AAA Working Group
Internet-Draft
Category: Standards Track
<draft-ietf-aaa-diameter-mobileip-01.txt>

Pat R. Calhoun
Sun Laboratories, Inc.
Charles E. Perkins
Nokia Research Center
March 2001

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

Mobile IP, as defined in [4], defines a method that allows a Mobile Node to change its point of attachment to the Internet with minimal service disruption. Mobile IP does not provide any specific support for mobility across disparate administrative domains, and therefore does not specify how usage can be accounted for, which has limited the applicability of Mobile IP in a IPv4 commercial deployment. The Mobile IP protocol [4] requires that mobile nodes have static home agent and home addresses, which is not desirable in a commercial network. Recent specification [8] allows a mobile node to use its NAI instead of its home address, which better accommodates current administrative practice.

This document specifies Extension 4 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. Diameter nodes conforming to this specification MUST include an Extension-Id AVP with a value of four in the Device-Reboot-Ind Command [1]. 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 Diameter functions that allow the AAA server to act as a Key Distribution Center (KDC), whereby dynamic registration keys are created and distributed to the mobility entities for the purposes of securing Mobile IP Registration messages.

As with the Diameter base protocol, AAA servers implementing the Mobile IP extension can process users' identities supplied in a Network Access Identifier (NAI) format [6], which is used for Diameter message routing purposes. Mobile nodes include their NAI in Registration messages, as defined in [8]. The use of the NAI is consistent with the roaming model defined by the ROAMOPS Working Group [7].

The Diameter Mobile-IP Extension meets the requirements specified in [3, 16]. Later subsections in this introductory section provide some examples and message flows of the Mobile IP and Diameter messages that occur when a Mobile Node requests service in a foreign network. In this document, the role of the "attendant" [3] is performed by the foreign agent for the Mobile-IP Extension, and these terms will be used interchangeably.

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, the foreign agent 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 for possible inclusion as Diameter AVPs. The AMR message is then forwarded to the local Diameter server, known as the AAA-Foreign, or AAAF.

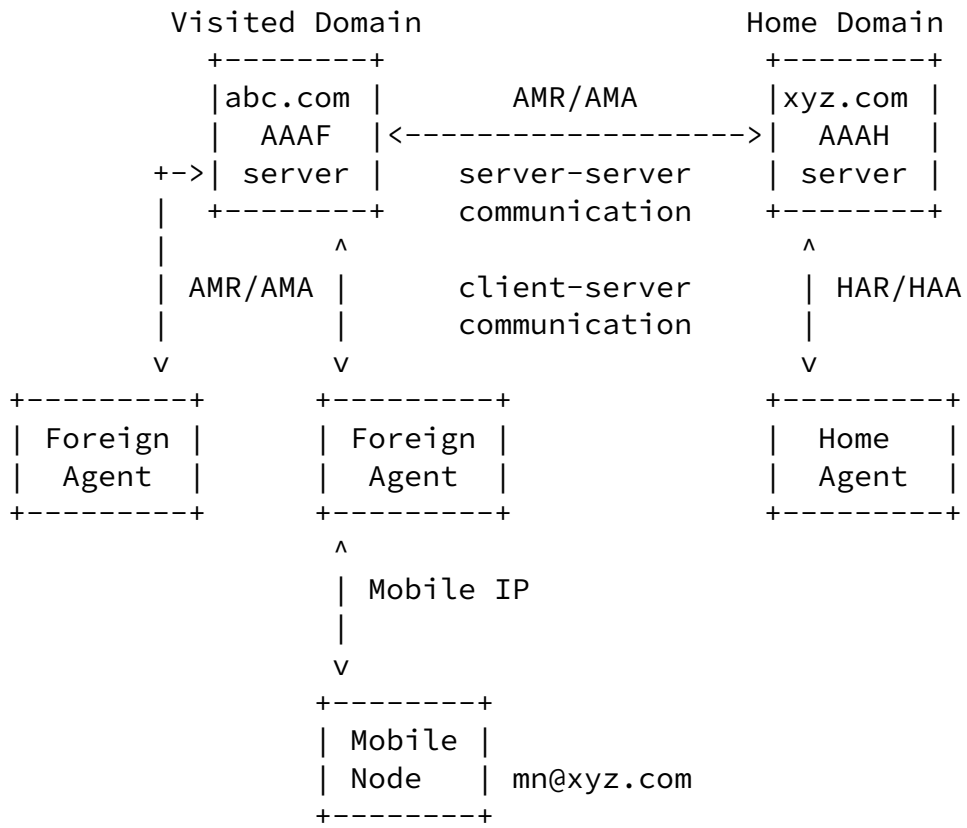


Figure 1: Inter-Domain Mobility

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 shows an example in which a mobile node (mn@xyz.com) requests service from a foreign provider (abc.com). The request received by the AAAF is forwarded to xyz.com's AAAH server.

Figure 2 shows the message flows involved when the attendant (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 AAA services every time a Registration Request is received from the mobile, but rather only when the prior authorization from the AAAH expires. The expiration time of the authorization (and registration keys, if allocated by the AAA server) is communicated through the Authorization-Lifetime AVP in the AA-Mobile-Node-Answer (AMA, see section 2.2) from the AAAH.

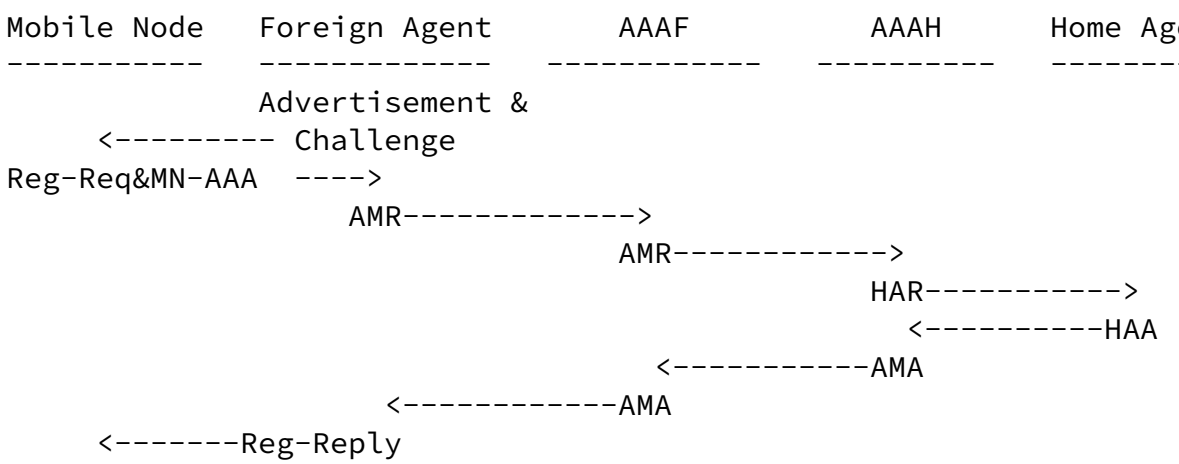


Figure 2: Mobile IP/Diameter Message Exchange

The foreign agent (as shown in Figure 2) MAY provide a challenge, which gives it direct control over the replay protection in the Mobile IP registration process, as described in [5]. The mobile node includes the Challenge and MN-AAA authentication extension to enable authorization by AAAH. If the authentication data supplied in the MN-AAA extension is invalid, AAAH returns the response (AMA) with the Result-Code AVP set to DIAMETER_ERROR_AUTH_FAILURE (see section 3.0).

If the Mobile Node was successfully authenticated, the AAAH checks for the MIP-Home-Agent-Address AVP. If one was specified, the AAAH checks that the address is that of a known Home Agent, and one that the Mobile Node is allowed to request. If no Home Agent was specified, and if the MIP-Feature-Vector has the Home-Agent-Requested flag set, and if allowed by policy in the home domain, the AAAH SHOULD allocate a home agent 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 the scope of this specification.

If AAAH does not know the address of the home agent (perhaps because it will be allocated by AAAF within the visited domain as described in section 1.3), then AAAH sends an AMA message back to AAAF which does not contain a MIP-Reg-Reply AVP.

Otherwise, if the home agent address is known, the AAAH then sends a Home-Agent-MIP-Request (HAR), which contains the Mobile IP Registration Request message data encapsulated in the MIP-Reg-Request AVP, to the assigned or requested Home Agent. The AAAH MAY allocate a home address for the mobile node, and include it in a MIP-Mobile-Node-Address AVP within the HAR, or else leave this allocation responsibility for the Home Agent.

Upon receipt of the HAR, the Home Agent first processes the Diameter message. If the HAR is invalid, a HAA is returned with the Result-Code AVP set to DIAMETER_ERROR_BAD_HAR (see section 3.0). Otherwise, the Home Agent processes the MIP-Reg-Req AVP and creates the Registration Reply, encapsulating it within the MIP-Reg-Reply AVP. If a home address is needed, the Home Agent MUST assign one and include the address in both the Registration Reply and within the MIP-Mobile-Node-Address AVP. The Diameter response is then forwarded

to the AAAH.

Upon receipt of the HAA, the AAAH sets the Command-Code field to AA-Mobile-Node-Answer (AMA) and forwards the message to the AAAF. The AAAH includes the MIP-Home-Agent-Address and MIP-Mobile-Node-Address AVPs in the AMA message, enabling appropriate firewall controls for the penetration of tunneled traffic between the Home Agent and the Mobile Node.

The AAAF is responsible for ensuring that the AMA message is properly forwarded to the correct foreign agent.

1.3 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 a foreign agent detects that the mobile node has a home agent address equal to 0.0.0.0 or 255.255.255.255 in the Registration Request message, it MUST add a MIP-Feature-Vector AVP with the Home-Agent-Requested flag set to one. If the home address address is equal to 255.255.255.255, then the foreign agent also MUST set the Home-Address-Allocatable-Only-in-Home-Domain flag equal to one.

When the AAAF receives a AMR message with the Home-Agent-Requested flag set to one, and the Home-Address-Allocatable-Only-in-Home-Domain flag equal to zero, AAAF MAY set the Foreign-Home-Agent-Available flag in the MIP-Feature-Vector AVP to inform the AAAH that it is willing and able to assign a Home Agent for the Mobile Node.

In the event that the mobile node requests a home agent in the foreign network, and the AAAF authorizes its use, the AAAF MUST set the Home-Agent-In-Foreign-Network bit in the MIP-Feature-Vector AVP. This could happen when the AAA request is sent to "extend" a mobile node's current session.

When the AAAH receives a AMR message, it first checks the authentication data supplied by the mobile node, according to the MIP-Reg-Req AVP and MIP-MN-AAA-Auth AVP, and determines whether to authorize the mobile node. If the AMR indicates that the AAAF has

offered to allocate a home agent for the mobile node, then the AAAH

must decide whether its local policy would allow the user to have a Home Agent in the foreign network. If so, and after checking authorization from the data in the AMR message, the AAAH sends the AMA message to the AAAF that does not contain the MIP-Home-Agent-Address.

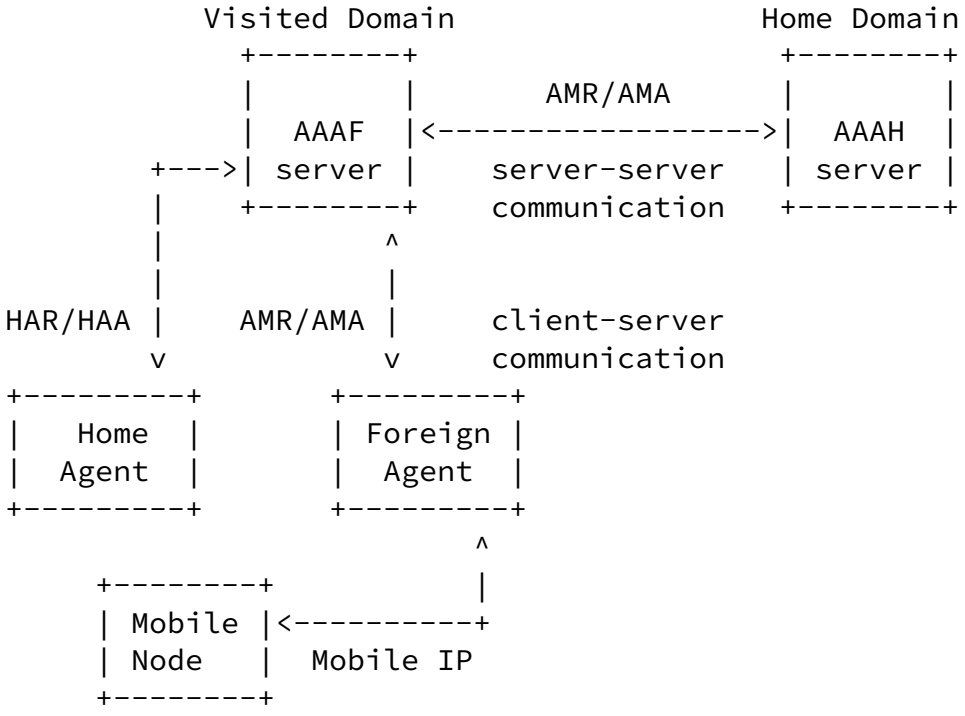


Figure 3: Home Agent allocated in Visited Domain

Upon receipt of a HAA from the Home Agent in the Visited Domain, with the Result-Code AVP indicating success, the AAAF MUST issue a HAI message to the AAAH. The HAI message MUST include the MIP-Home-Agent-Address and the MIP-Mobile-Node-Address AVPs.

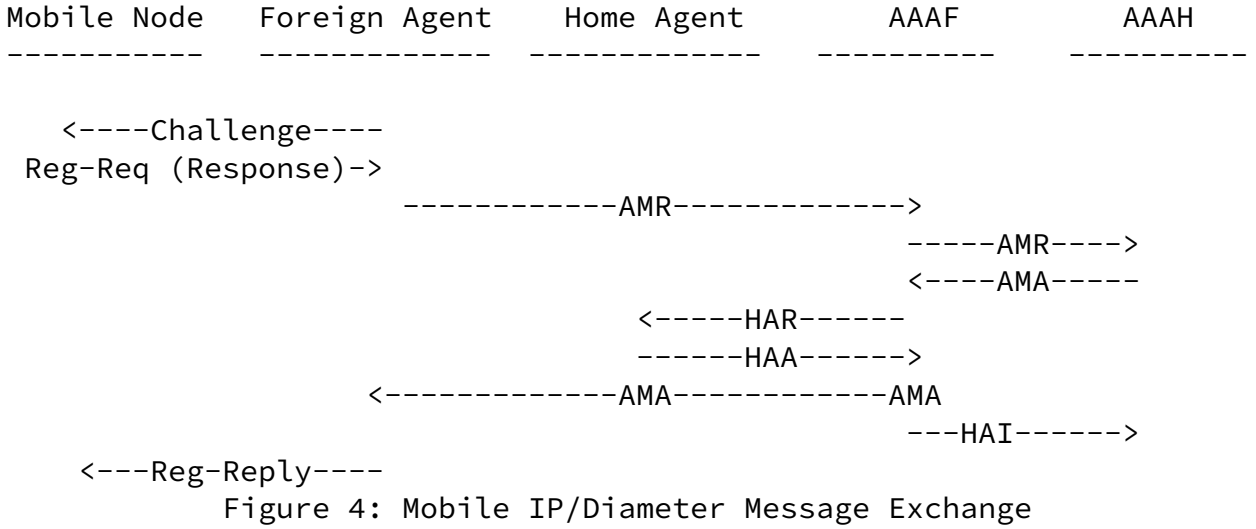


Figure 4: Mobile IP/Diameter Message Exchange

If the Mobile Node moves to another Foreign Network, it MAY either request to keep the same Home Agent within the old foreign network, or request to get a new one in the new foreign network. If the AAAH is willing to provide the requested service, the mobile node will have to interact with two AAAFs.

Figure 5 shows the message flows for a Mobile Node requesting to keep the Home Agent assigned in Foreign network 1 when it moves to foreign network 2. Upon reception of the AMR in Foreign network 2, the AAAF follows the procedures described earlier and forwards AMR to the Mobile Node's home network, i.e. its AAAH. If the Mobile Node was successfully authenticated the AAAH checks for the MIP-Home-Agent-Address and the MIP-Previous-FA-NAI AVPs. If a Home Agent was specified, and it belongs to a different domain than the Foreign Agent in the MIP-Previous-FA-NAI AVP, the AAAH MUST verify whether it will permit this type of the service to the Mobile Node.

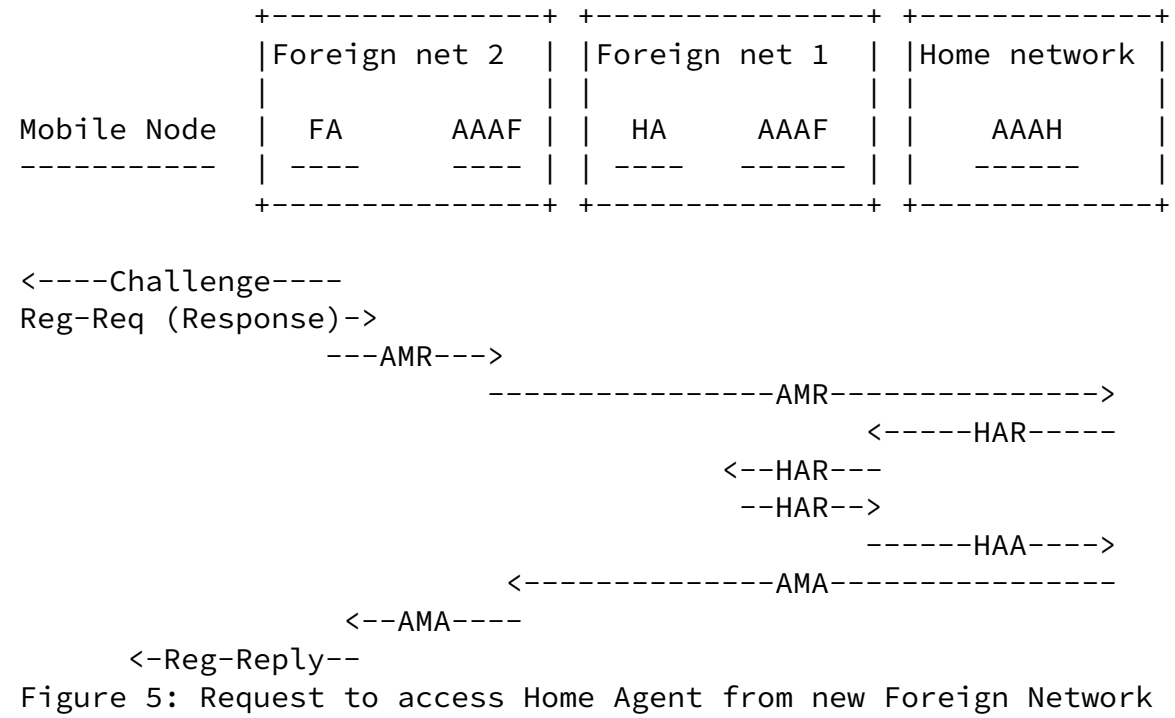


Figure 5: Request to access Home Agent from new Foreign Network

If the Mobile Node is allowed to keep the Home Agent the AAAH then sends a HAR, which contains the Mobile IP Registration Request message data encapsulated in the MIP-Reg-Request AVP and the MIP-Home-Agent-Address AVP with Home Agent address, the optional KDC session keys to the AAAF in foreign network 1. Upon reception the AAAF in foreign network 1 will forward the HAR to the Home Agent if its local policy allows such service. If the AAAF does not permit such service, it MUST return a DIAMETER_ERROR_NO_FOREIGN_HA_SERVICE.

When the AAAF receives a successful HAA, the AAAF will forward the HAA back to the AAAH. The HAA MUST include the MIP-Home-Agent-Address

and the MIP-Mobile-Node-Address AVPs. The AAAH will then send back an AMA to the AAAF in foreign network 2.

If the old Foreign Network does not permit the use of its Home Agent when the Mobile Node moves to a new foreign network, the Mobile Node MAY allocate a new Home Agent in its current network, as described above. However, when the AAAH receives such a request, it MUST send a Diameter Session-Termination-Indication message to the old AAAF, which will enable the old foreign network to release any resources, and will cause any necessary accounting messages.

[ed: Charlie would prefer that the AMA be sent directly from foreign net 1 to foreign net 2. This would optimize the signaling, and would reduce latency involved in the handoff. More work needed here]

1.4 Diameter Session Termination

A Foreign and Home Agent following this specification MAY expect their respective Diameter servers to 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 Session-Termination-Request (STR) [1] to their respective Diameter servers.

The Home Diameter server SHOULD only deallocate all resources after the STR is received from the Home Agent. This ensures that a Mobile Node that moves from one Foreign Agent to another (hand-off) does not cause the Home Diameter Server to free all resources for the Mobile Node. The Diameter Server is free to initiate the session termination at any time by issuing the Session-Termination-Ind (STI) [1].

2.0 Command-Code Values

This section defines Command-Code [1] values that MUST be supported by all Diameter implementations conforming to this specification. The following Command Codes are defined in this specification:

Command-Name	Abbreviation	Code	Section
AA-Mobile-Node-Answer	AMA	261	2.2
AA-Mobile-Node-Request	AMR	260	2.1
Home-Agent-Allocated-Ind	HAI	279	2.5
Home-Agent-MIP-Answer	HAA	263	2.4
Home-Agent-MIP-Request	HAR	262	2.3

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

The AA-Mobile-Node-Request (AMR), indicated by the Command-Code field set to 260, is sent by an attendant, acting as a Diameter client, to a server in order to request the authentication and authorization of a Mobile Node. The Foreign Agent uses information found in the Registration Request to construct the following AVPs that are to be included as part of the AMR:

home address (MIP-Mobile-Node-Address AVP),
home agent address (MIP-Home-Agent-Address AVP),
mobile node NAI (User-Name AVP [1]).

If the mobile node's home address is zero, the foreign agent MUST NOT include a MIP-Mobile-Node-Address AVP in the AMR. In this case, the AAAF MAY set the Foreign-Home-Agent-Available flag in the MIP-Feature-Vector AVP in the AMR message to indicate that it is willing to assign a Home Agent in the visited domain.

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

Message Format

```
<AA-Mobile-Node-Request> ::= < Diameter Header: 260 >
                             { Session-ID }
                             { Extension-Id }
                             { User-Name }
                             { Destination-Realm }
```

```
                                { Origin-FQDN }
                                { Origin-Realm }
                                { Authorization-Lifetime }
                                { MIP-Reg-Request }
                                { MIP-MN-AAA-Auth }
                                [ MIP-Mobile-Node-Address ]
                                [ MIP-Home-Agent-Address ]
                                [ MIP-Feature-Vector ]
                                [ MIP-FA-MN-Preferred-SPI ]
                                [ MIP-FA-HA-Preferred-SPI ]
                                [ MIP-Previous-FA-NAI ]
                                [ MIP-Previous-FA-Addr ]
                              * [ AVP ]
                              * [ Proxy-State ]
                              * [ Route-Record ]
                             0*1< Integrity-Check-Value >
```


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

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

The MIP-Home-Agent-Address AVP contains the Home Agent assigned to the Mobile Node, while the MIP-Mobile-Node-Address AVP contains the home address that was assigned.

The AMA message MUST contain the MIP-FA-to-HA-Key, MIP-FA-to-MN-Key and MIP-Reg-Reply AVPs if they were received by AAAH in the HAA message.

Message Format

```
   <AA-Mobile-Node-Answer> ::= < Diameter Header: 261 >
                               < Session-Id >
                               { Extension-Id }
                               { Session-Timeout }
                               { Authorization-Lifetime }
                               { Result-Code }
```

```
                                { Destination-Realm }
                                [ Error-Reporting-FQDN ]
                                [ Origin-FQDN ]
                                [ MIP-Reg-Reply ]
                                [ MIP-MN-to-HA-Key ]
                                [ MIP-FA-to-MN-Key ]
                                [ MIP-FA-to-HA-Key ]
                                [ MIP-Home-Agent-Address ]
                                [ MIP-Mobile-Node-Address ]
                              * [ AVP ]
                              * [ Proxy-State ]
                              * [ Route-Record ]
                             0*1< Integrity-Check-Value >
```

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

The Home-Agent-MIP-Request (HAR), indicated by the Command-Code field set to 262, is sent by the AAA to the Home Agent. If the Home Agent is to be assigned in a foreign network, the HAR is issued by AAAF. If the HAR message does not include a MIP-Mobile-Node-Address AVP, and the Registration Request has 0.0.0.0 for the home address, and the HAR is successfully processed, the Home Agent MUST allocate one

such address to the mobile node. If the home agent's local AAA server allocates the mobile node's home address, it MUST include the assigned address in an MIP-Mobile-Node-Address AVP.

If a AAAF receives a HAR that does not include the MIP-Reg-Reply AVP, then a Home Agent MUST be assigned in the foreign network.

When registration keys are requested for use by the mobile node (see section 5.0), the AAAH MUST create them and include them in the HAR message. When a Foreign-Home registration key is requested, it will be created and distributed by the AAA server in the same domain as the home agent.

Message Format

```
   <Home-Agent-MIP-Request> ::= < Diameter Header: 262 >
                                < Session-Id >
                                { Extension-Id }
```

```
                                  { Session-Timeout }
                                  { Authorization-Lifetime }
                                  { MIP-Reg-Request }
                                  { Origin-FQDN }
                                  { Origin-Realm }
                                  { User-Name }
                                  { Destination-Realm }
                                  [ MIP-MN-to-HA-Key ]
                                  [ MIP-MN-to-FA-Key ]
                                  [ MIP-HA-to-MN-Key ]
                                  [ MIP-HA-to-FA-Key ]
                                  [ MIP-FA-to-MN-Key ]
                                  [ MIP-FA-to-HA-Key ]
                                  [ MIP-Mobile-Node-Address ]
                                * [ AVP ]
                                * [ Proxy-State ]
                                * [ Route-Record ]
                               0*1< Integrity-Check-Value >
```

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

The Home-Agent-MIP-Answer (HAA), indicated by the Command-Code field set to 263, is sent by the Home Agent to its local AAA server in response to a Home-Agent-MIP-Request. If the home agent allocated a home address for the Mobile Node, the address MUST be included in the MIP-Mobile-Node-Address AVP. The Result-Code AVP MAY contain one of the values defined in section 3.0 instead of the values defined in [1].

Message Format

```
   <Home-Agent-MIP-Answer> ::= < Diameter Header: 263 >
                               < Session-Id >
                               { Extension-Id }
                               { Session-Timeout }
                               { Authorization-Lifetime }
                               { Result-Code }
                               { Origin-FQDN }
                               { Origin-Realm }
                               { Destination-Realm }
```

```
                                  [ Error-Reporting-FQDN ]
                                  [ MIP-Reg-Reply ]
                                  [ MIP-Home-Agent-Address ]
                                  [ MIP-Mobile-Node-Address ]
                                  [ MIP-FA-to-MN-Key ]
                                  [ MIP-FA-to-HA-Key ]
                                * [ AVP ]
                                * [ Proxy-State ]
                                * [ Route-Record ]
                               0*1< Integrity-Check-Value >
```

2.5 Home-Agent-Allocated-Ind (HAI) Command

The Home-Agent-Allocated-Ind (HAI), indicated by the Command-Code field set to 279, is sent by the AAAF to the AAAH upon receipt of a successful HAA when the Home Agent was assigned in the visited network. The HAI MUST include the MIP-Home-Agent-Address and MIP-Mobile-Node-Address AVPs.

Message Format

```
   <Home-Agent-Allocated-Ind> ::= < Diameter Header: 279 >
                                  < Session-Id >
                                  { Extension-Id }
                                  { Origin-FQDN }
                                  { Origin-Realm }
                                  { Session-Timeout }
                                  { Authorization-Lifetime }
                                  { Destination-Realm }
                                  { Destination-FQDN }
                                  [ MIP-Home-Agent-Address ]
                                  [ MIP-Mobile-Node-Address ]
                                * [ AVP ]
                                * [ Proxy-State ]
                                * [ Route-Record ]
                               0*1< Integrity-Check-Value >
```


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.

3.1 Hop-by-Hop Failures

Proxies receiving messages with the Result-Code AVP set to an error within the Hop-by-Hop failure category SHOULD attempt to take some local action to correct the error. If no local action can be taken to correct the problem, the error MUST be forwarded towards the originator of the message.

DIAMETER_ERROR_BAD_KEY 6009
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 6010
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_AUTH_FAILURE 6011
This error code is used by AAAH to inform AAAF that the authentication data in the MN-AAA authentication extension is invalid.

DIAMETER_ERROR_MIP_REPLY_FAILURE 6012
This error code is used by the Home Agent when processing of the Registration Request has failed.

DIAMETER_ERROR_BAD_HAR-day 6013
This error code is used by HA to inform the AAA server that the Home-Agent-Request (HAR) message could not be processed correctly.

DIAMETER_ERROR_NO_FOREIGN_HA_SERVICE 6014
This error is used by the AAAF to inform the AAAH that allocation of a Home Agent in the Foreign Agent is not permitted at this time.

4.0 Mandatory AVPs

The following table describes the Diameter AVPs defined in the Mobile IP extension, their AVP Code values, types, possible flag values and

whether the AVP MAY be encrypted.

Attribute Name	AVP Code	Section Defined	Value Type	AVP Flag rules: MUST	MAY	SHLD NOT	MUST NOT	MAY Encr
MIP-Auth-Input-Data-Length	338	4.8.2	Unsigned32	M	P		V	Y
MIP-Authenticator-Length	339	4.8.3	Unsigned32	M	P		V	Y
MIP-Authenticator-Offset	340	4.8.4	Unsigned32	M	P		V	Y
MIP-Feature-Vector	337	4.7	Unsigned32	M	P		V	Y
MIP-Home-Agent-Address	334	4.4	Address	M	P		V	Y
MIP-MN-AAA-Auth	322	4.8	Grouped	M	P		V	Y
MIP-MN-AAA-SPI	341	4.8.1	Unsigned32	M	P		V	Y
MIP-Mobile-Node-Address	333	4.3	Address	M	P		V	Y
MIP-Previous-FA-Addr	336	4.6	Address	M	P		V	Y
MIP-Previous-FA-FQDN	335	4.5	OctetString	M	P		V	Y
MIP-Reg-Request	320	4.1	OctetString	M	P		V	Y
MIP-Reg-Reply	321	4.2	OctetString	M	P		V	Y

4.1 MIP-Reg-Request AVP

The MIP-Reg-Request AVP (AVP Code 320) is of type OctetString and contains the Mobile IP Registration Request [4] sent by the Mobile Node to the Foreign Agent.

4.2 MIP-Reg-Reply AVP

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

4.3 MIP-Mobile-Node-Address AVP

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

contains the Mobile Node's Home Address.

4.4 MIP-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.

4.5 MIP-Previous-FA-NAI AVP

The MIP-Previous-FA-FQDN AVP (AVP Code 335) is of type OctetString and contains the Fully Qualified Domain Name of the Mobile Node's old Foreign Agent, encoded in the UTF-8 [18] format. The Mobile Node MAY include this information in the Registration Request when it moves its point of attachment to a new foreign agent under the same administrative domain as the old FA.

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 registration key that was previously allocated to the old Foreign Agent for the Mobile Node. The registration key is identified through the use of the MIP-Mobile-Node-Address AVP, which MUST be present if this extension is present.

In many circumstances, 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 (AAAH).

4.6 MIP-Previous-FA-Addr AVP

The MIP-Previous-FA-Addr AVP (AVP Code 336) is of type Address and contains the IP Address of the Mobile Node's old Foreign Agent. The Mobile Node MAY include this information in the Previous Foreign Agent Notification Extension to the Mobile IP Registration Request when it moves its point of attachment to a new foreign agent.

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 registration key that was previously allocated to the old Foreign Agent for the Mobile Node. The registration key is

identified through the use of the MIP-Mobile-Node-Address AVP, which MUST be present if this extension is present.

In many circumstances, 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 (AAAH).

4.7 MIP-Feature-Vector AVP

The MIP-Feature-Vector AVP (AVP Code 337) is of type Unsigned32 and is added with flag values set by the Foreign Agent or by the AAAF owned by the same administrative domain as the Foreign Agent. The Foreign Agent SHOULD include MIP-Feature-Vector AVP within the AMR message it sends to the AAAF.

Flag values currently defined include:

1	Mobile-Node-Home-Address-Requested
2	Home-Address-Allocatable-Only-in-Home-Domain
4	Home-Agent-Requested
8	Foreign-Home-Agent-Available
16	MN-HA-Key-Request
32	MN-FA-Key-Request
64	FA-HA-Key-Request
128	Home-Agent-In-Foreign-Network

The flags are set according to the following rules.

If the mobile node includes a valid home address (i.e., not equal to 0.0.0.0 or 255.255.255.255) in its Registration Request, the Foreign Agent zeroes the Mobile-Node-Home-Address-Requested flag in the MIP-Feature-Vector AVP.

If the mobile node sets the home address field equal to 0.0.0.0 in its Registration Request, the Foreign Agent sets the Mobile-Node-Home-Address-Requested flag to one, and zeroes the Home-Address-Allocatable-Only-in-Home-Domain flag in the MIP-Feature-Vector AVP.

If the mobile node sets the home address field equal to 255.255.255.255 in its Registration Request, the Foreign Agent sets both the Mobile-Node-Home-Address-Requested flag and the Home-

Address-Allocatable-Only-in-Home-Domain flag to one in the MIP-Feature-Vector AVP.

If the mobile node sets the home agent field equal to 0.0.0.0 in its Registration Request, the Foreign Agent sets the Home-Agent-Requested flag to one in the MIP-Feature-Vector AVP.

Whenever the Foreign Agent sets either the Home-Address-Requested flag or the Home-Agent-Request flag to one, it MUST set the MN-HA-Key-Request flag to one. The MN-HA-Key-Request flag is also set to one if the mobile node includes a Generalized MN-HA Key Request [15] extension, with the subtype set to AAA.

If the mobile node includes a Generalized MN-FA Key Request [15] extension with the AAA subtype in its Registration Request, the

Foreign Agent sets the MN-FA-Key-Request flag to one in the MIP-Feature-Vector AVP.

If the mobile node requests a home agent in the foreign network by setting the home address field to all ones, and the AAAF authorizes the request, the AAAF MUST set the Home-Agent-In-Foreign-Network bit to one.

If the Foreign Agent's local policy allows it to receive AAA Session Keys, and it does not have any existing keys with the Home Agent, it MAY set the FA-HA-Key-Request flag.

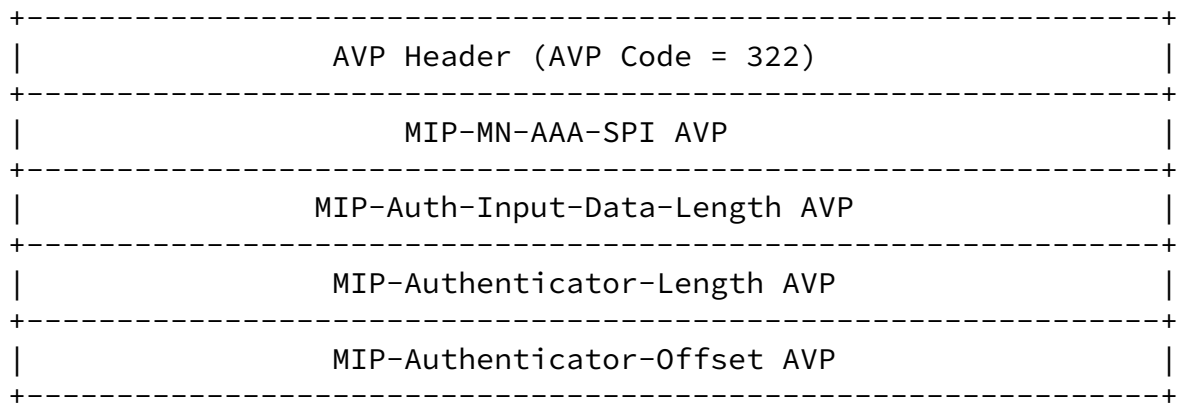
The Foreign Agent MUST NOT set the Foreign-Home-Agent-Available, and Home-Agent-In-Foreign-Network flag to one.

When the AAAF receives the AMR message, it MUST first verify that the sender was an authorized Foreign Agent. The AAAF then takes any actions indicated by the settings of the MIP-Feature-Vector AVP flags. The AAAF then MAY set additional flags. Only the AAAF may set the Foreign-Home-Agent-Available flag to one. This is done according to local administrative policy. When the AAAF has finished setting additional flags according to its local policy, then the AAAF transmits the AMR with the possibly modified MIP-Feature-Vector AVP to the AAAH.

4.8 MIP-MN-AAA-Auth AVP

The MN-AAA-Auth AVP (AVP Code 322) is of type Grouped and contains some ancillary data to simplify processing of the authentication data in the Mobile IP Registration Request [4] by the target AAA server. Its value has the following ABNF grammar:

```
MIP-MN-AAA-Auth   = ma-spi authinlen authlen authoffset
   ma-spi          = ; MIP-MN-AAA-SPI, See Section 4.8.1
   authinlen       = ; MIP-Auth-Input-Data-Length, /
                     ; See Section 4.8.2
   authlen         = ; MIP-Authenticator-Length, /
                     ; See Section 4.8.3
   authoffset      = ; MIP-Authenticator-Offset, /
                     ; See Section 4.8.4
```

4.8.1 MIP-MN-AAA-SPI AVP

The MIP-MN-AAA-SPI AVP (AVP Code 341) is of type Unsigned32 and indicates the algorithm by which the targeted AAA server (AAAH) should attempt to validate the Authenticator computed by the mobile node over the Registration Request data.

4.8.2 MIP-Auth-Input-Data-Length AVP

The MIP-Auth-Input-Data-Length AVP (AVP Code 338) is of type Unsigned32 and contains the length, in bytes, of the Registration Request data (data portion of MIP-Reg-Request AVP) that should be used as input to the algorithm (indicated by the MN-AAA-SPI AVP) used to determine whether the Authenticator Data supplied by the Mobile Node is valid.

4.8.3 MIP-Authenticator-Length AVP

The MIP-Authenticator-Length AVP (AVP Code 339) is of type Unsigned32 and contains the length of the authenticator to be validated by the targeted AAA server (i.e., AAAH).

4.8.4 MIP-Authenticator-Offset AVP

The MIP-Authenticator-Offset AVP (AVP Code 340) is of type Unsigned32 and contains the offset into the Registration Request Data, of the authenticator to be validated by the targeted AAA server (i.e., AAAH).

5.0 Key Distribution Center

The mobile node and mobility agents use registration keys to compute authentication extensions applied to registration messages, as defined in [4]: Mobile-Foreign, Foreign-Home and Mobile-Home. If registration keys are requested the AAA server(s) MUST create them after the Mobile Node is successfully authenticated and authorized.

The keys destined for each mobility entity are encrypted either using the secret shared with the entity [1], or via its public key [9], as indicated by the relevant security association. If the AAAH does not communicate directly with the Foreign Agent, those keys are encrypted using the security association shared with the AAAF. The Authorization-Lifetime AVP contains the number of seconds before

registration keys destined for the Home Agent and/or Foreign Agent expire. Absence or the AVP, or a value of zero indicates infinity (no timeout).

AAA support for key distribution departs slightly from the existing SPI usage, as described in [4]. The SPI values are used as key identifiers, meaning that each registration key has its own SPI value; nodes that share a key also share an SPI. If no preferred SPI value is indicated the registration keys the foreign agent needs, the AAA server MAY generate SPI values for the Mobility Agents as opposed to the receiver choosing its own SPI value. For example, suppose a Mobile Node and a Foreign Agent share a key that was generatied by AAAH with a corresponding SPI value of 37,496. All Mobile-Foreign Authentication extensions will be computed by either entity (in this example) using the shared key and MUST include the SPI value of 37,496.

Once the registration keys have been distributed, subsequent Mobile IP registrations need not invoke the AAA infrastructure until the keys expire. These registrations MUST include the Mobile-Home authentication extension. In addition, subsequent registrations MUST also include Mobile-Foreign authentication extension if the Mobile-Foreign key was generated and distributed by AAA; similarly for subsequent use of the Foreign-Home authentication extensions.

Each registration key that is generated by AAA will generally be distributed to two parties; for instance, a Mobile-Foreign key goes to both a mobile node and a foreign agent. The methods by which the key is encoded will depend upon the security associations available to the AAA server and each recipient of the key. These methods will often be different for the two recipients, so that the registration key under consideration has to be encoded twice.

See sections 6.1 and 6.2 for details about the format of the AVPs used to distribute the registration keys.

5.1 Distributing the Mobile-Home Registration Key

If the mobile node does not have a Mobile-Home registration key, then the AAAH is likely to be the only entity trusted that is available to the mobile node. Thus, the AAAH has to generate the Mobile-Home

registration key, and encode it for eventual consumption by the mobile node and home agent.

If the home agent is in the home domain, then AAAH can directly encode the Mobile-Home registration key into a MIP-HA-to-MN-Key AVP and include that AVP in the HAR message for delivery to the home agent.

If, on the other hand, the home agent is to be allocated in the visited domain, the AAAH does not transmit the HAR to the home agent. Instead, AAAH has to include the MIP-HA-to-MN-Key AVP in the AMR message which it sends to the AAAF. In this latter case, the Mobile-Home registration key is encoded into MIP-HA-to-MN-Key AVP using the method indicated by the security association between the AAAF and the AAAH. When the AAAF receives the AMR, it first allocates a home agent, and then creates a HAR message for that home agent. After the AAAF decodes the registration key, it re-encodes the key into a new MIP-HA-to-MN-Key AVP which is to be included within the HAR message.

The AAAH also has to arrange for the key to be delivered to the mobile node. Unfortunately, the AAA server only knows about Diameter messages and AVPs, and the mobile node only knows about Mobile IP messages and extensions[4]. The AAA server has to rely on a mobility agent (that also understands Diameter) to transfer the key into a Mobile IP MN-HA Key Reply extension to the Registration Reply message. This mobility agent (actually, the mobile node's home agent) can format the Reply message and extensions correctly for eventual delivery to the mobile node, by way of an AMA message sent to the appropriate foreign agent in the visited domain. That foreign agent will use the information in the MIP-Reg-Reply AVP to create a Mobile IP Registration Reply message, containing the MN-HA Key Reply extension, and transmit it to the mobile node.

For this purpose, AAAH encodes the Mobile-Home registration key into a MIP-MN-to-HA-Key AVP, using its security association with the mobile node. If the home agent is in the home domain, AAAH puts the MIP-MN-to-HA-Key AVP into the HAR message. Otherwise, the AAAH puts the MIP-MN-to-HA-Key AVP into the AMR message which will be sent back to AAAF. When AAAF creates the HAR message for the home agent in the visited domain, and decodes the registration key in the MIP-HA-to-MN-Key AVP from the AVP received from AAAH, AAAF then recodes the registration key into a new MIP-HA-to-MN-Key AVP which is to be

included as part of the HAR message. In either case, the home agent creates a Registration Reply with the MN-HA Key Reply extension, and formats the reply data into a MIP-Reg-Rep-AVP for delivery in a HAA message to the AAA server. After the HAA message is parsed by the AAA server, the AMA message containing the MIP-Reg-Rep AVP will eventually be received by the attendant (i.e., the foreign agent). The foreign agent can then use that AVP to recreate a Registration Reply message, containing the MN-HA Key Reply extension, for delivery to the mobile node.

In summary, the AAAH generates the Mobile-Home registration key and encodes it into a MIP-HA-to-MN-Key AVP and a MIP-MN-to-HA-Key AVP. These AVPs are delivered to a home agent by including them in a HAR message sent from either AAAH or AAAF. The home agent decodes the key for its own use. The home agent also copies the encoded registration key from the MIP-MN-to-HA-Key AVP into a MN-HA Key Reply extension appended to the Mobile IP Registration Reply message. This Registration Reply message MUST also include the Mobile-Home authentication extension, created using the newly allocated Mobile-Home registration key. The home agent then encodes the Registration Reply message and extensions into a MIP-Reg-Reply AVP included as part of the HAA message to be sent back to the AAA server.

5.2 Distributing the Mobile-Foreign Registration Key

The Mobile-Foreign registration key is also generated by AAAH (upon request), so that it can be encoded into a MIP-MN-to-FA-Key AVP and copied by the home agent into a "General MN-FA Key Reply Extension" extension [15] to the Mobile IP Registration Reply message. Since the foreign agent is in the same administrative domain as AAAF, the sequence of events for handling the MIP-FA-to-MN-Key AVP is similar to the way the MIP-HA-to-MN-Key AVP is handled when the home agent is allocated in the visited domain. Most of the other considerations for distributing the Mobile-Foreign registration key are also similar.

When the home agent is in the home domain, AAAH includes the MIP-MN-to-FA-Key AVP in the HAR message. Otherwise, AAAH includes the MIP-MN-to-FA-Key AVP in the AMR message to be sent back to the AAAF. In the latter case, AAAF sends the HAR message to the (newly allocated) home agent.

In either case, the home agent decodes the key, and recodes it into the key reply extension to the Mobile IP registration message. Then the home agent (as before) copies the Registration Reply message into the MIP-Reg-Reply AVP and places the result (possibly also containing the MN-HA Key Reply extension as in section 1.4.1) into the HAA message to be sent back to the AAA server. The home agent MUST also

append a Foreign-Home authentication extension to the Registration Reply message, using the newly allocated Foreign-Home registration key.

When the home agent is in the home domain, AAAH receives the HAA, and then includes the MIP-Reg-Reply AVP in the AMA message to be sent to AAAF. Otherwise, AAAF receives the HAA, and inserts it into an AMA message to be sent to the foreign agent.

AAAH also has to make the Mobile-Foreign registration key available to AAAF. It does this by encoding the key into a MIP-FA-to-MN-Key AVP, using its security association with AAAF, and placing the results in the AMA. Then the AAAF decodes the registration key, and recodes it into a newly formulated MIP-FA-to-MN-Key AVP which is to be sent to the foreign agent in the AMA message containing the MIP-Reg-Reply AVP from the home agent.

5.3 Distributing the Foreign-Home Registration Key

If the home agent is in the home domain, then AAAH has to generate the Foreign-Home registration key. Otherwise, it is generated by AAAF.

In the former case, AAAH encodes the registration key into a MIP-HA-to-FA-Key AVP and includes that AVP as part of the HAR message sent to the home agent, and waits for the HAA message to be returned.

Whether or not AAAH sends the HAR message, it also further encodes the same registration key and puts it into a MIP-FA-to-HA-Key AVP included as part of the AMA message to be transmitted back to AAAF.

If the home agent is in the visited domain, the AAAH includes the MIP-HA-to-FA-Key AVP as part of the AMR also. In this case, AAAF has to decode the Foreign-Home registration key and include it as part of the HAR message to be sent to the (newly allocated) home agent.

In either case, AAAF sends a AMA message, containing a MIP-Reg-Reply AVP and the MIP-FA-to-HA-Key AVP, to the foreign agent. First, the foreign agent recreates the necessary Registration Reply message from the AMA message. Then the foreign agent recovers the Foreign-Home registration key, using its security association with AAAF. The

foreign agent MUST then use this key to create a Mobile-Foreign authentication extension to the Registration Reply message.

5.4 Key Distribution Example

Figure 6 provides an example of subsequent Mobile IP message exchange, assuming that AAAH distributed registration keys for all three MN-FA, FA-HA and HA-MN authentication extensions.

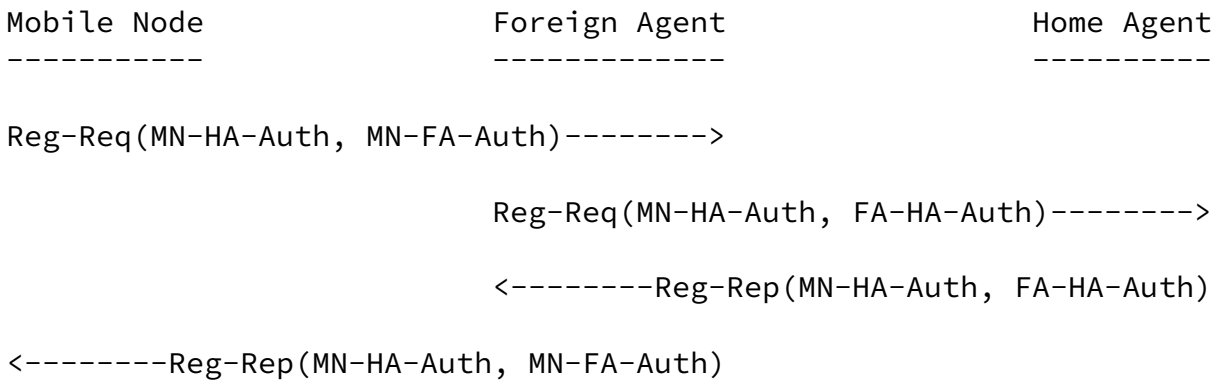


Figure 6: Mobile IP Message Exchange

6.0 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 (Mobile-Home, Mobile-Foreign, and Foreign-Home), can be dynamically created by the AAAH. This requires that the AAAH create Mobile-IP Registration Keys, and that these keys be distributed to the three mobile entities, via the Diameter Protocol. AAA servers supporting the Diameter Mobile IP Extension MUST implement the KDC AVPs defined in this document. In other words, AAA servers MUST be able to create three registration keys: the Mobile-Home, Mobile-Foreign, and Foreign-Home keys.

Each of these keys is encrypted two different ways, as needed for each key recipient. The mobile node and home agent registration keys are sent to the Home Agent, while the foreign agent's keys are sent to the foreign agent via the AAAF. This leads to six different AVPs,

since there are three keys, and each one has to be able to be encrypted in two different ways.

The names of the KDC AVPs indicate the two entities sharing the security association defined by the encrypted key material; the intended receiver of the AVP is the first named entity. So, for instance, the MIP-MN-to-HA-Key AVP contains the Mobile-Home key encrypted in a way that allows it to be recovered by the mobile node.

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

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

				AVP Flag rules				
Attribute Name	AVP Code	Section Defined	Value Type	MUST	MAY	SHLD NOT	MUST NOT	MAY Encr
MIP-FA-to-MN-Key	326	6.2.1	Grouped	M	P		V	Y
MIP-FA-to-HA-Key	328	6.2.2	Grouped	M	P		V	Y
MIP-HA-to-FA-Key	329	6.2.3	Grouped	M	P		V	Y
MIP-HA-to-MN-Key	332	6.2.4	Grouped	M	P		V	Y
MIP-MN-to-FA-Key	325	6.1.1	OctetString	M	P		V	Y
MIP-MN-to-HA-Key	331	6.1.2	OctetString	M	P		V	Y
MIP-Peer-SPI	342	6.2.5	Unsigned32	M	P		V	Y
MIP-FA-MN-Preferred-SPI	324	6.3	Unsigned32	M	P		V	Y
MIP-FA-HA-Preferred-SPI	327	6.4	Unsigned32	M	P		V	Y
MIP-Session-Key	343	6.2.6	OctetString	M	P		V	Y

6.1 Mobile Node Registration Keys

When the AAAH acts as a Key Distribution Center, and it is determined that keying material is to be created for Mobile Nodes, the AAAH

creates the keys and encodes them in the MIP-MN-to-FA-Key and MIP-MN-to-HA-Key AVPs as opaque data. The actual format of the AVP value is described in [15], and would contains the data immediately following the Mobile IP extension header.

The Mobile IP key described in [15] refers to the AAA SPI, which MUST be set to the value the AAAH shares with the Mobile Node. The Key Lifetime field is set to the same value as the one found in the Authorization-Lifetime AVP.

6.1.1 MIP-MN-to-FA-Key AVP

The MIP-MN-to-FA-Key AVP (AVP Code 325) is of type OctetString, and contains the Keying material described in the "Unsolicited MN-FA Key from AAA Subtype" in [15]. The FA SPI field of the data structure in [15] MUST be set to the same value as the Peer-SPI AVP within the FA-to-MN-Key AVP.

6.1.2 MIP-MN-to-HA-Key AVP

The MIP-MN-to-HA-Key AVP (AVP Code 331) is of type OctetString, and contains the Keying material described in the "Unsolicited MN-HA Key from AAA Subtype" in [15]. The HA SPI field of the data structure in [15] MUST be set to the same value as the Peer-SPI AVP within the HA-to-MN-Key AVP.

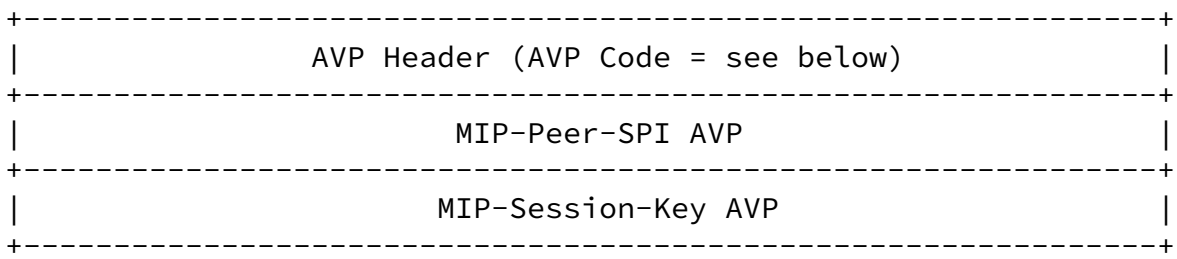
6.2 Mobility Agent Session Keys

The Mobility Agent session keys are the keys created by a Diameter server, which it distributes to Foreign and Home Agents, acting as Diameter clients. These session keys, described below, are of type Grouped, and therefore their value have the following ABNF format:

```
Mobility Agent Session Key AVP   = Peer-SPI Session-Key
   Peer-SPI        = ; MIP-Peer-SPI, See Section 6.2.5
   Session-Key     = ; MIP-Session-Key, See Section 6.2.6
```

The MIP-Peer-SPI AVP contains the Security Parameter Index, which the

Mobility Agent MUST use to refer to the Key contained in the MIP-Session-Key AVP.



6.2.1 MIP-FA-to-MN-Key AVP

The MIP-FA-to-MN-Key AVP (AVP Code 326) is of type Grouped, and contains the Foreign Agent's session key, which it shares with the Mobile Node. Its format is described in Section 6.2.

6.2.2 MIP-FA-to-HA-Key AVP

The MIP-FA-to-HA-Key AVP (AVP Code 328) is of type Grouped, and contains the Foreign Agent's session key, which it shares with the Home Agent. Its format is described in Section 6.2.

6.2.3 MIP-HA-to-FA-Key AVP

The MIP-HA-to-FA-Key AVP (AVP Code 329) is of type Grouped, and contains the Home Agent's session key, which it shares with the Foreign Agent. Its format is described in Section 6.2.

6.2.4 MIP-HA-to-MN-Key AVP

The MIP-HA-to-MN-Key AVP (AVP Code 332) is of type Grouped, and contains the Home Agent's session key, which it shares with the Mobile Node. Its format is described in Section 6.2.

6.2.5 MIP-Peer-SPI AVP

The MIP-Peer-SPI AVP (AVP Code 342) is of type Unsigned32, and contains the Security Parameter Index to use to reference the key in the associated MIP-Session-Key AVP.

6.2.6 MIP-Session-Key AVP

The MIP-Session-Key AVP (AVP Code 343) is of type OctetString and contains the Session Key to be used between two Mobile IP entities.

6.3 MIP-FA-MN-Preferred-SPI AVP

The MIP-FA-MN-Preferred-SPI AVP (AVP Code 324) is of type Unsigned32 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 MIP-FA-to-MN-Key AVP.

6.4 MIP-FA-HA-Preferred-SPI AVP

The MIP-FA-HA-Preferred-SPI AVP (AVP Code 327) is of type Unsigned32 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 MIP-FA-to-HA-Key AVP.

7.0 Accounting Considerations

This section contains the AVPs defined in this extension that are to be present in the Accounting-Request and optionally in the Accounting-Answer messages, defined in [12].

```
   <Service-Specific AVPs> ::= { MIP-Mobile-Node-Address }
```



```
                                { MIP-Home-Agent-Address }
                                [ MIP-Previous-FA-NAI ]
                                [ MIP-Previous-FA-Address ]
                                [ MIP-Feature-Vector ]
```

8.0 Interactions with Resource Management

The Resource Management extension [17] provides the ability for a Diameter node to query a peer for session state information. The document states that service-specific extensions are responsible for specifying what AVPs are to be present in the Resource-Token [17] AVP.

In addition to the AVPs listed in [17], the Resource-Token with the Extension-Id AVP set to four (4) MUST include the MIP-Mobile-Node-Address and the MIP-Home-Agent-Address AVP.

9.0 AVP Table

The following table presents the AVPs defined in this document, and specifies in which Diameter messages they MAY, or MAY NOT be present. Note that AVPs that can only be present within a Grouped AVP are not represented in this table.

The table uses the following 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.

	Command-Code				
Attribute Name	AMR	AMA	HAR	HAA	HAI
Authorization-Lifetime	1	1	1	1	1
Destination-FQDN	0+	1	0+	1	1
Destination-Realm	1	1	1	1	1
Error-Reporting-FQDN	0	0+	0	0+	0
Extension-Id	1	1	1	1	1
Integrity-Check-Value	0-1	0-1	0-1	0-1	0-1
MIP-FA-to-HA-Key	0	0-1	0-1	0-1	0
MIP-FA-to-MN-Key	0	0-1	0-1	0-1	0
MIP-Feature-Vector	0-1	0	0	0	0
MIP-FA-HA-Preferred-SPI	0-1	0	0	0	0
MIP-FA-MN-Preferred-SPI	0-1	0	0	0	0
MIP-HA-to-FA-Key	0	0	0-1	0	0
MIP-HA-to-MN-Key	0	0	0-1	0	0
MIP-Home-Agent-Address	0-1	0-1	0	0-1	0-1
MIP-MN-AAA-Auth	1	0	0	0	0
MIP-MN-to-FA-Key	0	0	0-1	0	0
MIP-MN-to-HA-Key	0	0-1	0-1	0	0
MIP-Mobile-Node-Address	0-1	0-1	0-1	0-1	0-1
MIP-Previous-FA-Address	0-1	0	0	0	0
MIP-Previous-FA-NAI	0-1	0	0	0	0
MIP-Reg-Reply	0	0-1	0	0-1	0
MIP-Reg-Request	1	0	1	0	0
Origin-FQDN	1	1	1	1	1
Origin-Realm	1	1	1	1	1
Proxy-State	0+	0+	0+	0+	0+
Result-Code	0	1	0	1	0
Route-Record	0+	0+	0+	0+	0+
Session-Id	1	1	1	1	1
Session-Timeout	0	1	1	1	1
User-Name	1	0	1	0	0

10.0 Acknowledgements

The authors would like to thank Nenad Trifunovic and Pankaj Patel for their participation in the Document Reading Party, to Erik Guttman for his very useful proposed text, and to Tony Johansson for the proposed text AND being in the doc reading party. The authors would also like to thank the participants of 3GPP2's TSG-P working group for their valuable feedback.

11.0 IANA Considerations

The command codes defined in Section 2.0 are values taken from the Command-Code [1] address space and extended in [9], [12] and [14]. IANA should record the values as defined in Section 2.0.

The Result-Code values defined in Section 3.0 are error codes as defined in [1] and extended in [9], [12] and [14]. They correspond to error values specific to the Mobile IP extension. IANA should record the values as defined in Section 3.0.

The AVPs defined in sections 4.0 and 6.0 were allocated from the AVP numbering space defined in [1], and extended in [9], [12] and [14]. IANA should record the values as defined in Sections 4.0 and 6.0.

12.0 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 registration 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].

13.0 References

[1] P. Calhoun, A. Rubens, H. Akhtar, E. Guttman, "Diameter Base Protocol", draft-ietf-aaa-diameter-01.txt, IETF work in progress, March 2001.

[2] Calhoun, Zorn, Pan, Akhtar, "Diameter Framework", draft-ietf-aaa- diameter-framework-01.txt, IETF work in progress, March 2001.

[3] S. Glass, S. Jacobs, C. Perkins, "Mobile IP Authentication, Authorization, and Accounting Requirements". RFC 2977. October 2000.

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

[5] C. Perkins, P. Calhoun, "Mobile IP Challenge/Response Extensions". RFC 3012. November 2000.

[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", RFC 2794, March 2000.

[9] P. Calhoun, W. Bulley, S. Farrell, "Diameter Strong Security Extensions", draft-calhoun-diameter-strong-crypto-06.txt, IETF work in progress, February 2001.

[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-ietf-aaa-diameter-accounting-01.txt, IETF work in progress, March 2001.

[13] H. Krawczyk, M. Bellare, and R. Cannetti. HMAC: Keyed-Hashing for Message Authentication. RFC 2104, February 1997.

[14] P. Calhoun, W. Bulley, A. Rubens, J. Haag, "Diameter NASREQ Extension", draft-ietf-aaa-diameter-nasreq-01.txt, IETF work in progress, March 2001.

[15] C. Perkins, P. Calhoun, "AAA Registration Keys for Mobile IP", draft-calhoun-mobileip-aaa-key-03.txt, IETF work in progress, January 2001.

[16] T. Hiller and al, "CDMA2000 Wireless Data Requirements for AAA", draft-hiller-cdma2000-aaa-01.txt, IETF work in progress, June

2000.

[17] P. Calhoun, "Diameter Resource Management", draft-calhoun-diameter-res-mgmt-06.txt, IETF Work in Progress, February 2001.

[18] F. Yergeau, "UTF-8, a transformation format of ISO 10646", RFC 2279, January 1998.

14.0 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: +1 650-625-2502
E-Mail: charliep@iprg.nokia.com

15.0 Full Copyright Statement

16.0 Expiration Date

This memo is filed as <draft-ietf-aaa-diameter-mobileip-01.txt> and expires in August 2001.