INTERNET DRAFT
Category: Standards Track
Title: draft-calhoun-diameter-mobileip-04.txt
Date: December 1999

Pat R. Calhoun
Sun Laboratories, Inc.
Charles E. Perkins
Nokia Research Center

DIAMETER Mobile IP Extensions

Status of this Memo

Abstract

This document specifies an extension to the DIAMETER base protocol that allows a DIAMETER server to authenticate, authorize and collect accounting information for services rendered to a mobile node. Combined with the Inter-Domain capability of the base protocol, this

extension allows mobile nodes to receive service from foreign service providers. The DIAMETER Accounting extension will be used by the Foreign and Home agents to transfer usage information to the DIAMETER servers.

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 Mobile IP protocol, as defined in [4], assumes that mobility is performed in a single administrative domain, and therefore does not specify how usage can be accounted for, which limits the applicability of Mobile IP in a commercial deployment. Further, the protocol requires that a mobile node has a static home agent, and home address, which is not desirable in a commercial network.

This document specifies an extension to the DIAMETER base protocol [1] that allows a DIAMETER server to authenticate, authorize and collect accounting information for services rendered to a mobile node. Combined with the Inter-Domain capability of the base protocol, this extension allows mobile nodes to receive service from foreign service providers. The DIAMETER Accounting extension [12] will be used by the Foreign and Home agents to transfer usage information to the DIAMETER servers.

The Mobile IP protocol [4] specifies a security model that requires that mobile nodes and home agents share a pre-existing security association, which leads to scaling and configuration issues. This specification defines an optional DIAMETER function that allows the mobile's home AAA server to act as a Key Distribution Center (KDC), where dynamic session keys are created and distributed to the mobility entities for the purposes of securing Mobile IP Registration messages.

As with the DIAMETER base protocol, the Mobile IP extension requires the presence of users' identities in a format consistent with the Network Access Identifier (NAI) specification [6], which is used for DIAMETER message routing purposes. This requires mobile nodes to include their identity in Registration messages, as defined in [8]. The use of the NAI is consistent with the current roaming model, as defined by the ROAMOPS Working Group [7].

This specification defines the DIAMETER Mobile-IP Extension, and addresses all of the requirements specified in [3, 16]. This section

will provides some examples and message flows of the Mobile IP and DIAMETER messages that occur when a Mobile Node requests service in a foreign network.

The Extension number for this draft is four (4). DIAMETER nodes conforming to this specification MUST include an Extension-Id AVP with a value of four in the Device-Reboot-Ind Command [1].

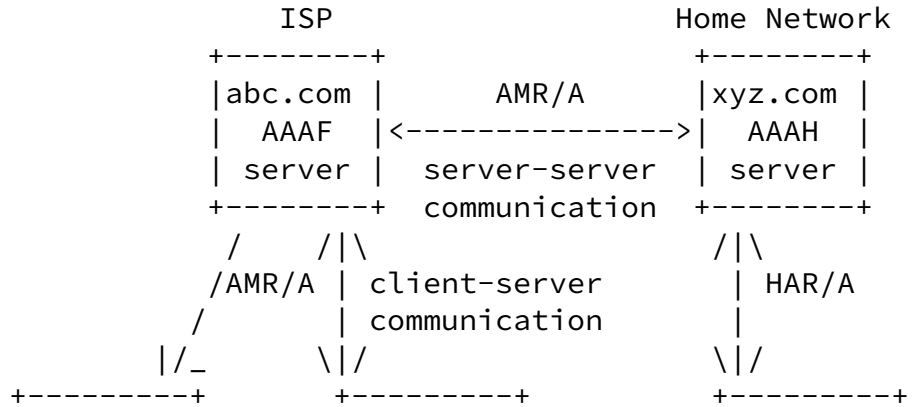
1.1 Requirements language

In this document, the key words "MAY", "MUST, "MUST NOT", "optional",

"recommended", "SHOULD", and "SHOULD NOT", are to be interpreted as described in [11].

1.2 Inter-Domain Mobile IP

When a Mobile Node node requests service by issuing a Registration Request to the foreign agent (FA), the FA creates the AA-Mobile-Node-Request (AMR) message, which includes the AVPs defined in section 2.1. The Home Address, Home Agent, Mobile Node NAI and other important fields are extracted from the registration messages and included as DIAMETER AVPs. The request is then forwarded to the FA's local DIAMETER server, known as the AAA-Foreign, or AAAF.



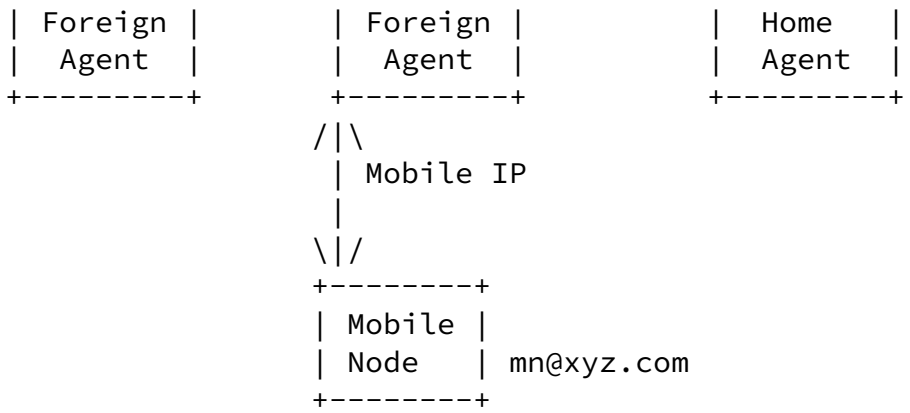
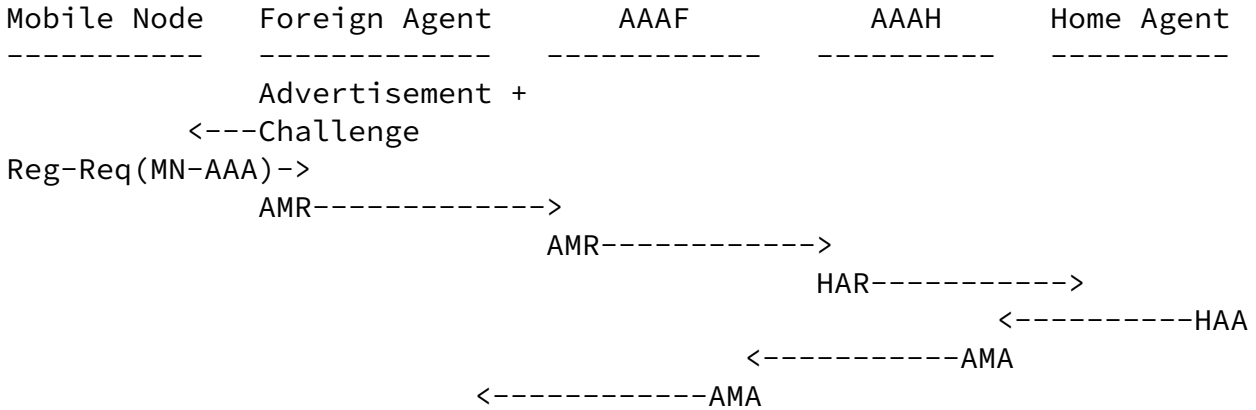


Figure 1: Inter-Domain Mobility

Upon receiving the AMR, the AAAF follows the procedures outlined in [1] to determine whether the AMR should be processed locally, or if it should be forwarded to another DIAMETER Server, known as the AAA-Home, or AAAH. Figure 1 describes an example of a mobile node (mn@xyz.com) requests service from a foreign provider (abc.com). The

request received by the AAAF is forwarded to abc.com's AAAH server.

Figure 2 provides an example of the message flows involved when the Foreign Agent invokes the AAA infrastructure to request that a mobile node be authenticated and authorized. Note that it is not required that the Foreign Agent invoke the AAA every time a Registration Request is received by the mobile, but rather when the prior authorization from the AAAH expires. The expiration of the authorization (and session keys, if used) is communicated through the Session-Time AVP in the response from the AAAH.



<-------Reg-Reply

Figure 2: Mobile IP/DIAMETER Message Exchange

The foreign agent depicted in figure 2 provides a challenge, which allows it to have direct control over the replay protection in the Mobile IP registration process, as described in [5]. The Challenge and MN-AAA authentication extension is used by the AAAH to authenticate the Mobile Node. If the value of the MN-AAA is invalid, the AAAH returns the AA-Mobile-Node-Answer (AMA, see section 2.2) with the Result-Code AVP set to an 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, and one that the Mobile Node is allowed to request. 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.

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 a local policy decision.

The AAAH then sends a Home-Agent-MIP-Request (HAR), which contains the Mobile IP Registration Request encapsulated in the MIP-Registration-Request AVP, to the assigned or requested Home Agent. If the Mobile-Node-Address AVP contains a NULL address (0.0.0.0), it is a request on behalf of the Mobile Node that a home address be assigned. The AAAH MAY manage the allocation of a home address for the mobile node, or leave the NULL address if it requires that the Home Agent perform the address assignment.

Upon receipt of the HAR, the Home Agent processes the DIAMETER message as well as the Mobile IP Registration Request. If the DIAMETER message is invalid, a HAR is returned with the Result-Code AVP set to an appropriate value (see section 3.0). If the HAR is valid, the Home Agent processes the registration message and creates the Registration Reply, encapsulated within the MIP-Registration-

Reply AVP. If a home address was requested, the Home Agent MUST assign one and include the address in both the Registration Reply and within the DIAMETER Mobile-Node-Address AVP. The DIAMETER response is then forwarded to the AAAH.

Upon receipt of the HAA, the AAAH sets the Command-Code AVP to AA-Mobile-Node-Answer (AMA) to the AAAF. The AAAF is responsible for ensuring that the message is properly forwarded to the correct foreign agent.

1.3 Key Distribution Center

If the AAAH is configured to act as a Key Distribution Center (KDC), the AAAH MUST create three short-lived keys when a Mobile Node is successfully authenticated and authorized. The three keys are used by the mobility entities to compute the three authentication extensions defined in [4]; Mobile-Foreign, Foreign-Home and Mobile-Home.

The keys destined for each mobility entity are encrypted either using the secret shared with the entity [1], or via its public key [9]. The keys are encrypted using the security association shared with the entity in question. If the AAAH does not communicate directly with the Foreign Agent, the FA's keys are encrypted using the security association shared with the AAAF. The Session-Timeout AVP contains the number of seconds before the session keys expire. A value of zero indicates infinity (no timeout).

KDC support requires a departure from the existing SPI usage, as 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 and MUST include the SPI value of 37,496.

The AAAH MUST include all of the session keys in the HAR message sent to the Home Agent. If the HAR and the Registration Request are successfully processed, the Home Agent MUST include the Mobile Node's session keys in the Registration Reply [15], and the Foreign Agent's session keys in the HAA message (see section 2.4). The Registration Reply MUST include the Mobile-Home authentication extension using the session key distributed for that purpose by the AAAH. Similarly, the Reply SHOULD include the Foreign-Home authentication extension using the appropriate session key distributed by the AAAH.

Upon receipt of the successful AA-Mobile-Node-Answer (AMA) the AAAF decrypts the FA-to-MN-Key and the FA-to-HA-Key AVPs. The AMA is transmitted to the Foreign Agent.

Upon receipt of the AMA, the Foreign Agent decrypts its session keys found in the FA-to-MN-Key and FA-to-HA-Key, and validates the Foreign-Home authentication extension using the session key. The Foreign Agent MUST also include a Mobile-Foreign authentication extension using the newly distributed session key it shares with the Mobile Node.

Once the session keys have been distributed to the three mobility entities, subsequent registrations do not need to invoke the AAA infrastructure unless the keys expire. These registrations MUST include the MN-FA, FA-HA and MN-HA authentication extensions. Figure 3 provides an example of subsequent Mobile IP message exchange.

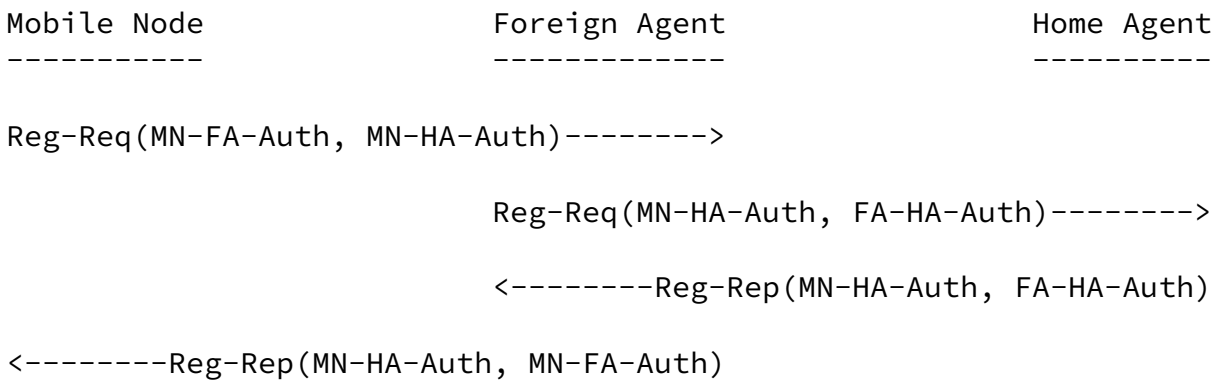


Figure 3: Mobile IP Message Exchange

1.4 Allocation of Home Agent in Foreign Network

The DIAMETER Mobile IP extension allows a Home Agent to be allocated in a foreign network, as required in [3, 16]. When the AAAF receives the AMR message with a NULL address in the Home-Agent-Address AVP, it MAY 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. Upon receiving such a message, the AAAH must decide whether its local policy would allow the user to have a Home Agent in the foreign network.

In the event that the AAAH is willing to let the Mobile Node have a Home Agent in the foreign network, it sends the AMA message to the AAAF with the Home-Agent-Address AVP set to the NULL address. The Home Agent's session keys MUST be encrypted using the security association the AAAH shares with the AAAF.

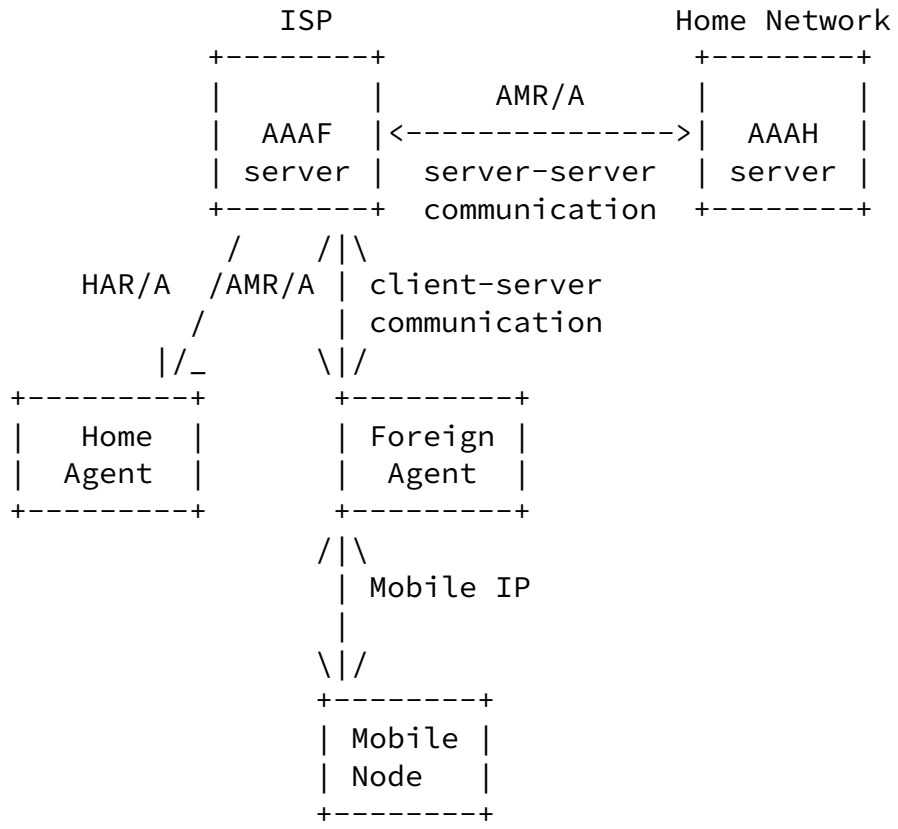


Figure 4: Home Agent allocated in Foreign Domain

Upon receiving the message, the AAAF MUST re-encrypt both the Foreign and Home Agent's session keys, and forward the HAR message to a local Home Agent. The HAA is sent to the AAAF, which then forwards the answer to the AAAH. The return path is identical to the one previously defined in section 1.2. The HAA MUST be received by the AAAH, otherwise it has no assurances that service is being provided, and all subsequent accounting information could be rejected. The HAA

is also used by the AAAH to receive the Home Address assigned to the Mobile Node. Figure 5 provides a message flow for a case where the Home Agent is allocated in the foreign domain.

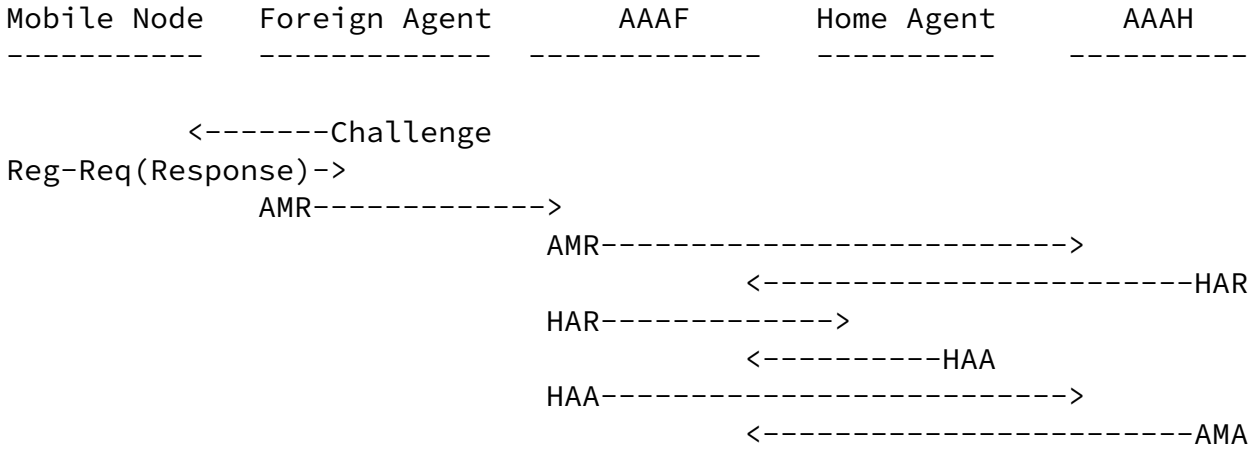


Figure 5: Mobile IP/DIAMETER Message Exchange

If the Mobile Node moves to another Foreign Network, 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. A non-NULL Home-Agent-Address AVP indicates that service from the same Home Agent is desired by the Mobile Node. When the Mobile Node requests such a service, the AAAH MUST interact with two AAAFs if it is willing to allow the Mobile Node to receive such service. The AAAH issues the HAR to the AAAF that oversees that Home Agent, and the AMA is issued to the AAAF that oversees the Foreign Agent.

1.5 DIAMETER Session Termination

A Foreign and Home Agent assume that their respective AAA servers maintain session state information for each mobile node in their networks. In order for the DIAMETER Server to release any resources allocated to a specific mobile node, the mobility agents MUST send a Mobile-Node-Termination-Ind (MTI) to their respective AAA servers.

The MTI message MAY also be issued by a DIAMETER server towards a client, which is done to request that a particular session be terminated.

2.0 Command-Code AVP Values

This section defines Command-Code [1] values that MUST be supported by all DIAMETER implementations conforming to this specification.

2.1 AA-Mobile-Node-Request (AMR) Command

The AA-Mobile-Node-Request (AMR), indicated by the Command-Code AVP set to 260, is sent by a Foreign Agent acting as a DIAMETER client to a server to request the authentication and authorization of a Mobile Node. The Foreign Agent uses information found in the Registration Request to construct the AMR such as the home address (Mobile-Node-Address AVP), home agent address (Home-Agent-Address AVP), mobile node NAI (User-Name AVP [1]). If the home address is set to a NULL address (0.0.0.0), it is an indication that the Mobile Node wishes to have a home address assigned to it in the Registration Reply.

If the AMR message includes a Foreign-Home-Agent-Available AVP and the Home-Agent-Address AVP has a NULL address, it is an indication that the AAAF is willing to assign a Home Agent in the foreign domain.

If the Previous-FA-NAI AVP is found in the request, the DIAMETER client requests that the server return the session key that was assigned to the previous Foreign Agent for use with the Mobile Node and Home Agent. The session key is identified through the use of the Mobile-Node-Address AVP.

Message Format

```
<AA-Mobile-Node-Request>  ::= <DIAMETER Header>
                              <Command-Code AVP = 260>
                              <Session-ID AVP>
                              <User-Name AVP>
                              {<Host-IP-Address AVP> ||
                               <Host-Name AVP>}
                              [<Destination-NAI AVP>]
                              <MIP-Registration-Request AVP>
                              <MN-FA-Challenge-Length AVP>
                              <MN-FA-Response AVP>
                              <Mobile-Node-Address AVP>
                              <Home-Agent-Address AVP>
                              <MN-AAA SPI AVP>
                              [<FA-MN-Preferred-SPI>]
```

```
                                    [<FA-HA-Preferred-SPI>]
                                    [<Previous-FA-NAI AVP>]
                                    [<Proxy-State [1] AVP>]
                                    [<Timestamp AVP>
                                     <Nonce AVP>
                                     <Integrity-Check-Value AVP>]
```

2.2 AA-Mobile-Node-Answer (AMA) Command

The AA-Mobile-Node-Answer (AMA), indicated by the Command-Code AVP set to 261, is sent by the AAAH in response to the AA-Mobile-Node-Request message. A successful response MUST include the MIP-Registration-Reply AVP. The Result-Code AVP MAY contain one of the values defined in section 3.0, in addition to the values defined in [1].

The Home-Agent-Address AVP contains the Home Agent assigned to the Mobile Node, while the Mobile-Node-Address AVP contains the home address that was assigned. A successful response MUST NOT have either AVP set to a NULL address.

Message Format

```
   <AA-Mobile-Node-Answer>  ::= <DIAMETER Header>
                                <Command-Code AVP = 261>
                                <Session-Id AVP>
                                {<Host-IP-Address AVP> ||
                                 <Host-Name AVP>}
                                <Destination-NAI AVP>
                                <Result-Code AVP>
                                [<Error-Code AVP>]
                                [<MIP-Registration-Reply AVP>]
                                [<FA-to-MN-Key AVP>]
                                [<FA-to-HA-Key AVP>]
                                <Home-Agent-Address AVP>
                                <Mobile-Node-Address AVP>
                                <Session-Timeout AVP>
                                [<Proxy-State AVP>]
                                [<Timestamp AVP>
                                 <Nonce AVP>
                                 <Integrity-Check-Value AVP>]
```

2.3 Home-Agent-MIP-Request (HAR) Command

The Home-Agent-MIP-Request (HAR), indicated by the Command-Code AVP set to 262, is sent by the AAAH to the Home Agent. If the Home Agent is to be assigned in a foreign network, the HAR is issued to the AAAF overseeing the Home Agent. If the HAR message includes a NULL home address in the Mobile-Node-Address AVP and the request is successfully processed, the Home Agent MUST allocate one such address to the mobile node.

If a AAAF receives a HAR with the Mobile-Home-Agent AVP set to a NULL address, it is a request that a Home Agent be assigned in the foreign network.

If the AAAH is configured as a Key Distribution Center (see section 1.3), the AAAH MUST create the session keys and include them in the HAR message.

Message Format

```
<Home-Agent-MIP-Request>  ::= <DIAMETER Header>
                              <Command-Code AVP = 262>
                              <Session-Id AVP>
                              {<Host-IP-Address AVP> ||
                               <Host-Name AVP>}
                              <User-Name AVP>
                              [<Destination-NAI AVP>]
                              <MIP-Registration-Request AVP>
                              [<HA-to-MN-Key AVP>]
                              [<MN-to-HA-Key AVP>]
                              [<HA-to-FA-Key AVP>]
                              [<MN-to-FA-Key AVP>]
                              [<FA-to-HA-Key AVP>]
                              [<FA-to-MN-Key AVP>]
                              <Home-Agent-Address AVP>
                              <Mobile-Node-Address AVP>
                              <Session-Timeout AVP>
                              [<Proxy-State AVP>]
                              [<Timestamp AVP>
```

```
                                    <Nonce AVP>
                                    <Integrity-Check-Value AVP>]
```

2.4 Home-Agent-MIP-Answer (HAA) Command

The Home-Agent-MIP-Answer (HAA), indicated by the Command-Code AVP set to 263, is sent by the Home Agent to its local AAA server in response to a Home-Agent-MIP-Request. In the event that this message is sent to an AAAF in a foreign network, the message MUST be forwarded to the AAAH. The Result-Code AVP MAY contain one of the values defined in section 3.0, in addition to the values defined in [1].

Message Format


```
<Home-Agent-MIP-Answer>  ::= <DIAMETER Header>
                             <Command-Code AVP = 263>
                             <Session-Id AVP>
                             {<Host-IP-Address AVP> ||
                              <Host-Name AVP>}
                             <Destination-NAI AVP>
                             <Result-Code AVP>
                             [<Error-Code AVP>]
                             <MIP-Registration-Reply AVP>
                             <Mobile-Node-Address AVP>
                             <Home-Agent-Address AVP>
                             [<FA-to-HA-Key AVP>]
                             [<FA-to-MN-Key AVP>]
                             [<Proxy-State AVP>]
                             [<Timestamp AVP>
                              <Nonce AVP>
                              <Integrity-Check-Value AVP>]
```

2.5 Mobile-Node-Terminate-Ind (MTI) Command

The Mobile-Node-Terminate-Ind (MTI), indicated by the Command-Code AVP set to 264, is sent by a Foreign Agent or Home Agent to the their local DIAMETER server to inform the server that an active session has been terminated. The MTI message MAY be sent by a DIAMETER Server to the Foreign and Home Agent as an explicit request that the Mobile Node's session be terminated.

Message Format

```
Mobile-Node-Terminate-Ind  ::= <DIAMETER Header>
                               <Command-Code AVP = 264>
                               <Session-Id AVP>
                               {<Host-IP-Address AVP> ||
                                <Host-Name AVP>}
                               <User-Name AVP>
                               [<Destination-NAI AVP>]
                               <Mobile-Node-Address AVP>
                               <Home-Agent-Address AVP>
                               [<Proxy-State AVP>]
                               [<Timestamp AVP>
                                <Nonce AVP>
                                <Integrity-Check-Value AVP>]
```

3.0 Result-Code AVP Values

This section defines new Result-Code [1] values that MUST be

supported by all DIAMETER implementations that conform to this specification.

DIAMETER_ERROR_BAD_KEY 16
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 17
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 18
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 19
This error code is used by the Home Agent to inform the DIAMETER server that the Registration Request failed.

4.0 Mandatory AVPs

The following table describes the DIAMETER AVPs defined in the Mobie IP extension, their AVP Code values, types, possible flag values and whether the AVP MAY be encrypted.

				AVP Flag rules				
Attribute Name	Attribute Code	Section Defined	Value Type	MUST	MAY	SHOULD NOT	MUST NOT	Encr Cand
MIP-Registration-Request	320	4.1	Data	M	P		T,V	Y
MIP-Registration-Reply	321	4.2	Data	M	P		T,V	Y
MN-FA-Challenge-Length	322	4.3	Integer32	M	P		T,V	Y
MN-FA-Response	323	4.4	Data	M	P		T,V	Y
Mobile-Node-Address	333	4.5	Address	M	P		T,V	Y
Home-Agent-Address	334	4.6	Address	M	P		T,V	Y
Previous-FA-NAI	335	4.7	String	M	P		T,V	Y
Foreign-Home-Agent-Available	337	4.8	Integer32	M	P		T,V	Y
MN-AAA-SPI	336	4.9	Integer32	M	P		T,V	Y

4.1 MIP-Registration-Request AVP

The MIP-Registration-Request AVP (AVP Code 320) is of type data and contains the Mobile IP Registration Request [4] sent by the Mobile

Node to the Foreign Agent.

4.2 MIP-Registration-Reply AVP

The MIP-Registration-Reply AVP (AVP Code 321) is of type data and contains the Mobile IP Registration Reply [4] sent by the Home Agent to the Foreign Agent.

4.3 MN-FA-Challenge-Length AVP

The MN-FA-Challenge-Length AVP (AVP Code 322) is of type Interger32 and contains the number of octets in the MIP-Registration-Request AVP that are to be used by the AAAH as the challenge value used in the computation of the Response (see section 4.4).

4.4 MN-FA-Response AVP

The MN-FA-Response AVP (AVP Code 323) is of type data and contains the authenticator field of the Mobile Node's challenge response found in the Mobile IP MN-AAA authentication extension [5]. The authenticator is the value computed by the mobile node using the Registration Request and the security association shared with its AAAH. This AVP is used to authenticate the Mobile Node.

The data field contains the mobile node's challenge response and is used to authenticate the mobile node. Although any authentication algorithm can be used, all implementations MUST support MD5's prefix+suffix mode, as described in [5], and MAY support the HMAC mode. The challenge value used in the computation is found in the MIP-Registration-Request AVP. The length of the challenge is found in the MN-FA-Challenge-Length AVP.

4.5 Mobile-Node-Address AVP

The Mobile-Node-Address AVP (AVP Code 333) is of type Address and 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.

4.6 Home-Agent-Address AVP

The Home-Agent-Addess AVP (AVP Code 334) is of type Address and 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. If this AVP is set to the NULL address in the AMA message, it is an indication that a Home Agent MUST be allocated in the foreign network. If the address is set to 255.255.255.255 in the AMR, it is a request from the Mobile Node that the Home Agent MUST be allocated only within the home network.

4.7 Previous-FA-NAI AVP

The Previous-FA-NAI AVP (AVP Code 335) is of type String and contains the Network Access Identifier [6] 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 Mobile-Node-Address 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.

4.8 Foreign-Home-Agent-Available AVP

The Foreign-Home-Agent-Available AVP (AVP Code 336) is of type Integer32 and is added with a value of one by the AAAF owned by the same administrative 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.

4.9 MN-AAA-SPI AVP

The MN-AAA-SPI AVP (AVP Code 336) is of type Integer32 and is sent in the AA-Mobile-Node-Request by the Foreign Agent, and contains the SPI value found in the Mobile-IP MN-AAA Authentication Extension [5]. The SPI can be used by the AAAH to identify the security context to use in order to authenticate the Mobile Node. When possible, it is recommended that the AAAH makes use of the Mobile Node's NAI to identify the security context, when possible.

5.0 Key Distribution Center (KDC) AVPs

The Mobile-IP protocol defines a set of security associations shared between the Mobile Node, Foreign Agent and Home Agents. These three security associations (MN-FA, MN-HA and FA-HA), can be dynamically created by the AAAH. This requires that the AAAH create Mobile-IP Session Keys, and that these keys be distributed to the three mobile entities, via the DIAMETER Protocol. The KDC AVPs SHOULD be supported.

When Key Distribution Center services are required, the AAAH creates three session keys; the MN-FA, MN-HA and the FA-HA keys. Each of these keys are encrypted two different ways, one for each key recipient. The mobile node and home agent Session Keys are sent to the Home Agent, while the foreign agent's keys are sent to the foreign agent via the AAAF.

If strong authentication and confidentiality of the session keys is required, it is recommended that the strong security extension [9] be used.

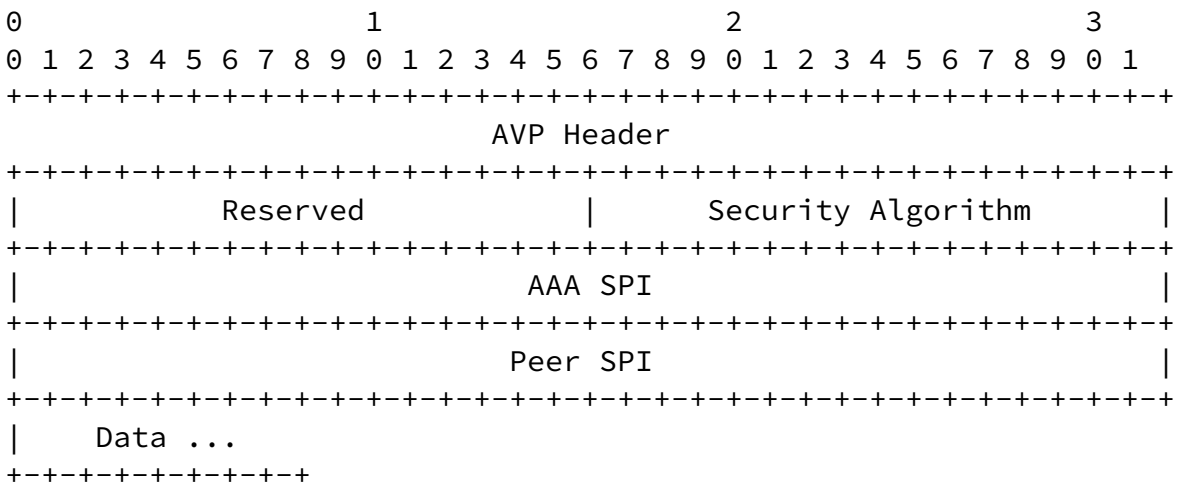
The following table describes the DIAMETER AVPs defined in the Mobie IP extension, their AVP Code values, types, possible flag values and whether the AVP MAY be encrypted.

				AVP Flag rules				
Attribute Name	Attribute Code	Section Defined	Value Type	MUST	MAY	SHOULD NOT	MUST NOT	Encr Cand
MN-to-FA-Key	325	5.1	Complex	M	P		T,V	Y

MN-to-HA-Key	331	5.1	Complex	M	P		T,V	Y
FA-to-MN-Key	326	5.2	Complex	M	P		T,V	Y
FA-to-HA-Key	328	5.2	Complex	M	P		T,V	Y
HA-to-MN-Key	332	5.2	Complex	M	P		T,V	Y
HA-to-FA-Key	329	5.2	Complex	M	P		T,V	Y
FA-MN-Preferred-SPI	324	5.3	Integer32	M	P		T,V	Y
FA-HA-Preferred-SPI	327	5.4	Integer32	M	P		T,V	Y

5.1 Mobile Node Session Key AVP

The session keys AVPs destined for the Mobile Node are of type complex, and MUST have the AVP length field set to at least 21. The AVP has the following format:



AVP Code
325 for MN-FA Key, destined for Mobile Node
331 for MN-HA Key, destined for Mobile Node

Security Algorithm
The security algorithm field specifies the algorithm that was used to encrypt the session keys. The values are consistent with those found in [15], which also contains the formula used for encryption. The following are currently defined:

Algorithm Identifier	Name	Reference
2	MD5/prefix+suffix	RFC 2002 [14]

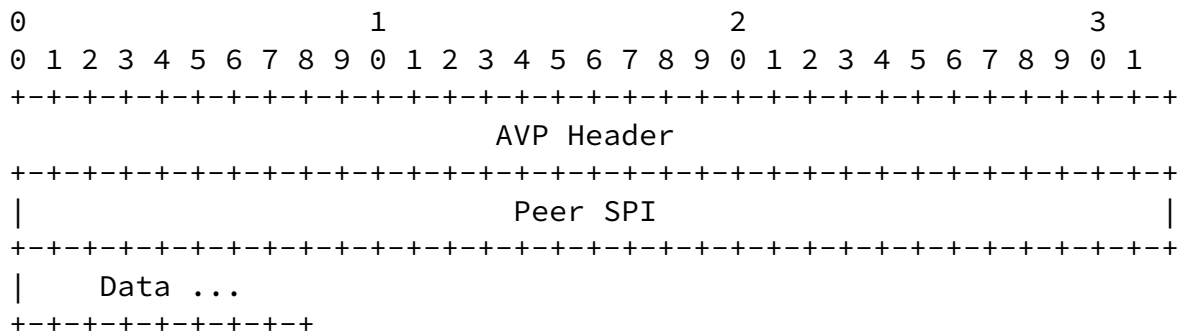
AAA SPI
A 32-bit opaque value, indicating the SPI that the target must use to determine the algorithm to use for recovering the encrypted security information.

Peer SPI
A 32-bit opaque value, which the target MUST use to index all the necessary information recovered from the security information after it is decoded.

Data
The data field contains the encrypted key used to create a Mobility Security Association between the mobility nodes.

5.2 Mobility Agent Session Key AVPs

The session keys AVPs destined for the Foreign and Home Agents are of type complex, and MUST have the AVP length field set to at least 13. The AVP has the following format:



AVP Code
326 for FA-MN Key, destined for Foreign Agent
328 for FA-HA Key, destined for Foreign Agent
329 for HA-FA Key, destined for Home Agent
332 for MN-HA Key, destined for Home Agent

Peer SPI
A 32-bit opaque value, which the target MUST use to index all the necessary information recovered from the security information after it is decoded.

Data

The data field contains the encrypted key used to create a Mobility Security Association between the mobility nodes.

5.3 FA-MN-Preferred-SPI AVP

The FA-Preferred-SPI AVP (AVP Code 324) is of type Integer32 and is sent in the AA-Mobile-Node-Request by the Foreign Agent. The AVP contains the SPI that the Foreign Agent would prefer to have assigned by the AAAH in the FA-to-MN-Key AVP.

5.4 FA-HA-Preferred-SPI AVP

The FA-Preferred-SPI AVP (AVP Code 324) is of type Integer32 and is sent in the AA-Mobile-Node-Request by the Foreign Agent. The AVP contains the SPI that the Foreign Agent would prefer to have assigned by the AAAH in the FA-to-HA-Key AVP.

6.0 Acknowledgements

The authors would like to thank Nenad Trifunovic, Tony Johansson and Pankaj Patel for their participation in the Document Reading Party. The authors would also like to thank the participants of TIA's TR45.6 working group for their valuable feedback.

7.0 IANA Considerations

The values for the Command Code AVP in section 2.0 were taken from the numbering space defined for Command-Code AVP in [1]. The numbers for the various AVPs defined in section 4.0 and 5.0 were taken from the AVP numbering space defined in [1]. The Result-Code AVP values defined in section 3.0 were taken from the Result-Code AVP numbering space defined in [1]. The numbering for the AVP, Command Codes and Result Codes MUST NOT conflict with values specified in [1], or any other DIAMETER extension.

8.0 Security Considerations

This specification describes the DIAMETER extension necessary to authenticate and authorize a Mobile IP Mobile Node. The authentication algorithm used is dependent upon the transforms available by the Mobile IP protocol, and [5]. This specification also defines a method by which the home DIAMETER server can create and distribute short-lived session keys to be used to authenticate Mobile IP registration messages. The keys are distributed in an encrypted format through the DIAMETER protocol, and SHOULD be encrypted using the methods defined in [9].

9.0 References

[1] P. Calhoun, A. Rubens, H. Akhtar, E. Guttman, "DIAMETER Base Protocol", draft-calhoun-diameter-11.txt (work in progress), December 1999.

[2] Calhoun, Zorn, Pan, Akhtar, "DIAMETER Framework", draft-calhoun-diameter-framework-05.txt (work in progress), December 1999.

[3] S. Glass, S. Jacobs, C. Perkins, "Mobile IP Authentication, Authorization, and Accounting Requirements", draft-ietf-mobileip- aaa-reqs-01.txt (work in progress), October 1999.

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

[5] C. Perkins, P. Calhoun, "Mobile IP Challenge/Response Extensions", draft-ietf-mobileip-challenge-06.txt (work in progress), October 1999.

[6] B. Aboba, M. Beadles "The Network Access Identifier." RFC 2486.

January 1999.

[7] B. Aboba, G. Zorn, "Criteria for Evaluating Roaming Protocols", RFC 2477, January 1999.

[8] P. Calhoun, C. Perkins, "Mobile IP Network Address Identifier Extension", draft-ietf-mobileip-mn-nai-05.txt (work in progress), October 1999.

[9] P. Calhoun, W. Bulley, S. Farrell, "DIAMETER Strong Security Extensions", draft-calhoun-diameter-strong-security-00.txt (work in progress), December 1999.

[10] Kent, Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

[11] S. Bradner, "Key words for use in RFCs to Indicate Requirement

Levels", BCP 14, RFC 2119, March 1997.
[12] J. Arkko, P. Calhoun, P. Patel, G. Zorn, "DIAMETER Accounting Extension", draft-calhoun-diameter-accounting-02.txt (work in progress), December 1999.
[13] H. Krawczyk, M. Bellare, and R. Cannetti. HMAC: Keyed-Hashing for Message Authentication. RFC 2104, February 1997.
[14] C. Perkins, Editor. IP Mobility Support. RFC 2002, October 1996.
[15] C. Perkins, P. Calhoun, "AAA Registration Keys for Mobile IP", draft-calhoun-mobileip-aaa-keys-00.txt (work in progress), October 1999.
[16] T. Hiller et al., "Cdma2000 Wireless Data Requirements for AAA", draft-hiller-cdma2000-AAA-00.txt (work in progress), October 1999.

10.0 Authors' Addresses

Questions about this memo can be directed to:

Pat R. Calhoun
Network and Security Research Center, Sun Labs
Sun Microsystems, Inc.
15 Network Circle
Menlo Park, California, 94025
USA

Phone: 1-650-786-7733
Fax: 1-650-786-6445
E-mail: pcalhoun@eng.sun.com

Charles E. Perkins
Nokia Research Center
313 Fairchild Drive
Mountain View, California 94043
USA

Phone: +1 650-625-2986
  Fax: +1 650-691-2170
E-Mail: charliep@iprg.nokia.com

11.0 Full Copyright Statement