-Recv-Key, and the next up to 32 octets (if present) are stored into MS-MPPE-Send-Key.

- Diameter Accounting-EAP-Auth-Method AVPs, if present, are discarded.

6.2 Diameter Request forwarded as RADIUS Request

Diameter-EAP-Request to RADIUS Access-Request:

- The Diameter EAP-Payload AVP is translated to RADIUS EAP-Message attribute(s).

- An empty Diameter EAP-Payload AVP signifies EAP-Start, and it is translated to an empty RADIUS EAP-Message attribute.

- If the Diameter EAP-MTU AVP is present, it is translated to the RADIUS Framed-MTU attribute. If both an EAP-MTU AVP and a

Framed-MTU AVP are present in the Diameter-EAP-Request, the Framed-MTU AVP is discarded.

- The type (or expanded type) field from the EAP-Payload AVP can be saved either in a local state table, or encoded in a RADIUS Proxy-State attribute. This information is needed to construct an Accounting-EAP-Auth-Method AVP for the answer message (see below).

RADIUS Access-Accept/Reject/Challenge to Diameter-EAP-Answer:

- If the RADIUS Access-Challenge message does not contain an Error-Cause attribute [DynAuth] with value 202 (decimal), "Invalid EAP Packet (Ignored)" [RFC2869bis], any RADIUS EAP-Message attributes are translated to a Diameter EAP-Payload AVP, concatenating them if multiple attributes are present.

- If the Error-Cause attribute with value 202 is present, any RADIUS EAP-Message attributes are translated to a Diameter EAP-Reissued-Payload AVP, concatenating them if multiple attributes are present.

- As described in [NASREQ], if the Session-Timeout attribute is present in a RADIUS Access-Challenge message, it is translated to the Diameter Multi-Round-Time-Out AVP.

- If the vendor-specific RADIUS MS-MPPE-Recv-Key and/or MS-MPPE-Send-Key attributes [RFC2548] are present, they can be translated to a Diameter EAP-Master-Session-Key AVP. Their values are concatenated (MS-MPPE-Recv-Key first, MS-MPPE-Send-Key next), and the concatenated value is stored into a Diameter EAP-Master-Session-Key AVP.

- If the Diameter-EAP-Answer will have a succesful result code, the saved state (see above) can be used to construct an Accounting-EAP-Auth-Method AVP.

6.3 Accounting Requests

In Accounting-Requests, the vendor-specific RADIUS MS-Acct-EAP-Type attribute [RFC2548] can be translated to a Diameter Accounting-EAP-Auth-Method AVP, and vice versa.

When translating from Diameter to RADIUS, note that the MS-Acct-EAP-Type attribute does not support expanded EAP types. Type values greater than 255 should be translated to type 254.

7. IANA Considerations

This document does not create any new namespaces to be maintained by IANA, but it defines new values in namespaces that have been defined in the Diameter Base protocol [BASE].

- This specification assigns the value 268 from the Command Code namespace defined in [BASE]. See Section 3 for more information.
- This specification assigns the values TBD from the AVP Code namespace defined in [BASE]. See Section 4.1 for the assignment of the namespace in this specification.
- This specification assigns the value TBD from the Application Identifier namespace defined in [BASE]. See Section TBD above for more information.

8. Security Considerations

(NOTE: This section is still very much under construction, and will be revised in later versions. Comments are welcome!)

Diameter peer-to-peer connections can be protected with IPsec or TLS. These mechanisms are believed to provide sufficient protection under the normal Internet threat model--that is, assuming the authorized nodes engaging in the protocol have not been compromised, but the attacker has complete control over the communication channels between them. This includes eavesdropping, message modification, insertion, man-in-the-middle and replay attacks. The details and related security considerations are discussed in [BASE].

The rest of this section deals with two important topics that are not completely covered by [BASE] and [NASREQ]: authorization and attacks by compromised nodes.

Authorization here means the act of determining if a Diameter message received from an authenticated Diameter peer should be accepted (and not authorization of users requesting network access from a NAS). The Diameter base protocol gives only overall guidelines and does not specify any particular mechanisms, and neither does this document. However, Section 8.1 gives some examples of possible authorization mechanisms to illustrate the importance of proper authorization, and to provide concrete examples for discussing authorization-related security considerations (it might be useful to place some of this text in a separate "Diameter authentication and authorization" document--if you're interested in writing that, contact the authors).

The last part of this section deals with attacks by nodes that have been properly authorized (to function as a NAS, Diameter agent, or Diameter server) but have been compromised. In general, it is not possible to completely protect against attacks by compromised nodes, but this section offers some advice that can be used to limit the extent of the damage.

Note that much of the discussion in this section is not really specific to Diameter EAP application, but applies to many other Diameter applications as well.

8.1 Authorization

When two Diameter nodes communicate, they can authenticate each other using IPsec or TLS. However, just authentication is not enough--authorization is also needed. Authorization tries to answer questions such as the following.

- When a Diameter server receives a Diameter-EAP-Request, is the node that sent it authorized to act as a NAS for the specific user, service type, and so on, in question?
- Correspondingly, when the NAS contacts the server to send the Diameter-EAP-Request, is the server is authorized to act as home server for the realm in question?
- Similar considerations apply to Accounting-Request/Answer messages: Is the NAS authorized to send this accounting request?, Is the server authorized to act as an accounting server for this session?
- In Re-Auth-Request and Abort-Session-Request, the command is initiated by the server, but similar considerations apply.
- Session-Termination-Request/Answer (TBW)
- Hop-by-hop messages (Capabilities-Exchange-Request/Answer, Device-Watchdog-Request/Answer, Disconnect-Peer-Request/Answer) are not discussed in this section.

Authorization is often left as an implementation issue, and this is indeed a reasonable approach when authorization is based on local access control lists (ACLs). In this case, other nodes do not need to know how ACLs are specified or implemented. It is also possible to implement complex authorization conditions (for instance, "ap1788.example.com is authorized to act as a WLAN access point for users whose name does not contain the letter "a", but only between 8AM and 4PM", to give a rather unlikely example).

However, when authorization can't be based solely on local ACLs, the issue becomes significantly more complex. First, interoperability between different vendors requires public specifications, and authorization can't be left solely as an "implementation issue" anymore. Second, these specifications are likely to support only very simple authorizations (such as "authorized to act as Diameter client"), instead of arbitrarily complex rules like the nonsense example given above.

The authorization requirements also depend on many issues, such as the size of the network, the trust relationships between the nodes, and the Diameter application and commands in question.

8.1.1 Direct connection, NAS point of view

Let's first consider the case where the NAS contacts the home server directly. There are two somewhat different subcases, depending on how the NAS finds the home server.

In the simplest case, the NAS has all the home servers statically configured in its peer table and realm-based routing table (see [BASE], Sections 2.6 and 2.7). This is likely to occur small networks. Authentication can be based either on certificates or pre-shared keys.

In this case authorization is most likely based on the realm-based routing table (that can be considered to contain an "implicit" local ACL). To give a concrete example, if "mars.example.com" is configured as the server for realm "example.com", this can be considered to imply that mars.example.com is authorized to act as the home server for that realm.

The situation is a bit different if the NAS finds the home server using, for instance, DNS queries or redirect messages. In this case, authentication is probably based on certificates, but how does a NAS know if the server authenticated as "mars.example.com" is authorized to act as the home server for the realm "example.com"? A couple of possibilities follow:

- "Server CA": A certificate issued by some particular Certificate Authority (CA) implies authorization to act as the home server (for all realms). This provides rather coarse-grained authorization, and has obvious problems if the same CA also issues certificates for other purposes (such as NASes or web servers).

- Certificate name matching: The NAS requires a certificate issued by some particular CA, and also compares the DNS name in the certificate with the realm name. Like the previous approach,

there are problems if the same CA issues certificates for other purposes. There are several possibile comparison rules (these examples are not meant to be exhaustive):

* "Simple": the server is authorized if the realm name is equal to the DNS name in the certificate with first component removed.

* "Suffix": the server is authorized if the realm name is a suffix of the DNS name in the certificate.

* "Last-2-or-3": the server is authorized if the last two or three components of the DNS name and realm name are equal. Whether two or three components are required depends on the last component. For instance, two is enough for "com", but three is required for "au", because Australia uses a second-level domain structure (.com.au, .org.au, etc.).

All of these comparison rules have some problems. For instance, using the "simple" rule, mars.example.com can't be authorized for the realm "sales.example.com". With the "suffix" and "last-2-or-3" rules, "jupiter.sales.example.com" is authorized for not only the realm "sales.example.com" but also "example.com". And none of the rules can authorize mars.example.com for the realm "example.org".

o Authorization using DNS records (probably secured by DNSSEC): For instance, a DNS SRV record "_diameter._sctp.example.com" pointing to mars.example.com could imply authorization to act as a home server for the realm "example.com" (although [BASE], Section 5.2 seems to forbid this).

o Authorization implied by redirect: If the home server was located as a result of a redirect message, and the redirect agent that provided the answer is trustworthy, this could be used as authorization if better information is not available (see also next section about authorizing redirect agents).

Some future possibilities (not known to be used yet in Diameter) include the following.

o Certificate name matching combined with an extendedKeyUsage extension, specifying whether the host is authorized to act as a home server, NAS, or something else (such as web server). This avoids the problems involved if the same CA issues certificates for other purposes as well, but no extendedKeyUsage value has been defined for Diameter servers yet.

- The server's certificate could contain an authorization extension with realm name(s). This would avoid many of the problems in certificate name matching, but no such extensions has been defined yet.

- Attribute certificates: The server also presents an attribute certificate that contains the realm name. No attribute certificate profile has been defined for Diameter, and there is no standardized way to transport the attribute certificates with IKE or TLS.

For reasons described in the next section (Attacks by compromised nodes), a NAS may also perform more fine-grained access control. For instance, a NAS may want to restrict the ability to initiate callback to some home servers. How such restricted authorizations would be specified is beyond the scope of this document.

8.1.2 Direct connection, server point of view

(TO BE WRITTEN)

8.1.3 Diameter agents

(NOTE: This section is very much under construction)

If authorization can be complex even in the case of direct connections, it gets worse with agents, unless authorization is made more "coarse-grained". Consider questions such "is this Diameter proxy authorized to forward my requests to realm example.com?", or "is this Diameter proxy authorized to forward requests from NAS ap1788.example.com?"

It is important to remember that authorizing a Diameter agent to work as a relay, proxy or translation agent involves considerable trust in the agent. The security mechanisms specified in [BASE] provide only hop-by-hop security. Diameter agents can eavesdrop and modify AVPs in the messages they forward, and even with Diameter Path Authorization (see [BASE] Section 2.10), a Diameter agent that is authorized to forward messages from party X can also forge messages that look like they came from X.

Some Diameter agent may be authorized as a redirect agent only (TO BE WRITTEN)

8.2 Attacks by compromised nodes

The hop-by-hop security mechanisms (IPsec and TLS) combined with proper authorization provide good protection against "outside"

attackers (denial-of-service is, of course, possible). This section deals with attacks in which an attacker has compromised an authorized NAS, Diameter agent, or Diameter server.

(Attacks between the user and the NAS are beyond the scope of this document, since they do not use Diameter, and depend on the link layer used.)

Unlike the base protocol security considerations, this section considers the Diameter NASREQ/EAP messages not just as bit strings, but as messages with a meaning (that cause some actions to happen). Thus, the question is not "can the attacker modify this packet" but "what can an attacker who compromises an authorized NAS, agent, or server do using Diameter EAP messages?"

8.2.1 Impersonating as the user (NAS, agents)

Unlike CHAP in NASREQ, in EAP the NAS or agents cannot successfully replay old EAP messages (unless the EAP method is seriously broken).

8.2.2 Impersonating as the network (NAS, agents)

If the EAP method used does not provide mutual authentication, obviously anyone can impersonate as the network to the user. When EAP mutual authentication is used, it occurs between the user and the Diameter home server. This means that it is usually not possible for the user to validate the identity of the NAS using EAP alone (the possession of the session keys by the NAS proves that the user is talking to *some* authorized NAS, but not which).

Some EAP methods, such as EAP Archie [Archie], try to provide a "binding" where some identity of the NAS (such as MAC address) is also communicated inside the EAP messages. However, the usefulness of this binding is rather limited in many environments.

In many networks an attacker who has not compromized any trusted nodes can still mount a "relay attack" (for the lack of better word). In this attack, the attacker just forwards messages between the user and a legitimate NAS (without modifying them), causing the user to access the network via a different NAS than would have otherwise happened. This attack might make sense if, for instance, the attacker can eavesdrop the network near some NASes, but not all, or if the user is charged more for network access via foreign NASes than local ones.

It is rather obvious that an attacker who has compromised a NAS can "impersonate" as the network to the user (until the compromise is noticed and NAS authorization revoked). The attacker can also use

this "relay attack" to cause the user to access the network via the compromised NAS instead of other, non-compromised, NASes.

Prevention of this "relay attack" is rather difficult, and is beyond the scope of this document. Note that validating a NAS identity (using the "binding" provided by Archie, for instance) does not usually help. For instance, in WLANs, the user does not usually securely know the MAC address of the "right" access point--it's simply picked from a beacon message that has the correct SSID and good signal strength (something that's easy to spoof).

8.2.3 Privacy issues (NAS, agents)

Diameter messages can contain AVPs that can be used to identify the user (e.g., User-Name) and approximate location of the user (e.g. Origin-Host for WLAN access points, Calling-Station-Id for fixed phone lines). Thus, any Diameter nodes that process the messages may be able to determine the geographic location of users.

Note that in many cases, the user identity is also sent in clear inside EAP-Payload AVPs, and it may be possible to eavesdrop this between the user and the NAS.

This can mitigated somewhat by using EAP methods that provide identity protection (see [RFC2284bis], Section 7.3), and using Session-Id or pseudonyms for accounting.

8.2.4 Offline cryptographic attacks (NAS, agents)

Some EAP methods are vulnerable to dictionary attacks or other methods that try to recover long-term secrets from EAP messages. Usually the EAP messages can also be eavesdropped between the user and the NAS, so good EAP methods provide sufficient protection against this type of attacks.

8.2.5 AVP editing (NAS, agents, server)

Diameter agents can modify, insert, and delete AVPs. Diameter agents are usually meant to modify AVPs, and the protocol in general cannot distinguish well-intentioned and malicious modifications (see [RFC2607] for more discussion).

Authentication method negotiation attacks are discussed in the next Section.

An attacker who compromises a Diameter agent or server can modify AA-Answer/Diameter-EAP-Answer messages and..

- Deny access to authorized users (Result-Code).
- Give unauthorized users access (Result-Code).
- Give attacker a login session to a host otherwise protected by firewalls (Login-Host).
- Redirect an authorized user's login session to a host controlled by the attacker (Login-Host).
- Route an authorized user's traffic through a host controlled by the attacker (various tunneling AVPs).
- Redirect an authorized user's DNS requests to a malicious DNS server (various vendor-specific AVPs).
- Modify routing tables at the NAS and thus redirect packets destined for someone else (Framed-Route, Framed-Routing).
- Remove packet filters and other restrictions for user (Filter, Callback, various vendor-specific AVPs).
- Cause the NAS to call some number, possibly expensive toll number controlled by the attacker (callback AVPs)
- Execute Command Line Interface (CLI) commands on the NAS (various vendor-specific attributes).

Some of these attacks can be prevented if the NAS can be configured not to accept some particular AVPs, or not accept them from all Diameter servers. For instance, if a particular destination realm never uses tunneling, answer messages containing tunneling AVPs could be rejected.

An attacker who compromises a NAS or agent can modify AA-Requests, and...

- Change NAS-Identifier/NAS-Port/Origin-Host (or something) so that a valid user appears to be accessing the network from a different NAS than in reality.
- Modify Calling-Station-ID (either to hide the true value, gain access, or frame someone else).
- Modify password change messages (some vendor-specific attributes)
- Modify usage information in accounting messages.

- Modify Class/State AVPs?

8.2.6 Negotiation attacks (NAS, agents, server)

This section deals with attacks where the NAS, any Diameter agents, or Diameter server attempts to cause the authenticating user to choose a less secure authentication method (either something else than EAP, or a less secure EAP method).

For example, a session that would normally be authenticated with EAP would instead authenticated via CHAP or PAP; alternatively, a connection that would normally be authenticated via a more secure EAP method such as EAP-TLS might be made to occur via a less secure EAP method, such as MD5-Challenge.

(TO BE WRITTEN, possibly copy text from 2869bis)

Negotiation attacks within EAP are discussed in [RFC2284bis], Section 7.8.

Negotiation attacks between the user and the NAS are beyond the scope of this document.

8.2.7 Session key distribution (agents, server)

Since there are currently no end-to-end (NAS-to-home server) security mechanisms specified for Diameter, any agents that process Diameter-EAP-Answer messages can see the contents of the EAP-Session-Key AVP. For this reason, this specification strongly recommends avoiding Diameter agents when they cannot be trusted to keep the keys secret.

In environments where agents are present, several factors should be considered when deciding whether the agents that are authorized (and considered "trustworthy enough") to grant access to users and specify various authorization and tunneling AVPs are also "trustworthy enough" to handle the session keys. These factors include (but are not limited to) the type of access provided (e.g., public Internet or corporate internet), security level of the agents, and the possibilities for attacking user's traffic after it has been decrypted by the NAS.

Note that the keys communicated in Diameter messages are usually short-term session keys (or short-term master keys that are used to derive session keys). To actually cause any damage, those session keys must end with some malicious party; that party must be able to eavesdrop, modify, or insert traffic between the user and the NAS

during the lifetime of those keys (e.g., in 802.11i the attacker must also eavesdrop the "four-way handshake"); and that eavesdropping or modification must cause some damage.

9. Acknowledgements

This Diameter application relies heavily on earlier work on Diameter NASREQ application [NASREQ] and RADIUS EAP support [RFC2869bis]. Much of the material in this specification has been copied from these documents.

The authors would also like to acknowledge the following people for their contributions to this document: Bernard Aboba, Jari Arkko, Pat Calhoun, Henry Haverinen, and John Loughney. (TBD: Who's missing from this list?)

Normative References

[BASE] Calhoun, P., Loughney, J., Guttman, E., Zorn, G. and J. Arkko, "Diameter Base Protocol", draft-ietf-aaa-diameter-17 (work in progress), December 2002.

[NASREQ] Calhoun, P., Zorn, G., Spence, D. and D. Mitton, "Diameter Network Access Server Application", draft-ietf-aaa-diameter-nasreq-11 (work in progress), February 2003.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2284bis] Blunk, L., Vollbrecht, J., Aboba, B., Carlson, J. and H. Levkowetz, "Extensible Authentication Protocol (EAP)", draft-ietf-eap-rfc2284bis-04 (work in progress), June 2003.

Informative References

[Archie] Walker, J. and R. Housley, "The EAP Archie Protocol", draft-jwalker-eap-archie-01 (work in progress), June 2003.

[DynAuth] Chiba, M., Dommety, G., Eklund, M., Mitton, D. and B. Aboba, "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", draft-chiba-radius-dynamic-authorization-20 (work in progress), May 2003.

[IEEE-802.1X]
Institute of Electrical and Electronics Engineers, "Local and Metropolitan Area Networks: Port-Based Network Access Control", IEEE Standard 802.1X, September 2001.

[IEEE-802.11i]
Institute of Electrical and Electronics Engineers, "Unapproved Draft Supplement to Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security", IEEE Draft 802.11i (work in progress), 2003.

[IKEv2] Kaufman, C., Ed., "Internet Key Exchange (IKEv2) Protocol", draft-ietf-ipsec-ikev2-08 (work in progress), May 2003.

[RADIUS1X]
Congdon, P., Aboba, B., Smith, A., Zorn, G. and J. Roese, "IEEE 802.1X RADIUS Usage Guidelines", draft-congdon-radius-8021x-29 (work in progress), April 2003.

[RFC1661] Simpson, W., "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994.

[RFC2548] Zorn, G., "Microsoft Vendor-specific RADIUS Attributes", RFC 2548, March 1999.

[RFC2607] Aboba, B. and J. Vollbrecht, "Proxy Chaining and Policy Implementation in Roaming", RFC 2607, June 1999.

[RFC2869bis]
Aboba, B. and P. Calhoun, "RADIUS Support For Extensible Authentication Protocol (EAP)", draft-aboba-radius-rfc2869bis-22 (work in progress), May 2003.

Authors' Addresses

Pasi Eronen (editor)
Nokia Research Center
P.O. Box 407
FIN-00045 Nokia Group
Finland

EMail: pasi.eronen@nokia.com

Tom Hiller
Lucent Technologies
1960 Lucent Lane
Naperville, IL 60566
USA

Phone: +1 630 979 7673
EMail: tom.hiller@lucent.com

Glen Zorn
Cisco Systems
500 108th Avenue N.E., Suite 500
Bellevue, WA 98004
USA

Phone: +1 425 344 8113
EMail: gwz@cisco.com

Appendix A. Changelog

(This section will not appear in the final version submitted to RFC editor.)

Changes from -02.d to -02.e:

- Added a section on accounting, and changed how the Accounting-EAP-Auth-Method is determined.
- Updates to "authorization" and "impersonating as the network" security considerations.

Changes from -02.c to -02.d:

- Some clarifications to Introduction section.
- Lots of clarifications and added diagrams in protocol overview

section. Moved non-EAP-supporting servers, User-Name AVP guidelines, and conflicting messages to separate sections.

- Added a new section about sessions and NASREQ interaction.
- Wrote a note about Reply-Message AVP, and added it back to ABNFs and occurance tables.
- Added EAP-Reissued-Payload AVP for signalling invalid packets, and RADIUS translation for this.
- Added EAP-Master-Session-Key AVP for keys, and suggestions for RADIUS translation.
- Attempted to clarify Framed-MTU RADIUS translation.
- Added a first attempt of security considerations section.
- Updated acknowledgements (please notify me if someone's missing).

Changes from -02.b to -02.c:

- Rephrased abstract and introduction sections.
- A couple of minor changes in Sections 2.1 and 2.2.
- Added text about advertising application support and role reversal.
- Changed type of Accounting-EAP-Auth-Method AVP from Enumerated to Unsigned64, and explained how it is determined.
- Removed references to EAP-Master-Session-Key AVP added in -02.b.
- Added Diameter-RADIUS translation of accounting AVPs.
- Added IANA Considerations section.
- References section: Updated RFC2284bis, added IEEE-802.11i and IKEv2, deleted RFC1510 ad RFC1938.

Changes from -02.a to -02.b:

- Added some text to Introduction section.
- Stole text from 2869bis about invalid packets, retransmissions, and fragmentation.

- In section 2.1, changed one "MAY" to "could" since it was not used to describe a requirement.

- Updated ABNF's and AVP occurance tables to match the current NASREQ-11 document.

- Added EAP-MTU and EAP-Master-Session-Key AVPs.

- Removed description of Configuration-Token, Nas-Port, Nas-Port-Id, and State AVPs (the text didn't add anything to their description in NASREQ).

- Added a first attempt of a section describing Diameter-RADIUS translation.

- Added references RFC2284bis, RFC2548, RFC2869bis, RADIUS1X, and DynAuth.

Changes from -01 to -02.a:

- New editor.

- Added Changelog appendix.

- Converted source to XML format. This will result in many small formatting changes in the ASCII version.

- Updated BASE and NASREQ references to current versions.

Intellectual Property Statement

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.