INTERNET DRAFT
Category: Standards Track
Title: draft-calhoun-diameter-mobileip-01.txt
Date: November 1998

Pat R. Calhoun
Charles E. Perkins
Sun Laboratories, Inc.

DIAMETER Mobile IP Extensions

Status of this Memo

Comments should be submitted to the diameter@ipass.com mailing list.

Distribution of this memo is unlimited.

This document is an Internet-Draft. 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.''

To view the entire list of current Internet-Drafts, please check the ``1id-abstracts.txt'' listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za (Africa), ftp.nordu.net (Northern Europe), ftp.nis.garr.it (Southern Europe), munnari.oz.au (Pacific Rim), ftp.ietf.org (US East Coast), or ftp.isi.edu (US West Coast).

Abstract

DIAMETER is an Authentication, Authorization and Accounting (AAA) Policy Protocol that is used between two entities for various services. This document defines an extension that allow a DIAMETER Client to request authentication and receive autorization information for a Mobile IP Mobile Node.

Table of Contents

1.0 Introduction

The Mobile IP [4] protocol defines a method that allows a Mobile Node to change its point of attachment to the Internet without service disruption. The protocol requires that all Mobility Agents share a pre-existing security association, which leads to scaling and configuration problems. Mobile IP also does not mention how Mobility

Agents account for services rendered, which does not make it an attractive protocol for use by service providers.

This document specifies extensions to DIAMETER that allow cross-domain authentication and authorization, assignment of Mobile Node Home Addresses, assignment of Home Agent, as well as Key Distribution to allow the Mobile IP network to scale in a large network of service providers.

The dynamic assignment of Mobile Node and Home Agent addresses are useful for Service Providers wishing to provide Mobile IP services for mobile nodes.

The DIAMETER Accounting extension [x] will be used to collect accounting information.

Small modifications to the Mobile IP protocol [4], which already exists in the TEP protocol [8], to allow a Mobile Node to identify itself using an NAI [6] in addition to an IP address. The use of the Network Access Identifier (NAI) [6] is consistent with the current roaming model which makes use of DIAMETER proxying [7].

The Extension number for this draft is four (4). This value is used in the Extension-Id Attribute value Pair (AVP) as defined in [1].

1.1 Specification of Requirements

In this document, several words are used to signify the requirements of the specification. These words are often capitalized.

MUST — This word, or the adjective "required", means that the definition is an absolute requirement of the specification.

MUST NOT — This phrase means that the definition is an absolute prohibition of the specification.

SHOULD — This word, or the adjective "recommended", means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications must be understood and carefully weighed before choosing a different course.

MAY — This word, or the adjective "optional", means that this item is one of an allowed set of alternatives. An implementation which does not include this option MUST be prepared to interoperate with another implementation which does include the option.

2.0 Command Codes

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

Command Name	Command Code
AA-Mobile-Node-Request	306
AA-Mobile-Node-Answer	307
Home-Agent-MIP-Request	308
Home-Agent-MIP-Answer	309

2.1 AA-Mobile-Node-Request (AMR)

Description

The AA-Mobile-Node-Request is sent by a Foreign Agent acting as a DIAMETER client to a server to request authentication and authorization of a Mobile Node.

The AA-Mobile-Node-Request message MUST include the MIP-Registration-Request, User-Name, MN-FA-Challenge, MN-FA-Response AVP as well as the Session-ID AVPs.

The Mobile-Node-Address AVP contains the the Home Address found in the Mobile Node's Registration Request. The Home-Agent-Address AVP contains the Home Address found in the Registration Request. If the Home Address is zero, it indicates that the Mobile Node is requesting that an address be allocated to it.

The User-Name AVP contains the NAI found in the Mobile IP Registration Request's Mobile-Node-NAI Extension.

If the Previous-FA-NAI AVP is found in the request, the DIAMETER Client is requesting that the Server return the Session Key that was assigned to the previous Foreign Agent for use with the Mobile Node. The Session Key is identified through the use of the Mobile-Foreign-SPI AVP.

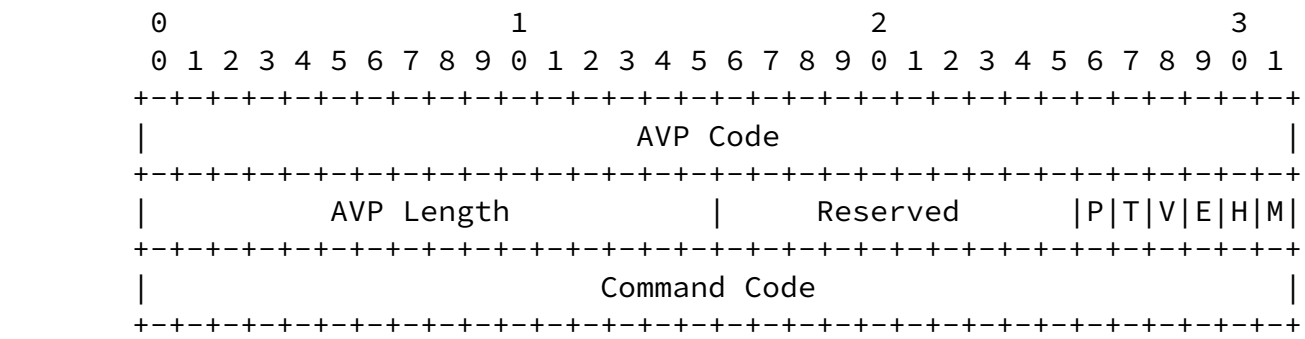
Message Format

```
<AA-Mobile-Node-Request>  ::= <DIAMETER Header>
                              <AA-Mobile-Node-Request Command AVP>
                              <Session-ID AVP>
                              <User-Name AVP>
                              <MIP-Registration-Request AVP>
                              <MN-FA-Challenge AVP>
                              <MN-FA-Response AVP>
                              <Mobile-Node-Address AVP>
                              <Home-Agent-Address AVP>
```

```
                                    [<Previous-FA-NAI AVP>]
                                    [<MN-FA-SPI AVP>]
                                    <Timestamp AVP>
                                    <Initialization-Vector AVP>
                                    {<Integrity-Check-Vector AVP> ||
                                     <Digital-Signature AVP> }
```

AVP Format

The AA-Mobile-Node-Request Command AVP format is shown below. The fields are transmitted from left to right.



AVP Code

256 DIAMETER-Command

AVP Length

The length of this AVP MUST be at exactly 12.

AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

Command Code

The Command Code field MUST be set to 306 (AA-Mobile-Node-Request).

2.2 AA-Mobile-Node-Answer (AMA)

Description

The AA-Mobile-Node-Answer is sent by the DIAMETER Server to the client in response to the AA-Mobile-Node-Request message. The message MUST include the Session-Id, Result-Code, MIP-Registration-Reply as well as the various key and SPI AVPs (see section 3.0) and MAY include the Home-Agent-Address and Mobile-

Node-Address AVPs.

The Home-Agent-Address AVP contains the Home Agent assigned to the Mobile Node. If the AVP contains a zero address, it is a request to allocate a Home Agent locally.

The Home-Agent-Address AVP contains the IP Address assigned to the Mobile Node. If this AVP contains a zero address, it is a request to allocate a Home Address for the Mobile Node.

The following error codes are defined for this message for use in the Error-Code AVP [1]:

DIAMETER_ERROR_UNKNOWN_DOMAIN 1
This error code is used to indicate to the initiator of the request that the requested domain is unknown and cannot be resolved.

DIAMETER_ERROR_USER_UNKNOWN 2
This error code is used to indicate to the initiator that the username request is not valid.

DIAMETER_ERROR_BAD_PASSWORD 3
This error code indicates that the password provided is invalid.

DIAMETER_ERROR_CANNOT_AUTHORIZE 4
This error code is used to indicate that the user cannot be authorized due to the fact that the user has expended local resources. This could be a result that the server believes that the user has already spent the number of credits in his/her account, etc.

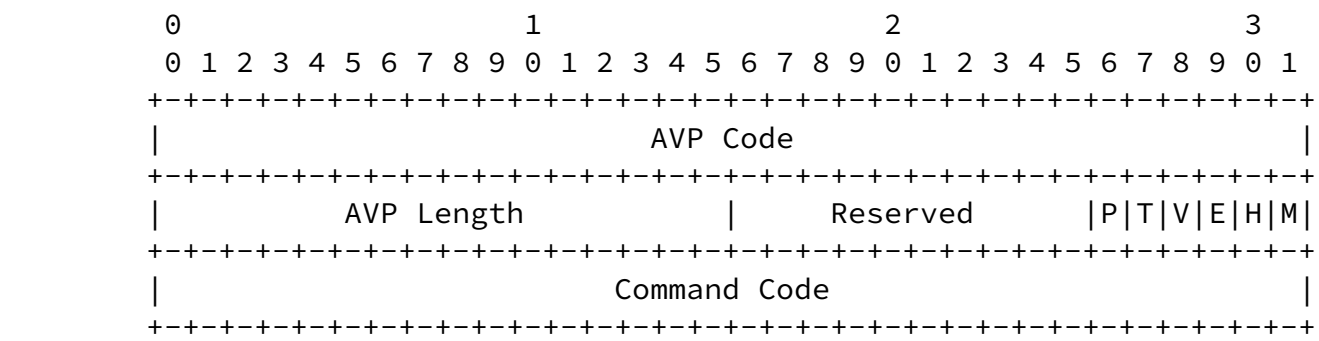
Message Format

```
<AA-Mobile-Node-Answer>  ::= <DIAMETER Header>
                             <AA-Mobile-Node-Answer Command AVP>
                             <Session-Id AVP>
                             <Result-Code AVP>
                             [<Error-Code AVP>]
                             <MIP-Registration-Reply AVP>
                             <MN-FA-SPI AVP>
                             <FA-to-MN-Key AVP>
                             <FA-HA-SPI AVP>
                             <FA-to-HA-Key AVP>
                             <Home-Agent-Address AVP>
                             <Mobile-Node-Address AVP>
                             <Session-Timeout AVP>
                             <Timestamp AVP>
                             <Initialization-Vector AVP>
                             {<Integrity-Check-Vector AVP> ||
```

<Digital-Signature AVP> }

AVP Format

The AA-Mobile-Node-Answer Command AVP format is shown below. The fields are transmitted from left to right.



AVP Code

256 DIAMETER-Command

AVP Length

The length of this AVP MUST be at exactly 12.

AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

Command Code

The Command Code field MUST be set to 307 (AA-Mobile-Node-Answer).

2.3 Home-Agent-MIP-Request (HAR)

Description

The Home-Agent-MIP-Request is sent by the home DIAMETER server to the Home Agent overseeing the Mobile Node to process the Mobile IP Registration Request.

The Home-Agent-MIP-Request message MUST include the MIP-Registration-Request, User-Name, Session-ID as well as the SPI and key AVPs (see section 3.0) to be used by the Mobile Node and the Home Agent.

If the Mobile-Node-Address AVP is set to a zero Address, it is a

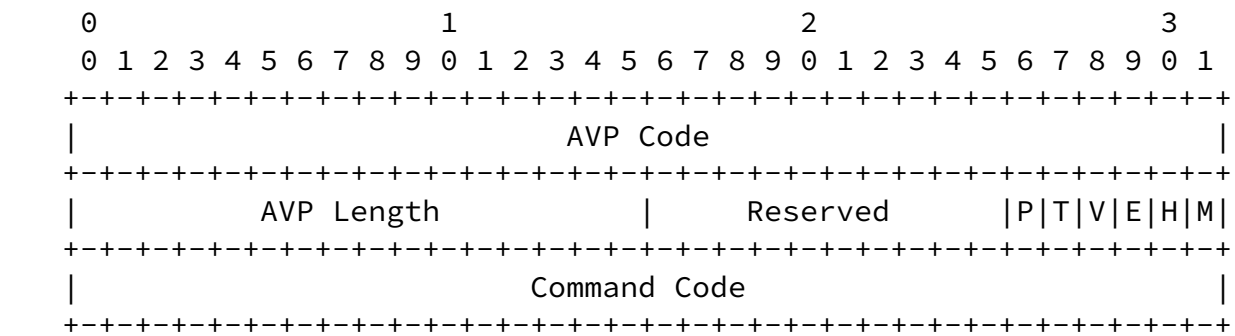
request to the Home Agent to allocate a Home Address to the Mobile Node.

Message Format

```
<Home-Agent-MIP-Request>  ::= <DIAMETER Header>
                              <Home-Agent-MIP-Request Command AVP>
                              <Session-Id AVP>
                              <User-Name AVP>
                              <MIP-Registration-Request AVP>
                              <MN-HA-SPI AVP>
                              <HA-to-MN-Key AVP>
                              <MN-to-HA-Key AVP>
                              <FA-HA-SPI AVP>
                              <HA-to-FA-Key AVP>
                              <MN-FA-SPI AVP>
                              <MN-to-FA-Key AVP>
                              <Home-Agent-Address AVP>
                              <Mobile-Node-Address AVP>
                              <Session-Timeout AVP>
                              <Timestamp AVP>
                              <Initialization-Vector AVP>
                              {<Integrity-Check-Vector AVP> ||
                               <Digital-Signature AVP> }
```

AVP Format

The Home-Agent-MIP-Request Command AVP format is shown below. The fields are transmitted from left to right.



AVP Code

256 DIAMETER-Command

AVP Length

The length of this AVP MUST be at exactly 12.

AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending

upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

Command Code

The Command Code field MUST be set to 308 (Home-Agent-MIP-Request).

2.4 Home-Agent-MIP-Answer (HAA)

Description

The Home-Agent-MIP-Answer is sent by the Home Agent to the home DIAMETER Server in response to the Home-Agent-MIP-Request. The message MUST include the Session-Id, Result-Code, MIP-Registration-Reply and the Mobile-Node-Address.

The following error codes are defined for this message for use in the Error-Code AVP [1]:

DIAMETER_ERROR_BAD_KEY 1
This error code is used by the Home Agent to indicate to the local DIAMETER Server that the key generated is invalid.

DIAMETER_ERROR_BAD_HOME_ADDRESS 2
This error code is used by the Home Agent to indicate that the Home Address chosen by the Mobile Node or assigned by the local DIAMETER server is unavailable.

DIAMETER_ERROR_TOO_BUSY 3
This error code is used by the Home Agent to inform the DIAMETER Server that it cannot handle an extra Mobile Node. Upon receiving this error the DIAMETER Server can try to use an alternate Home Agent if one is available.

DIAMETER_ERROR_MIP_REPLY_FAILURE 4
This error code is used by the Home Agent to inform the DIAMETER Server that the Registration Request failed.

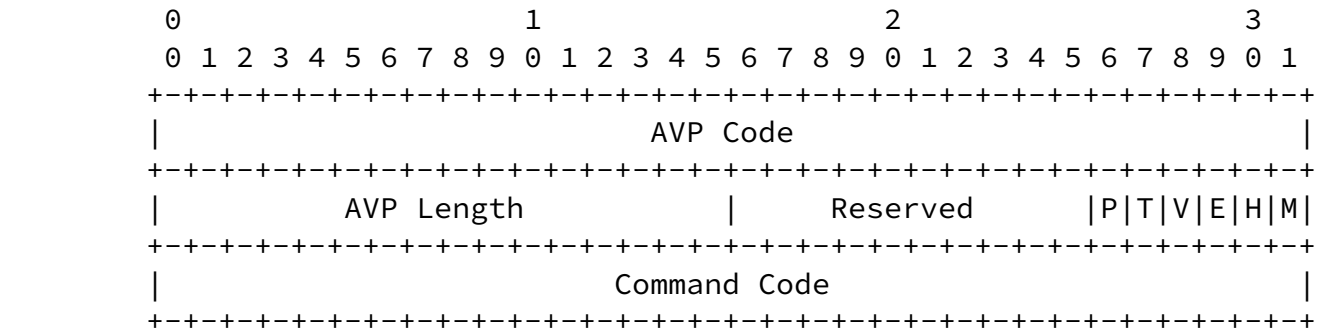
Message Format

```
<Home-Agent-MIP-Answer>  ::= <DIAMETER Header>
                             <Home-Agent-MIP-Answer Command AVP>
                             <Session-Id AVP>
                             <Result-Code AVP>
                             [<Error-Code AVP>]
                             <MIP-Registration-Reply AVP>
                             <Mobile-Node-Address AVP>
                             <Home-Agent-Address AVP>
                             <Timestamp AVP>
```

```
                                    <Initialization-Vector AVP>
                                    {<Integrity-Check-Vector AVP> ||
                                     <Digital-Signature AVP> }
```

AVP Format

The Home-Agent-MIP-Answer Command AVP format is shown below. The fields are transmitted from left to right.



AVP Code

256 DIAMETER-Command

AVP Length

The length of this AVP MUST be at exactly 12.

AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

Command Code

The Command Code field MUST be set to 309 (Home-Agent-MIP-Answer).

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:

Attribute Name	Attribute Code
MIP-Registration-Request	320
MIP-Registration-Reply	321
MN-FA-Challenge	322
MN-FA-Response	323

MN-FA-SPI	324
MN-to-FA-Key	325
FA-to-MN-Key	326
FA-HA-SPI	327
FA-to-HA-Key	328
HA-to-FA-Key	329
MN-HA-SPI	330
MN-to-HA-Key	331
HA-to-MN-Key	332
Mobile-Node-Address	333
Home-Agent-Address	334
Previous-FA-NAI	335

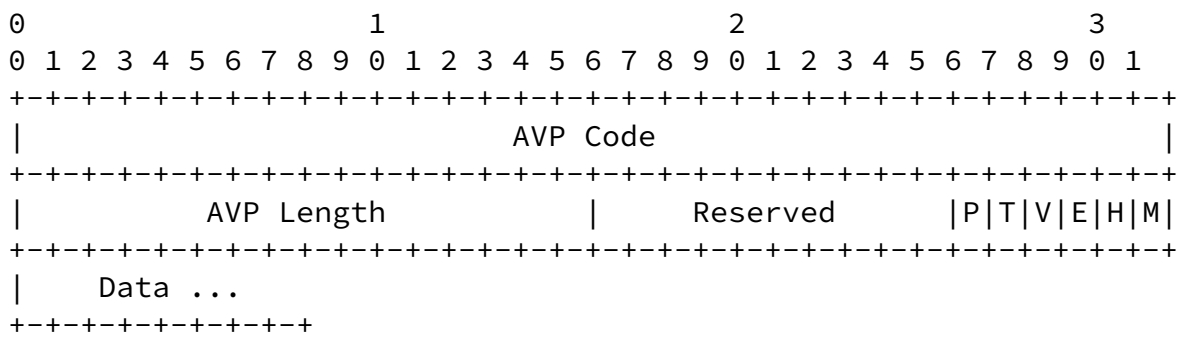
3.1 MIP-Registration-Request

Description

This AVP is used to carry the Mobile IP Registration Request [4] sent by the Mobile Node to the Foreign Agent within a DIAMETER message.

AVP Format

A summary of the MIP-Registration-Request AVP format is shown below.



Type

320 MIP-Registration-Request

AVP Length

The length of this attribute MUST be at least 9.

AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

Data

The data field contains the Mobile IP Registration Request.

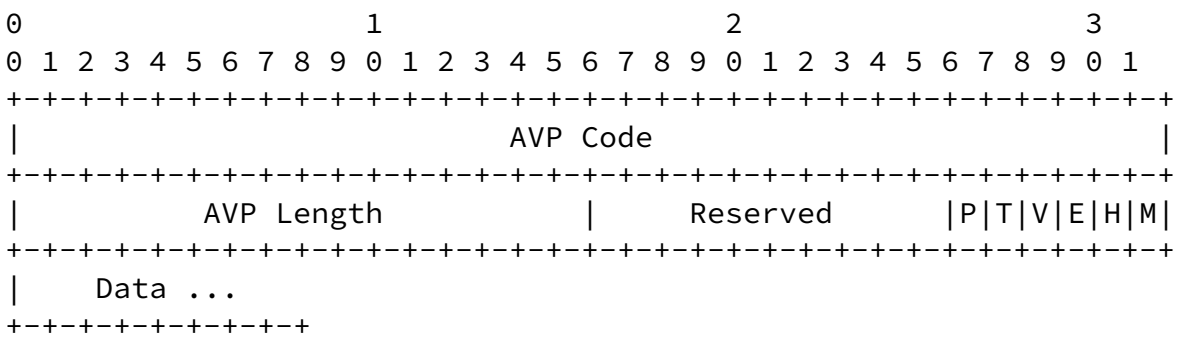
3.2 MIP-Registration-Reply

Description

This AVP is used to carry the Mobile IP Registration Reply [4] sent by the Home Agent to the Foreign Agent within a DIAMETER message.

AVP Format

A summary of the MIP-Registration-Reply AVP format is shown below.



AVP Code

321 MIP-Registration-Reply

AVP Length

The length of this attribute MUST be at least 9.

AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

Data

The data field contains the Mobile IP Registration Reply.

3.3 MN-FA-Challenge

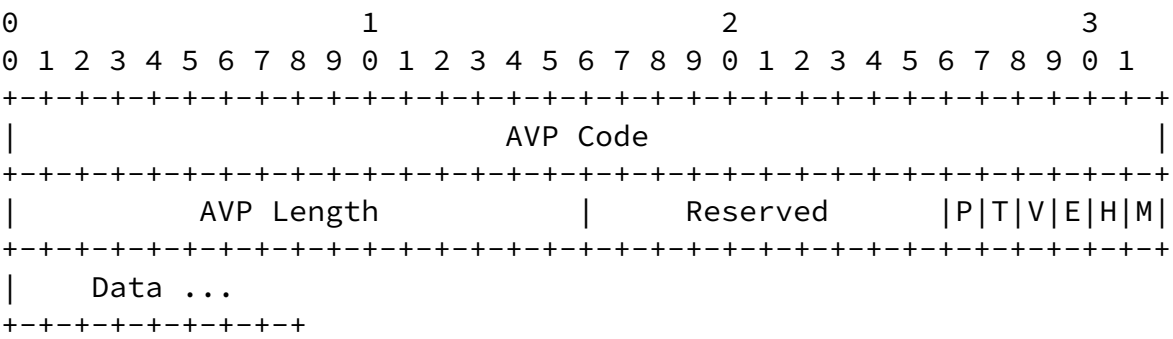
Description

The Challenge field consists of a 32 bit NTP timstamp followed by

a random value of at least 32 bits. The random value SHOULD be at least 96 bits in length [5].

AVP Format

A summary of the MN-FA-Challenge AVP format is shown below.



AVP Code

322 MN-FA-Challenge

AVP Length

The length of this attribute MUST be at least 16.

AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

Data

The data field contains the Foreign Agent's Challenge to the Mobile Node.

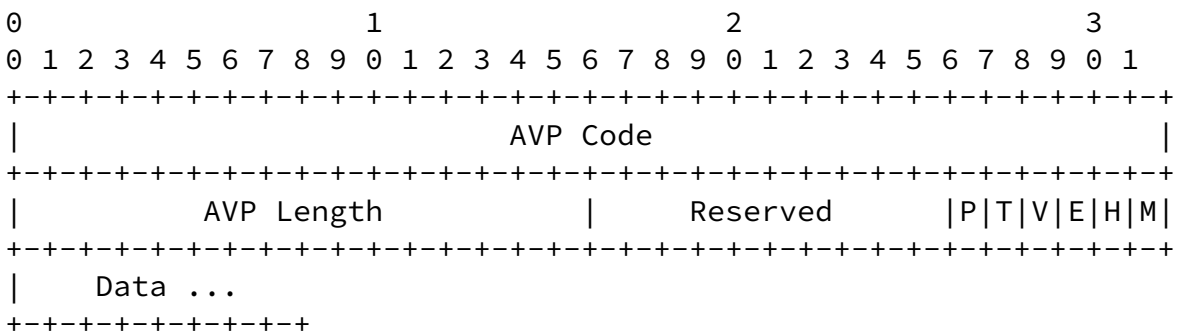
3.4 MN-FA-Response

Description

This AVP contains the Response generated by the Mobile Node as defined in the Mobile-Node Response extension [5]. The value is the result of the Challenge presented by the Foreign Agent hashed using the secret the Mobile Node shares with its Home DIAMETER Server.

AVP Format

A summary of the MN-FA-Response AVP format is shown below.



AVP Code

323 MN-FA-Response

AVP Length

The length of this attribute MUST be at least 9.

AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

Data

The data field contains the Mobile Node's Challenge Response.

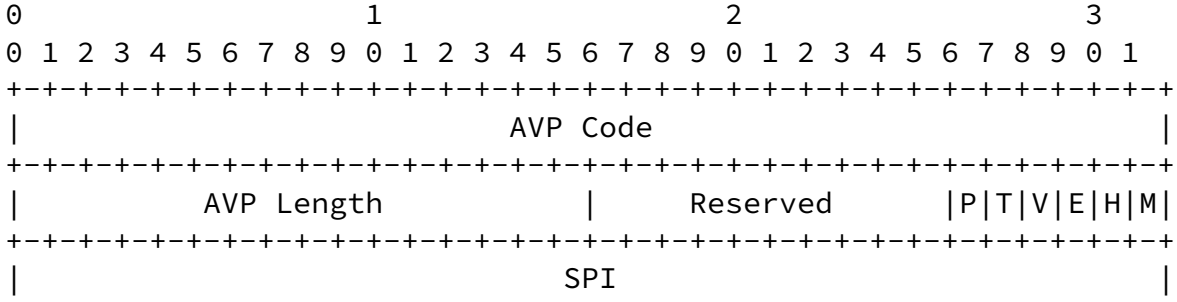
3.5 MN-FA-SPI

Description

The MN-FA-SPI is sent in both the Home-Agent-MIP-Request as well as the AA-Mobile-Node-Answer messages and contains the SPI value associated with the key generated by the home DIAMETER Server for use between the Foreign Agent and the Mobile Node (MN-to-FA-Key, FA-to-MN-Key).

AVP Format

A summary of the MN-FA-SPI AVP format is shown below.



AVP Code

324 MN-FA-SPI

AVP Length

The length of this attribute MUST be 12.

AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

Integer32

The Integer32 field contains the SPI value associated with the key shared between the Mobile Node and the Foreign Agent.

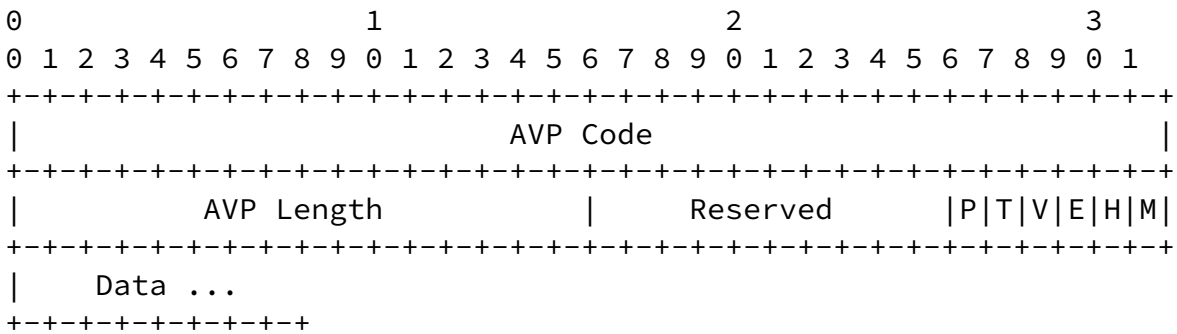
3.6 MN-to-FA-Key

Description

This AVP contains the Key generated by the home DIAMETER Server that must be used by the Mobile Node when computing the Mobile-Foreign Authentication extension in the Mobile IP Registration Request [4].

AVP Format

A summary of the MN-to-FA-Key AVP format is shown below.



AVP Code

325 MN-to-FA-Key

AVP Length

The length of this attribute MUST be at least 9.

AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

Data

The data field contains the encrypted key to be used by the Mobile Node when generating the Mobile IP Mobile-Foreign-Authentication-Extension.

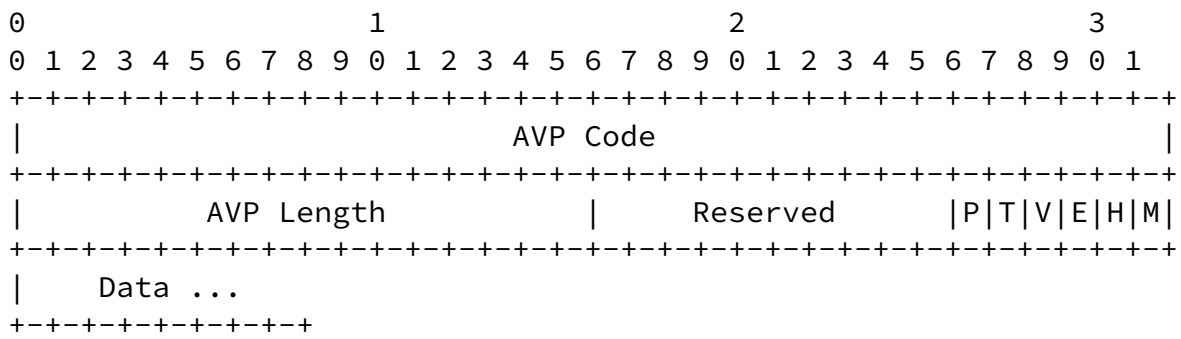
3.7 FA-to-MN-Key

Description

This AVP contains the Key generated by the home DIAMETER Server that must be used by the Foreign Agent when computing the Mobile-Foreign- Authentication extension in the Mobile IP Registration Reply [4].

AVP Format

A summary of the FA-to-MN-Key AVP format is shown below.



AVP Code

326 FA-to-MN-Key

AVP Length

The length of this attribute MUST be at least 9.

AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

Data

The data field contains the encrypted key to be used by the Foreign Agent when generating the Mobile IP Mobile-Foreign-Authentication-Extension.

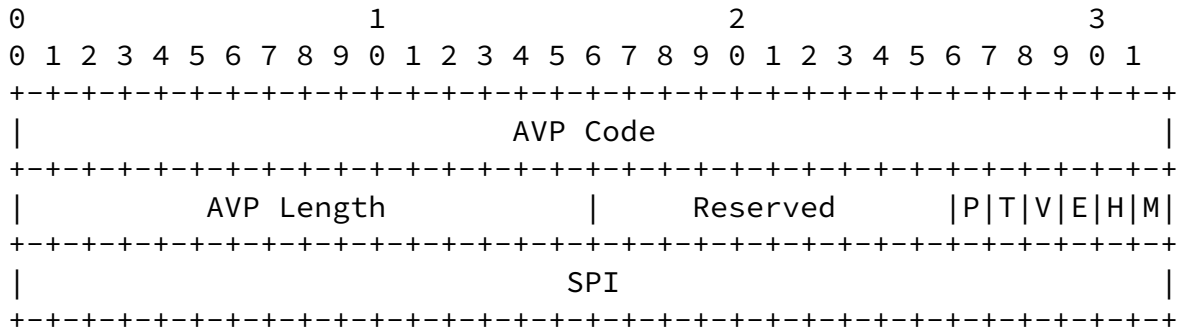
3.8 FA-HA-SPI

Description

The FA-HA-SPI is sent in both the Home-Agent-MIP-Request as well as the AA-Mobile-Node-Answer messages and contains the SPI value associated with the key generated by the home DIAMETER Server for use between the Foreign Agent and the Home Agent (FA-to-HA-Key, HA-to-FA-Key).

AVP Format

A summary of the FA-HA-SPI AVP format is shown below.



AVP Code

327 FA-HA-SPI

AVP Length

The length of this attribute MUST be 12.

AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

SPI

The SPI field contains the SPI value associated with the key shared between the Foreign Agent and the Home Agent.

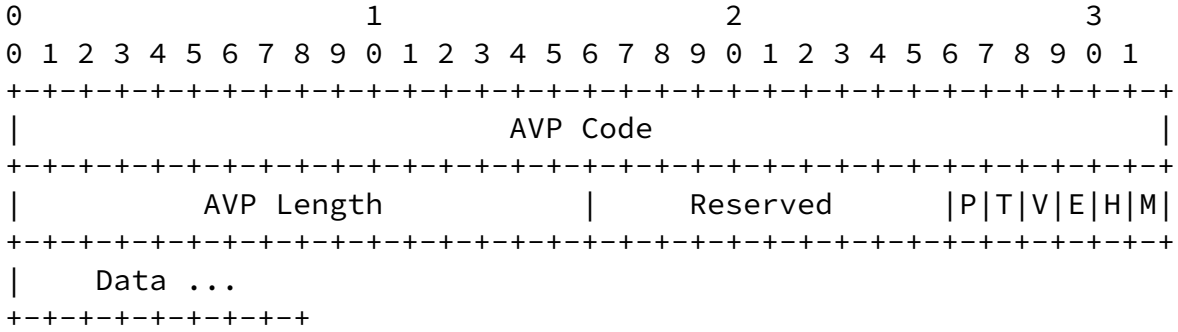
3.9 FA-to-HA-Key

Description

This AVP contains the Key generated by the home DIAMETER Server that must be used by the Foreign Agent when computing the Foreign-Home Authentication extension in the Mobile IP Registration Request [4].

AVP Format

A summary of the FA-to-HA-Key AVP format is shown below.



AVP Code

328 FA-to-HA-Key

AVP Length

The length of this attribute MUST be at least 9.

AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

Data

The data field contains the encrypted key to be used by the Foreign Agent when generating the Mobile IP Foreign-Home-Authentication-Extension.

3.10 HA-to-FA-Key

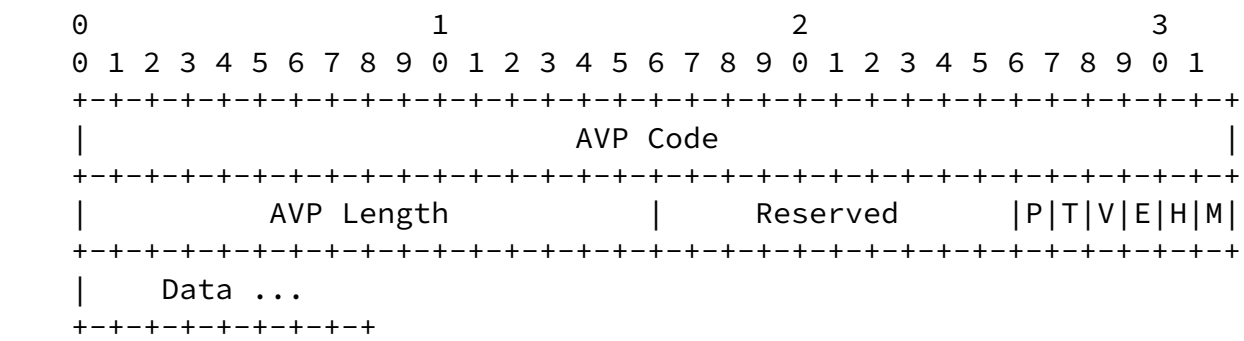
Description

This AVP contains the Key generated by the home DIAMETER Server that must be used by the Home Agent when computing the Foreign-

Home Authentication extension in the Mobile IP Registration Reply [4].

AVP Format

A summary of the HA-to-FA-Key AVP format is shown below.



AVP Code

329 HA-to-FA-Key

AVP Length

The length of this attribute MUST be at least 9.

AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

Data

The data field contains the encrypted key to be used by the Home Agent when generating the Mobile IP Foreign-Home-Authentication-Extension.

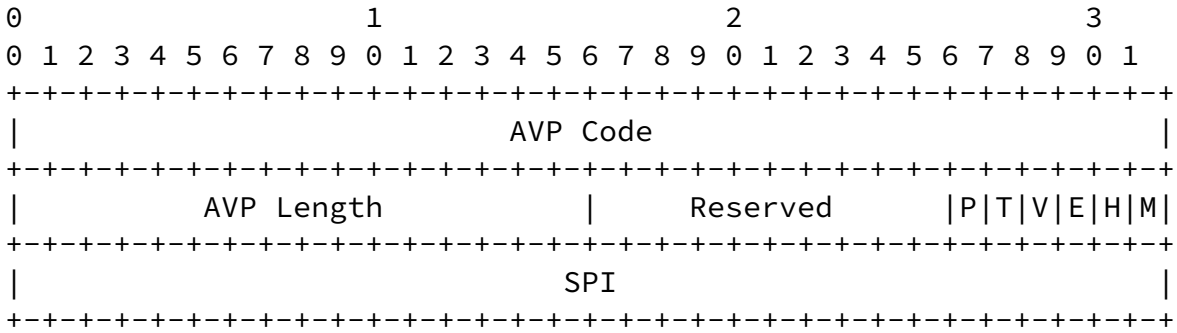
3.11 MN-HA-SPI

Description

The MN-HA-SPI is sent in both the Home-Agent-MIP-Request as well as the AA-Mobile-Node-Answer messages and contains the SPI value associated with the key generated by the home DIAMETER Server for use between the Mobile Node and the Home Agent (MN-to-HA-Key, HA-to-MN-Key).

AVP Format

A summary of the MN-HA-SPI AVP format is shown below.



AVP Code

330 MN-HA-SPI

AVP Length

The length of this attribute MUST be 12.

AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

Integer32

The Integer32 field contains the SPI value associated with the Session Key shared between the Mobile Node and the Home Agent.

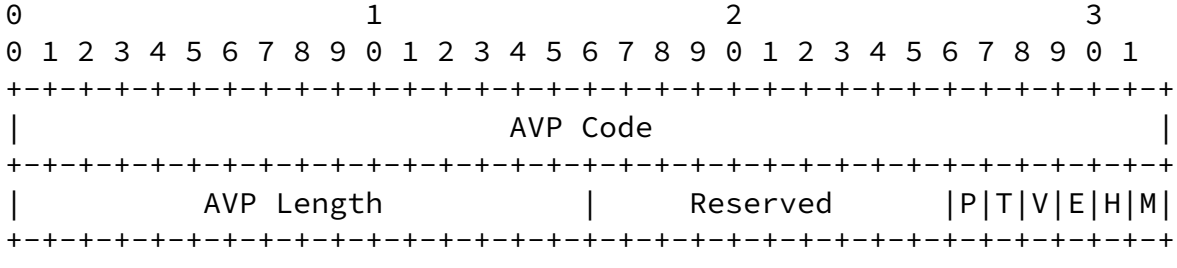
3.12 MN-to-HA-Key

Description

This AVP contains the Key generated by the home DIAMETER Server that must be used by the Mobile Node when computing the Mobile-Home Authentication extension in the Mobile IP Registration Request [4].

AVP Format

A summary of the MN-to-HA-Key AVP format is shown below.



```
|    Data ...
+-+-+-+-+-+-+-+-+
```

AVP Code

331 MN-to-HA-Key

AVP Length

The length of this attribute MUST be at least 9.

AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

Data

The data field contains the encrypted key to be used by the Mobile Node when generating the Mobile IP Mobile-Home-Authentication-Extension.

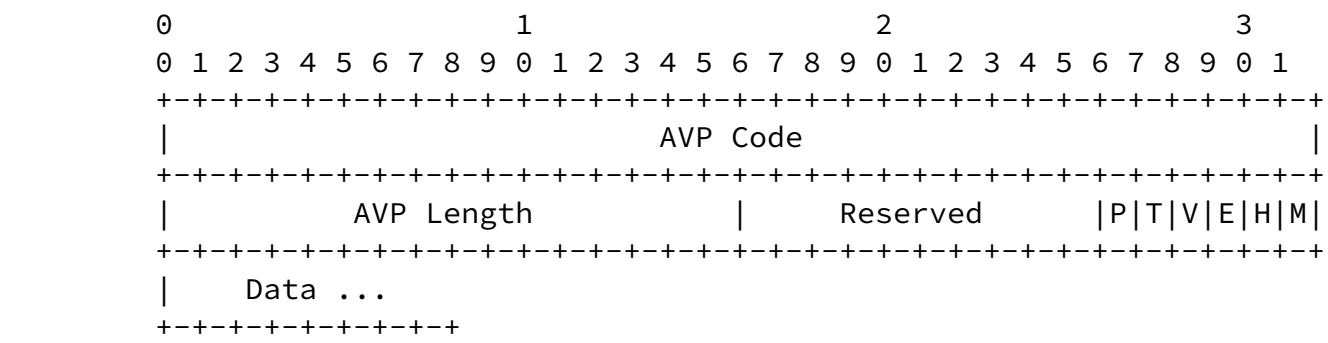
3.13 HA-to-MN-Key

Description

This AVP contains the Key generated by the home DIAMETER Server that must be used by the Home Agent when computing the Mobile-Home Authentication extension in the Mobile IP Registration Reply [4].

AVP Format

A summary of the HA-to-MN-Key AVP format is shown below.



AVP Code

332 HA-to-MN-Key

AVP Length

The length of this attribute MUST be at least 9.

AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

Data

The data field contains the encrypted key to be used by the Home Agent when generating the Mobile IP Mobile-Home-Authentication-Extension.

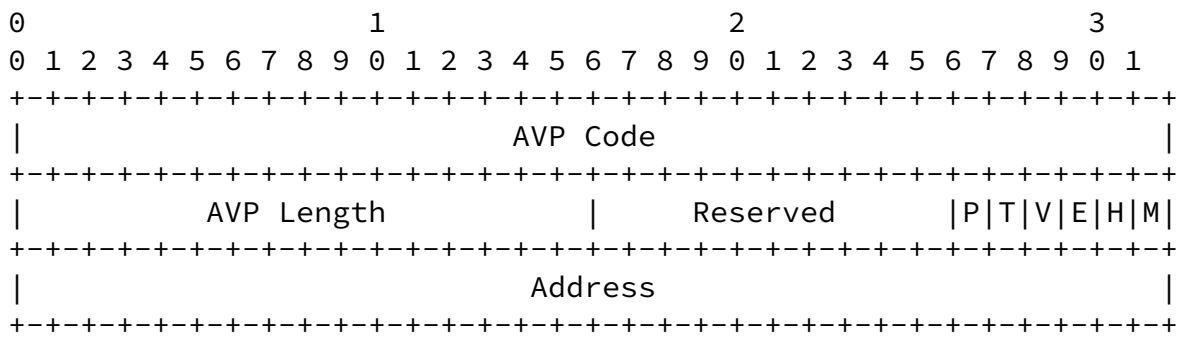
3.14 Mobile-Node-Address

Description

The Mobile-Node-Address AVP contains the Mobile Node's Home Address. When this AVP has a NULL Address (0.0.0.0), it is a request that a Home Address be allocated to the Mobile Node.

AVP Format

A summary of the Mobile-Node-Address AVP format is shown below.



AVP Code

333 Mobile-Node-Address

AVP Length

The length of this attribute MUST be 12.

AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

Address

The Address field contains the IP address assigned to the Mobile Node, or 0.0.0.0 if one is requested.

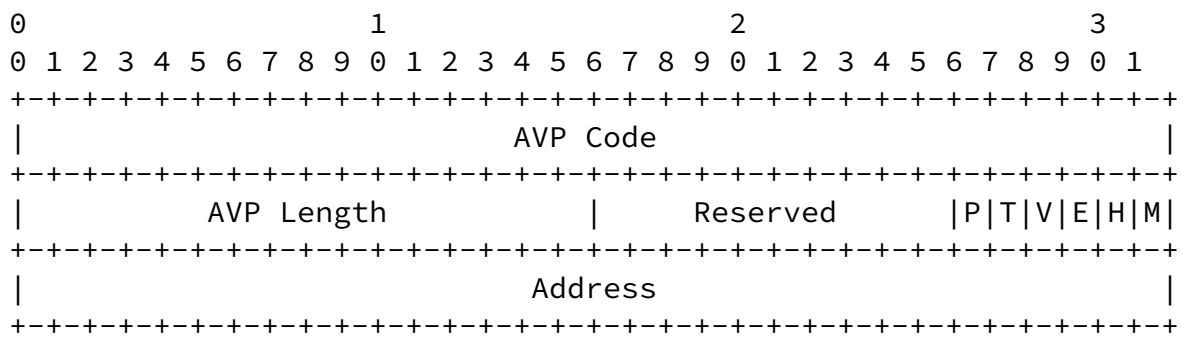
3.15 Home-Agent-Address

Description

The Home-Agent-Addess AVP contains the Mobile Node's Home Agent Address. When this AVP has a NULL address (0.0.0.0), it is a request that a Home Agent be allocated to the Mobile Node.

AVP Format

A summary of the Home-Agent-Address AVP format is shown below.



AVP Code

334 Home-Agent-Address

AVP Length

The length of this attribute MUST be 12.

AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

Address

The Address field contains the Home Agent address assigned to the Mobile Node. If the address is set to 0.0.0.0, the Mobile Node is requesting that a Home Agent be allocated either in the foreign network or in its home network. If the address is set to 255.255.255.255 the Mobile Node is requesting that the Home Agent be allocated only within its home network.

3.16 Previous-FA-NAI

Description

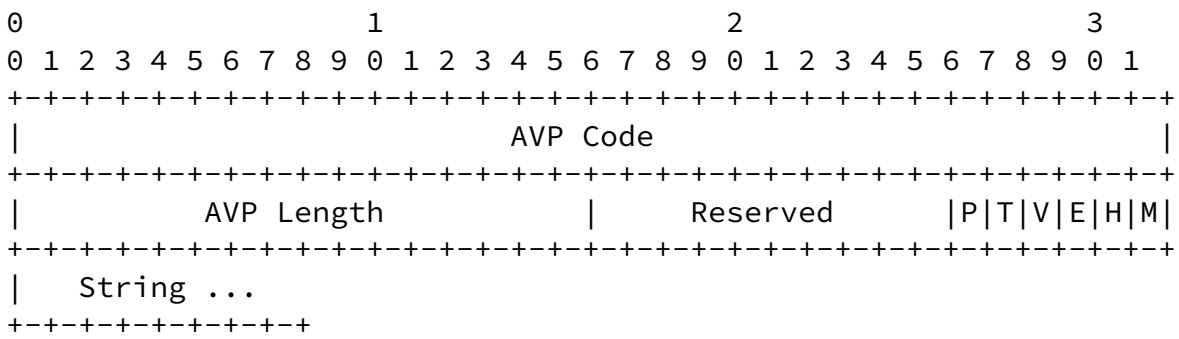
The Previous-FA-NAI AVP contains the Network Access Identifier of the Mobile Node's old Foreign Agent. The Mobile Node will include this information in the Registration Request when it moves it point of attachment to a new foreign agent under the same administrative domain as the old FA (identified by the domain part of the NAI).

When this AVP is present in the AA-Mobile-Node-Request, it indicates that the local DIAMETER Server overseeing the Foreign Agent should attempt to return the session key that was previously allocated to the old Foreign Agent for the Mobile Node. The session key is identified through the use of the MN-FA-SPI AVP, which MUST be present if this extension is present.

This allows the Mobile Node to move from one Foreign Agent to another within the same administrative domain without having to send the request back to the Mobile Node's Home DIAMETER Server.

AVP Format

A summary of the Previous-FA-NAI AVP format is shown below.



AVP Code

335 Previous-FA-NAI

AVP Length

The length of this attribute MUST be at least 9.

AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

String

The String field contains the Mobile Node's old Foreign Agent's NAI.

3.167 Foreign-Home-Agent-Available

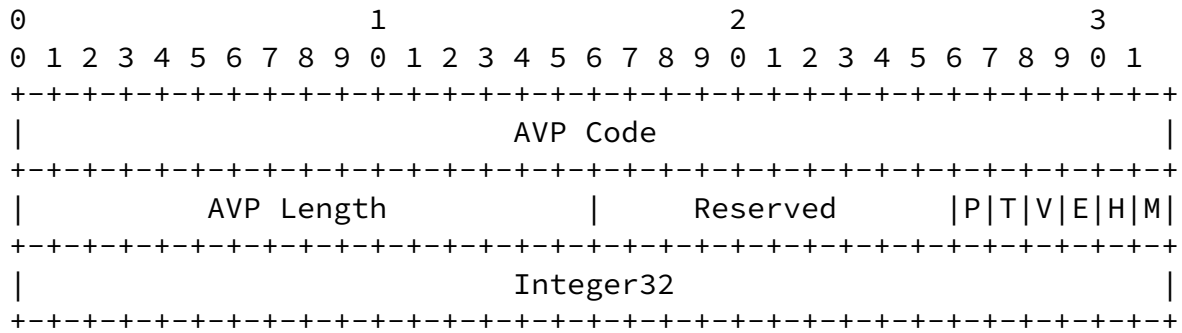
Description

The Foreign-Home-Agent-Available AVP is added by the AAAF owned by the same adminitrative domain as the Foreign Agent if it is willing and able to allocate a Home Agent within the Foreign network for the Mobile Node.

If this extension is present in the AMR and the Home-Agent-Address AVP is set to 0.0.0.0, the AAAH MAY allow the AAAF to assign a Home Agent for the Mobile Node. This is done by including the Home-Agent-Address AVP with a value of 0.0.0.0 in the AMR.

AVP Format

A summary of the Foreign-Home-Agent-Available AVP format is shown below.



AVP Code

335 Foreign-Home-Agent-Available

AVP Length

The length of this attribute MUST be at least 9.

AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

Integer32

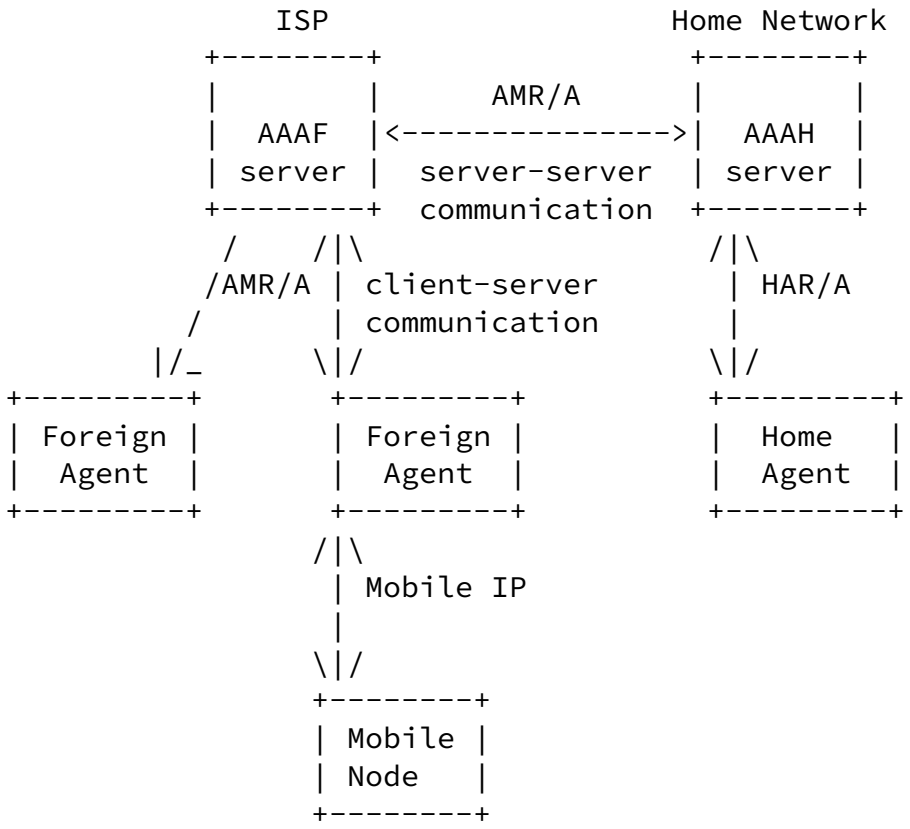
The Integer32 field MUST be set to 1 to inform the AAAH that the AAAF is able and willing to allocate a Home Agent for the Mobile Node.

4.0 Protocol Definition

This section will outline how the DIAMETER Mobile IP Extension can be used.

4.1 Inter-Domain Mobile IP

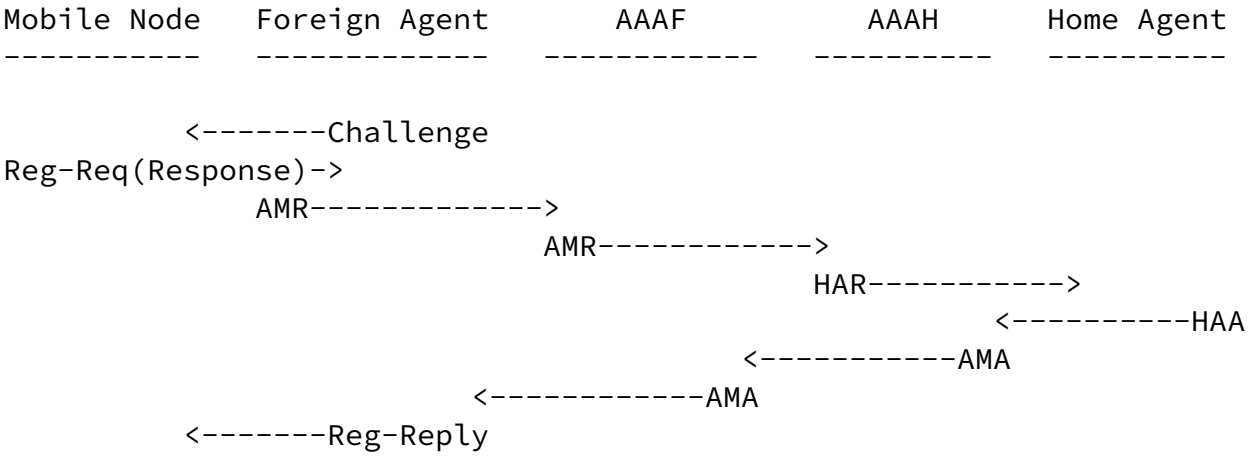
The following diagram is an example of an inter-domain Mobile IP network.



The AA-Mobile-Node-Request (AMR) is generated by the Foreign Agent and includes the AVPs defined in section 2.1. The Mobile-Node-Address AVP's value is copied from the Registration Request's Home Address field. The Home-Agent-Address AVP's value is copied from the Registration Request's Home Agent field. The value of the User-Name AVP is taken from the Mobile-Node-NAI extension as described in [8]. The request is then forwarded to the Foreign Agent's local DIAMETER server, known as the AAA-Foreign, or AAAF.

When the AAAF receives the message, it uses the User-Name AVP [1] to

determine whether authentication and authorization can be handled locally. The User-Name format is consistent with the NAI described in [6] and the user's domain is used to determine the Mobile Node's home DIAMETER Server (or AAAH). In the example below, the request cannot be processed by the AAAF, therefore the request is proxied [9] to the AAAH. Note that this exchange is only required when the Mobile Node attempts to gain service with a new Foreign Agent, or if the keys previously distributed expire.



The AAAH must first authenticate the user by validating the MN-FA-Challenge which contains a timestamp, which is described in [5]. If the timestamp information is valid, the AAAH uses the security association shared between the itself and the Mobile Node in order to validate the MN-FA-Response. If the response is invalid, the AAAH returns the AA-Mobile-Node-Answer (AMA, see section 2.2) with a Result-Code set to the appropriate value.

If the Mobile Node was successfully authenticated, the AAAH checks whether the Home-Agent-Address AVP specified a Home Agent. If one was specified, the AAAH must validate the address to ensure that it is a known Home Agent. If no Home Agent was specified the AAAH SHOULD allocate one on behalf of the Mobile Node. This can be done in a variety of ways, including using a load balancing algorithm in order to keep the load on all Home Agents equal. The actual algorithm used and the method of discovering the Home Agents is outside of this specification, but the method proposed in [4] can be used.

If the AMR's Mobile-Node-Address AVP did not specify an address, the AAAH has the option of assigning an address for the Mobile Node, or it can leave this up to the Home Agent. This is purely a local policy decision.

The AAAH then proceeds to generate three short-lived session keys; one which is shared between the Mobile Node and the Home Agent, one between the Mobile Node and the Foreign Agent, and one between the Foreign Agent and the Home Agent.

The keys destined for the Mobile Node are encrypted either using the

Mobile Node's secret or its public key [1]. The keys destined for the Foreign Agent are encrypted either using the secret shared between the AAAH and the AAAF, or using public key cryptography [1]. The keys destined for the Home Agent can be either encrypted using the secret it shares with the AAAH. The Session-Timeout AVP is included and contains the number of seconds before the session keys expire. A value of zero indicates that the session keys have no expiration.

Note that this extension requires a departure from the existing SPI usage described in [4]. The AAAH generates SPI values for the Mobility Agents as opposed to a receiver choosing its own SPI value. The SPI values are used as Key Identifiers, meaning that each short-lived session key has its own SPI value and since two nodes share a session key they share an SPI as well.

Suppose a Mobile Node and a Foreign Agent share a key that was created by the AAAH. The AAAH also generated a corresponding SPI value of 37,496. All Mobile-Foreign Authentication extensions must be computed by either entity using the shared session key would then include the SPI value of 37,496.

The AAAH then sends a Home-Agent-MIP-Request (HAR) to the assigned or requested Home Agent. The HAR contains the MIP-Registration-Request as well as the keys and SPIs destined for the Home Agent (HA-to-MN-Key, MN-HA-SPI, HA-to-FA-Key and FA-HA-SPI AVPs) and the Mobile Node (MN-FA-SPI, MN-to-FA-Key, MN-HA-SPI and MN-to-HA-Key AVP). The Mobile-Node-Address AVP contains an address if the Mobile Node specified a home address or if the AAAH assigned an address, but no address would be specified if the Home Agent were to assign one.

The Home Agent processes the DIAMETER Home-Agent-MIP-Request as well as the embedded Mobile IP Registration Request. If both are successfull, the Home Agent creates the Mobile IP Registration Reply, and furthermore includes the keying material to be used by the Mobile Node (MN-FA SPI, MN-to-FA-Key, MN-HA-SPI and MN-to-HA-Key) in the MIP-Registration-Reply AVP. If no Mobile-Node-Address AVP was present in the request the Home Agent must assign an address for the Mobile Node. The Result-Code AVP is included and the Home-Agent-MIP-Answer is sent to the AAAH.

The AAAH then issues a AA-Mobile-Node-Answer to the AAAF which includes the MIP-Registration-Reply, Result-Code and the Mobile-Node-Address AVP. The message also includes the keys and SPI AVPs used by the Foreign Agent (MN-FA-SPI, FA-to-MN-Key, FA-HA-SPI and the FA-to-HA-Key AVPs).

Upon receipt of the successful AA-Mobile-Node-Answer the AAAF decrypts the FA-to-MN-Key and the FA-to-HA-Key AVPs. These keys are then re-encrypted using the DIAMETER secret, unless IPSEC's ESP [x] is used between the Foreign Agent and the AAAF. The message is transmitted to the Foreign Agent.

The Foreign Agent, upon receipt of the AA-Mobile-Node-Answer, decrypts the appropriate KEY AVPs, and processes the Mobile IP Registration Reply which is then forwarded to the Mobile Node.

From this point on, all Registration Request and Replies need rely on the DIAMETER proxy chain, the Foreign Agent can contact the Home Agent directly using the keys which were previously distributed. This can continue until the session keys expire, as indicated in the Key-Lifetime AVP.

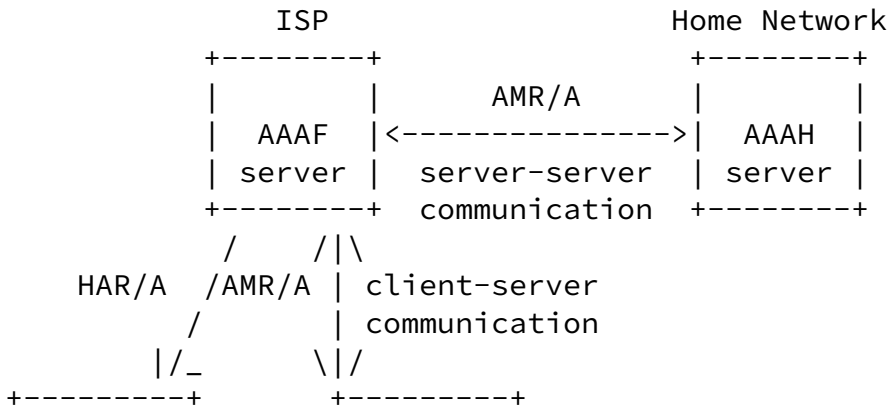
The following is an example of subsequent Mobile IP message exchange.

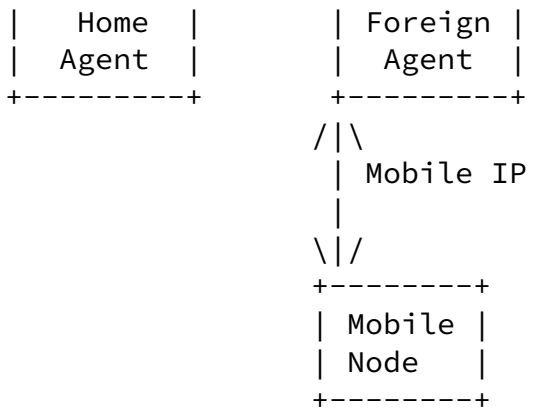
```
Mobile Node                Foreign Agent                Home Agent
-----------                -------------                ----------

Reg-Req(MN-FA-Auth, MN-HA-Auth)-------->

                           Reg-Req(MN-HA-Auth, FA-HA-Auth)-------->

                           <--------Reg-Rep(MN-HA-Auth, FA-HA-Auth)

<--------Reg-Rep(MN-HA-Auth, MN-FA-Auth)
```

Note that subsequent registrations MUST use the MN-FA Authentication extension[4].

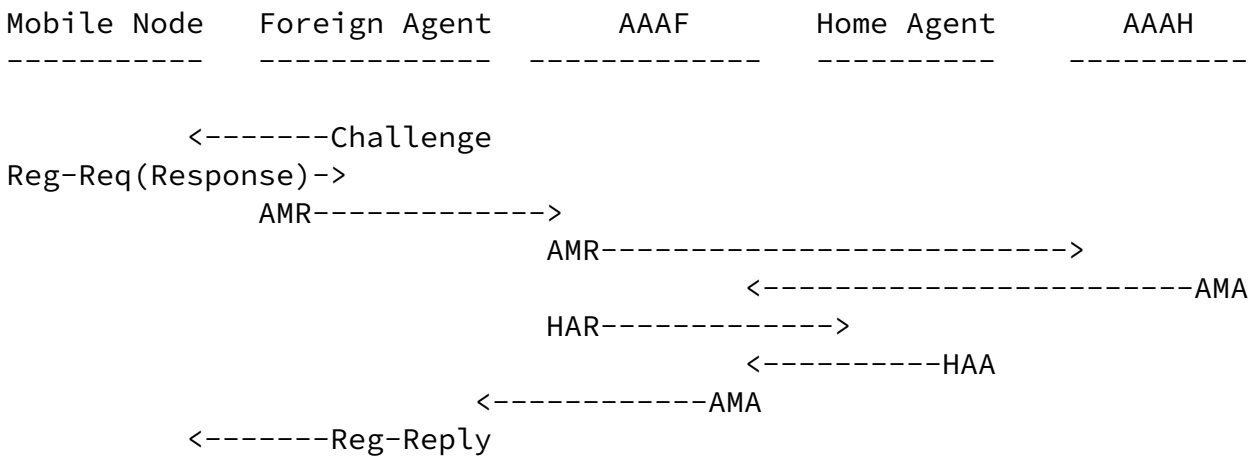
4.2 Allocation of Home Agent in Foreign Network

When the AAAF receives the AMR message, it can add the Foreign-Home-Agent-Available AVP to inform the AAAH that it is able and willing to assign a Home Agent for the Mobile Node. The AAAH will only allow this if the Home-Agent-Address in the AMR is set to zero (0). The AAAH does this by sending the AMA message to the AAAF with the Home-Agent-Address AVP set to zero (0). The AMA message still includes all of the keying information that was previously discussed, except that the keys for the Home Agent are encrypted using the security association the AAAH shares with the AAAF.





Upon receipt of such a message, the AAAF issues the HAR message to the Home Agent. Upon receipt of the response from the Home Agent the AAAF issues the AMA message to the Foreign Agent in the same method described earlier.



If the Mobile Node moves to another Foreign Network, which it detects from the Router Advertisement message, it can either request to keep the same Home Agent within the old foreign network, or it can request that a new one be assigned. If the Home-Agent-Address AVP is set to a value, it indicates that the same Home Agent should be used.

In this case the new AAAF would issue the AMR message towards the Mobile Node's AAAH, which would create the keys as previously defined. In this case all of the keys destined for the Home Agent would be encrypted using the security association it shares with the old Foreign Network's AAAF, while the keys for the Foreign Agent would be encrypted using the security association shared with the new Foreign Network's AAAF.

5.0 References

[1] Calhoun, Rubens, "DIAMETER", Internet-Draft, draft-calhoun-diameter-07.txt, Work in Progress, November 1998.

[2] Calhoun, Zorn, Pan, "DIAMETER Framework", Internet-Draft, draft-calhoun-diameter-framework-01.txt, Work in Progress, August 1998

[3] P. Calhoun, G. Montenegro, C. Perkins, "Tunnel Establishment Protocol", draft-ietf-mobileip-calhoun-tep-01.txt, Work in Progress, March 1998.

[4] C. Perkins, Editor. IP Mobility Support. RFC 2002, October 1996.

[5] P. Calhoun, C. Perkins, "Mobile IP Challenge/Response", draft-ietf-mobileip-challenge-00.txt, Work in Progress, November 1998.

[6] B. Aboba. "The Network Access Identifier." draft-ietf-roamops-nai-11.txt, Work in Progress, July 1998.

[7] Aboba, Zorn, "Roaming Requirements", draft-ietf-roamops-roamreq-09.txt, Work in Progress, April 1998.

[8] P. Calhoun, C. Perkins, "Mobile IP Dynamic Home Agent Allocation", draft-ietf-mobileip-ha-alloc-00.txt, Work in Progress, November 1998.

[9] P. Calhoun, W. Bulley, "DIAMETER Proxy Server Extensions", draft-calhoun-diameter-proxy-00.txt, Work in Progress, August 1998.

6.0 Authors' Addresses

Questions about this memo can be directed to:

Pat R. Calhoun
Technology Development
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

Charles E. Perkins
Technology Development
Sun Microsystems, Inc.
15 Network Circle
Menlo Park, California, 94025
USA

Phone: 1-650-786-6464
Fax: 1-650-786-6445
E-mail: charles.perkins@eng.sun.com