AAA Working Group
Internet-Draft
Category: Standards Track
<draft-ietf-aaa-diameter-mobileip-05.txt>

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

Diameter Mobile IPv4 Application

Status of this Memo

Abstract

This document specifies a Diameter application that allows a Diameter server to authenticate, authorize and collect accounting information for Mobile IPv4 services rendered to a mobile node. Combined with the Inter-Domain capability of the base protocol, this application allows mobile nodes to receive service from foreign service providers. Diameter Accounting messages 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 specification as defined in [4] recommends mobile nodes to have a static home address and a home agent. However this may not be always possible in certain deployment scenarios. Recent developments in areas that impact IP mobility in the IETF allow Mobile IP [4] to work just as well when mobile nodes do not have a static home agent and home address. 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 Application 4 to the Diameter base protocol [1] that allows a Diameter server to authenticate, authorize and collect accounting information for Mobile IPv4 services rendered to a mobile node. This application MUST NOT be used in conjunction with the Mobile IPv6 protocol.

Combined with the Inter-Domain capability of the base protocol, this application allows mobile nodes to receive service from foreign service providers. The Diameter Accounting messages 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 application 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 Application 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 either the home agents (for co-located mobile nodes) or foreign agents for the Mobile-IP Application, 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.

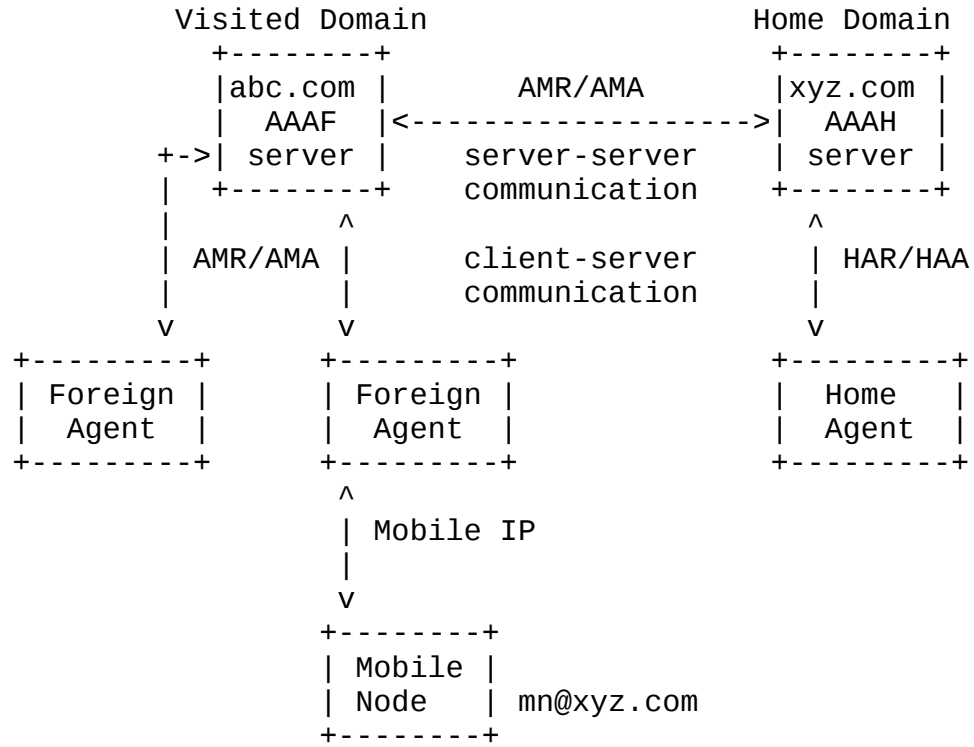

Figure 1: Inter-Domain Mobility

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 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.

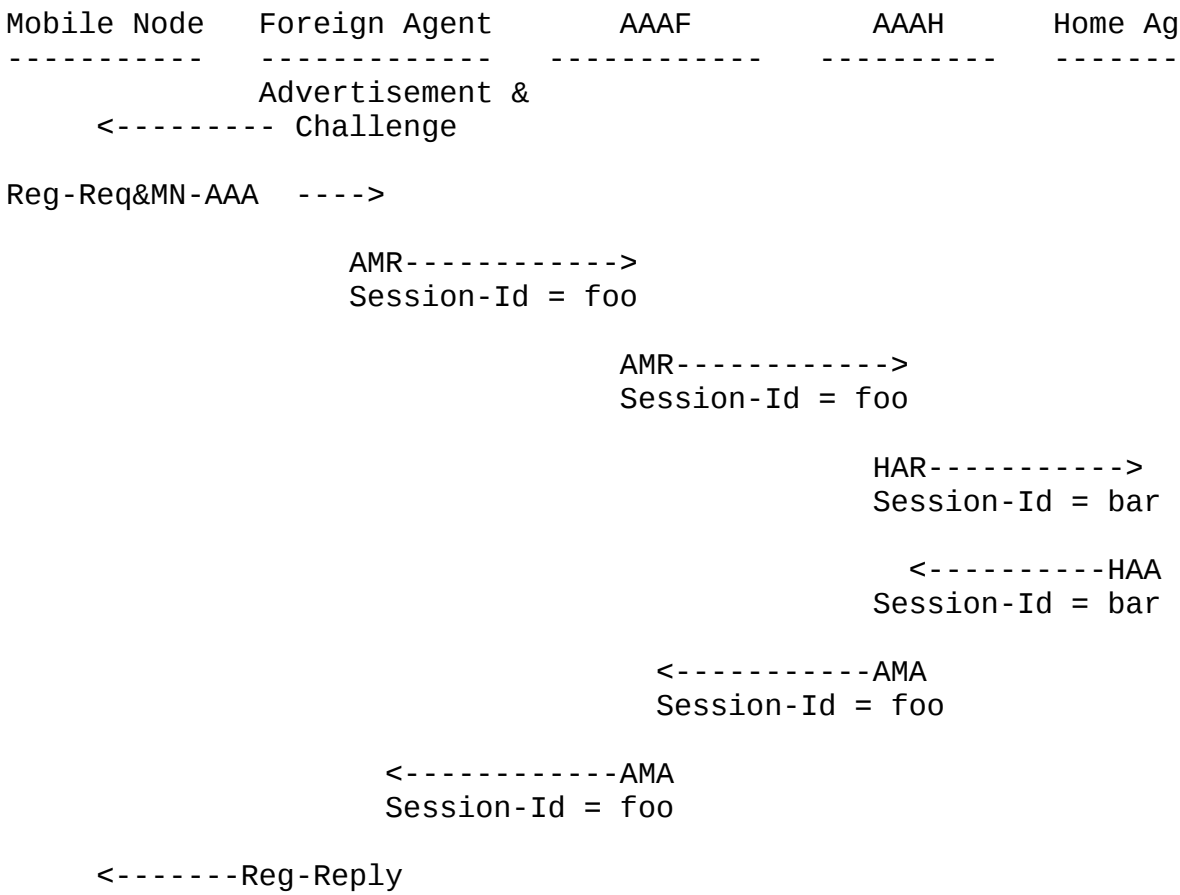

Figure 2: Mobile IP/Diameter Message Exchange

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).

In the event that the AMR generated by the FA is for a session that has was previously authorized by the AAAH, it MUST include the Destination-Host AVP, with the identity of the AAAH. The AAAH's identity can be retrieved from the Origin-Host AVP in the last AMA received for the session.

If the Mobile Node was successfully authenticated, the AAAH checks if the Home Agent was located in the foreign domain, by checking the Home-Agent-In-Foreign-Network flag of the MIP-Feature-Vector AVP. If the flag is enabled, then the Home Agent is located in the foreign domain then AAAH sends an HAR message to AAAF which contains a MIP-Reg-Request AVP.

If the Home Agent was not located in the foreign domain, 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, and the Home Agent's identity is included in the Destination-Host AVP. 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.

The AAAH then sends an 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.

For new sessions, the AAAH MUST create an accounting session identifier, which is added to the Accounting-Multi-Session-Id AVP in the HAR message sent to the home agent.

During the creation of the HAR, the AAAH MUST use a different session identifier than the one used in the AMR/AMA (see figure 2). Of course, the AAAH MUST use the same session identifier for all HARs initiated on behalf of a given mobile node's session. A mobile node's session is identified via its identity in the User-Name AVP, the MIP-Mobile-Node-Address and MIP-Home-Agent-Address AVPs. This is necessary in order to allow the session state machine, defined in the base protocol [1], to be used unmodified with this application.

Therefore, an STR from a foreign agent would free the session from the foreign agent, but not the one towards the home agent (see figure 3).

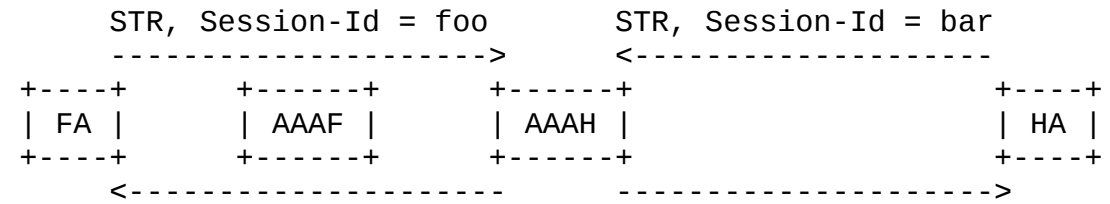

Figure 3: Session Termination and Session Identifiers

Upon receipt of the HAR, the Home Agent first processes the Diameter message. The Home Agent processes the MIP-Reg-Request 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 Accounting-Multi-Session-Id AVP in the HAR MUST be included in the HAA, which is then forwarded to the AAAH.

Upon receipt of the HAA, the AAAH creates the AA-Mobile-Node-Answer (AMA) message, includes the Accounting-Multi-Session-Id that was present in the HAA, and the MIP-Home-Agent-Address, 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 Support for Mobile IP Handoffs

Given the nature of Mobile IP, a mobile node MAY receive service from many foreign agents during a period of time. However, the Home Domain should not view these handoffs as different sessions, since this could affect billing systems. Furthermore, many foreign agents do not communicate, which makes it quite difficult for AAA information to be exchanged between these entities. Therefore, it MUST be assumed that a foreign agent is not aware that a registration request from a mobile node has been previously authorized.

The first registration request from a mobile node will therefore cause an AMR to be sent to its AAAF. The AMR will include a new session identifier, and MAY even be sent to a different AAAF in the visited network. It is also quite likely that the AMR will be

received by a different AAAH.

Since the new AAAH in the home network MAY not have access to the session identifier that was used by the old AAAH, it is necessary for the resulting HAR received by the HA to be identified as a continuation of an existing session. If the HA receives an HAR for a mobile node, with a new session identifier, and the HA can guarantee that this request is to extend service for an existing service, then the HA MUST be able to modify its internal session state information to reflect the new AAAH and session identifier. The HA MUST also issue an STR message with the old session identifier to the AAAH it was communicating with when using the old session identifier.

It is necessary for accounting records to have some commonality across handoffs in order for correlation to occur. Therefore, in the event that a home agent receives an HAR with a different Accounting-Multi-Session-id AVP (and obviously a different Session-Id AVP), the home agent MUST send an HAA with the Accounting-Multi-Session-Id AVP that was received by the AAAH in the first HAR for the mobile's session. This modified Accounting-Multi-Session-Id AVP will be returned to the foreign agent by the AAAH in the AMA. Both the foreign and home agents MUST include the Accounting-Multi-Session-Id in the accounting messages.

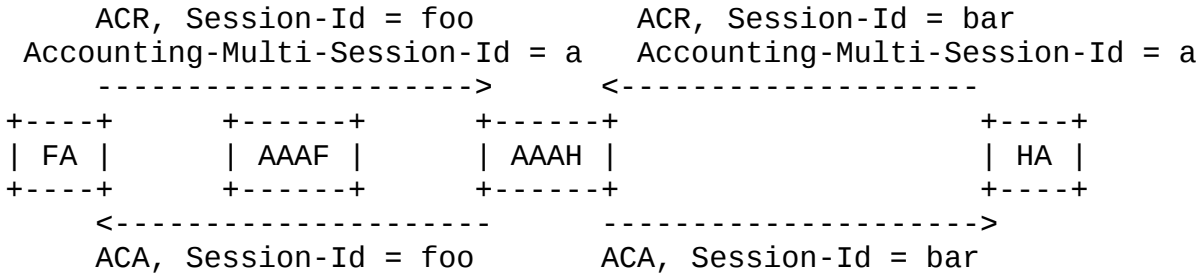

Figure 4: Accounting messages w/ Mobile IP Application

1.4 Allocation of Home Agent in Foreign Network

The Diameter Mobile IP application 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 agent 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. If the home agent address is set to 0.0.0.0, the foreign agent MUST set the Home-Address-Allocatable-Only-in-Home-Domain flag equal to zero.

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-Request 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 HAR message to the AAAF that does not contain the MIP-Home-Agent-Address. The AAAF MUST allocate a Home Agent, if one has not already been assigned to the Mobile Node, and the AAAF forwards the HAR message to the Home Agent.

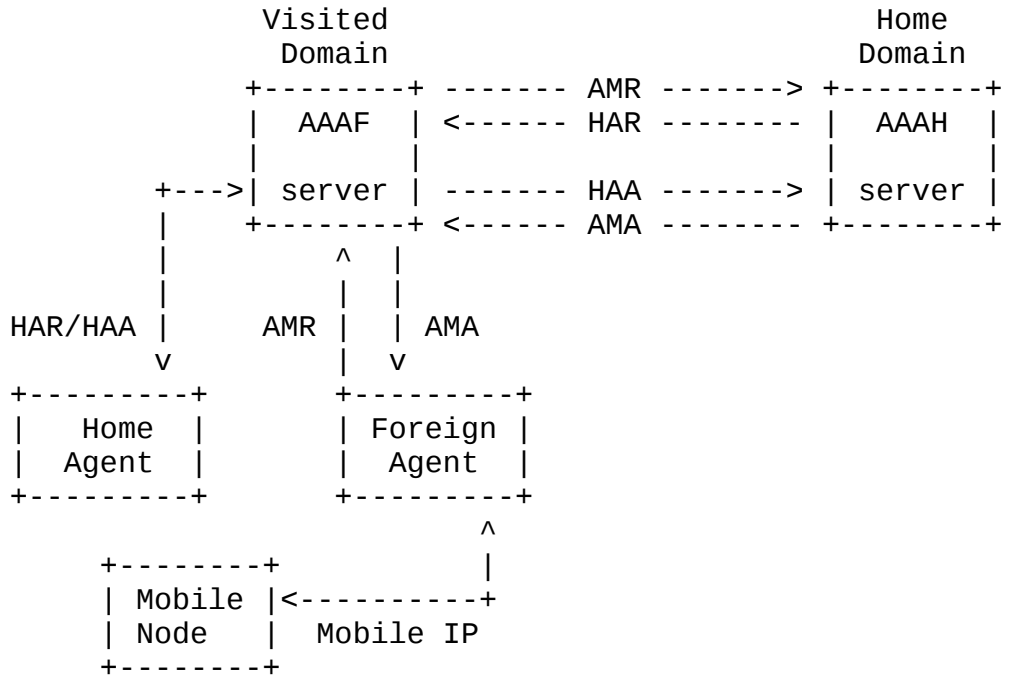

Figure 5: Home Agent allocated in Visited Domain

Upon receipt of a HAA from the Home Agent in the Visited Domain, with

the Result-Code AVP indicating success, the AAAF forwards the HAA to the AAAH in the home domain. The AMA is then constructed, and issued to the AAAF, and finally to the FA. The HAA and AMA MUST include the MIP-Home-Agent-Address and the MIP-Mobile-Node-Address AVPs.

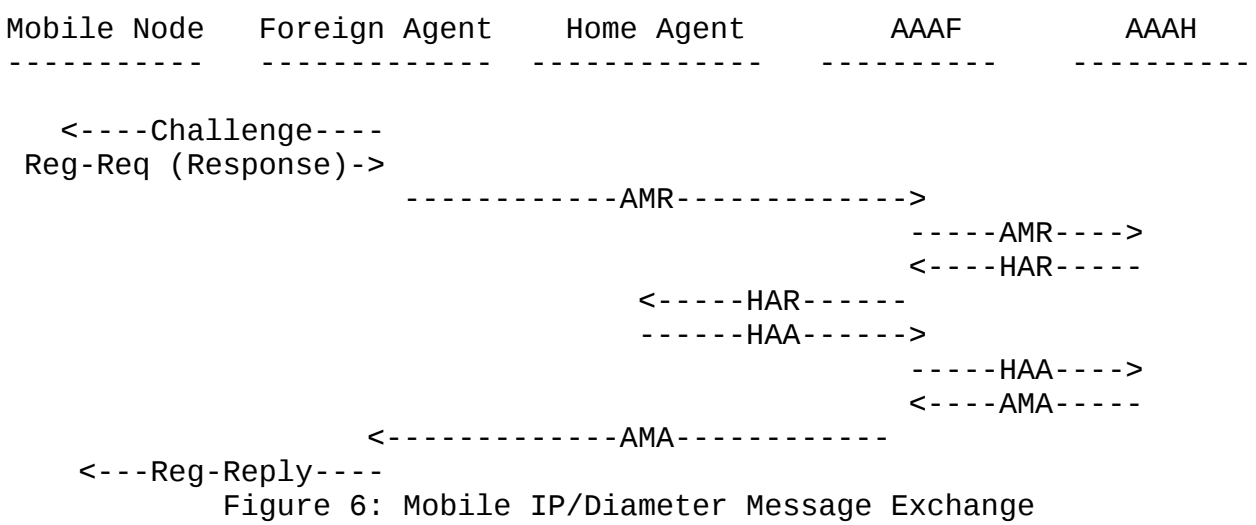

Figure 6: Mobile IP/Diameter Message Exchange

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 7 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 Origin-Host and the MIP-Previous-FA-Host AVPs. If a AAAH deduces that the Mobile Node has moved to a new domain, it must check whether the Mobile can still use the previously assigned Home Agent.

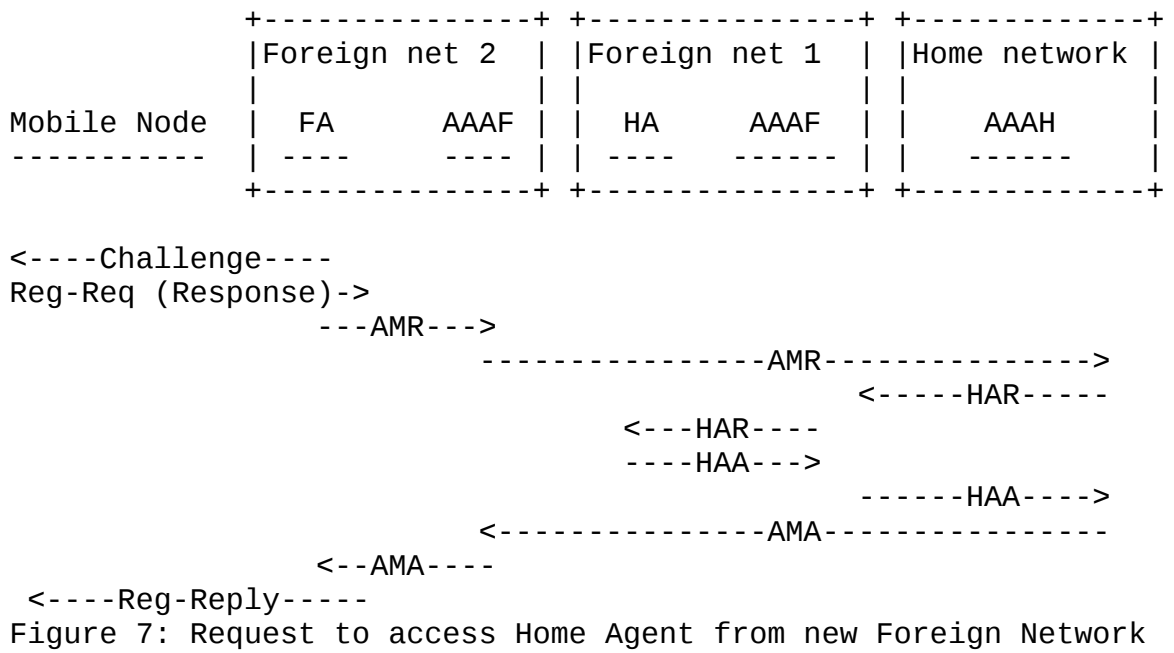

Figure 7: Request to access Home Agent from new Foreign Network

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, as well as any 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 AAAH or AAAF MUST return an AMA with the Result-Code AVP set to DIAMETER_ERROR_HA_NOT_AVAILABLE. Upon receipt of this error, the Foreign Agent MUST issue a Mobile IP Registration Reply to the Mobile Node with an appropriate error. The Mobile Node MAY attempt to request that a new Home Agent and Address be allocated. When the AAAH transmits such an error, it MUST issue a Diameter Abort-Session-Request message to the AAAF overseeing the Home Agent to enable it to release any resources.

1.5 Co-located Mobile Node

In the event that a Mobile Node registers with the Home Agent as a co-located Mobile Node, there is no Foreign Agent involved. Therefore, when the Home Agent receives the Registration Request, an AMR message is sent to the local AAAH server, with the Co-Located-Mobile-Node bit set in the MIP-Feature-Vector AVP.

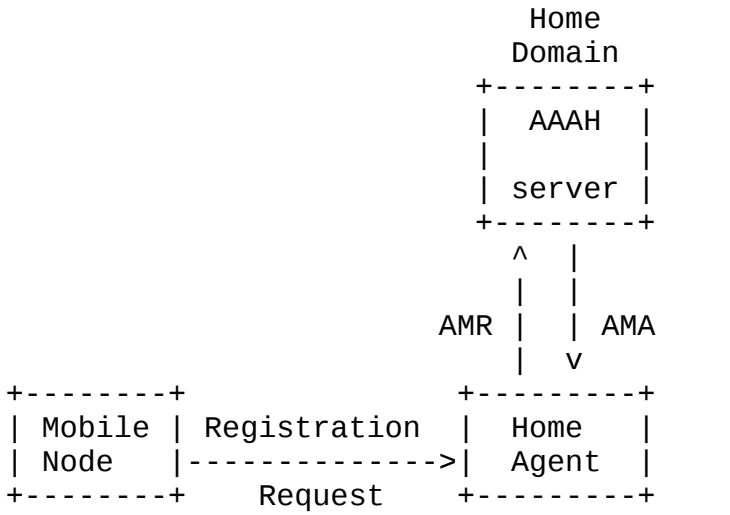

Figure 8: Co-located Mobile Node

If the MN-HA-Key-Requested bit was set in the AMR message from the Home Agent, the Home Agent and Mobile Node's session keys would be present in the AMA message.

1.6 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.

In the event that the AAAF wishes to terminate a session, its Abort-Session-Request (ASR) [1] message SHOULD be sent to the FA. Similarly, the AAAH SHOULD send its message to the Home Agent.

1.7 Advertising application support

Diameter nodes conforming to this specification MAY advertise support by including the value of four (4) in the Auth-Application-Id or the Acct-Application-Id AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer command [1].

1.8 Fast Handoff support

This application requires that foreign agents issue an AMR upon receipt of the first registration message from a mobile node, regardless of the fact that the mobile node MAY have been previously authorized to another foreign agent.

The Mobile IP Working Group is currently investigating fast handoff proposals, and the Seamoby WG is looking at creating a protocol that would allow AAA state information to be exchange between foreign agents during a handoff. These proposals MAY allow future enhancements to the Diameter protocol, in order to reduce the amount of Diameter exchanges required during a handoff.

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	260	2.2
AA-Mobile-Node-Request	AMR	260	2.1
Home-Agent-MIP-Answer	HAA	262	2.4
Home-Agent-MIP-Request	HAR	262	2.3

2.1 AA-Mobile-Node-Request

The AA-Mobile-Node-Request (AMR), indicated by the Command-Code field set to 260 and the 'R' bit set in the Command Flags field, 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 (or Home Agent in the case of a co-located Mobile Node) 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]).
MN-HA Key Request (MIP-Feature-Vector AVP)
MN-FA Key Request (MIP-Feature-Vector AVP)
MN-AAA Authentication Extension
Foreign Agent Challenge Extension

If the mobile node's home address is zero, the foreign or home agent MUST NOT include a MIP-Mobile-Node-Address AVP in the AMR. If the home agent address is zero or all ones, the MIP-Home-Agent-Address AVP MUST NOT be present in the AMR.

If a Foreign Agent is used in a visited network, 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-Host 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 User-Name AVP.

Message Format

```
<AA-Mobile-Node-Request> ::= < Diameter Header: 260, REQUEST >
                             < Session-ID >
                             { Auth-Application-Id }
                             { User-Name }
                             { Destination-Realm }
                             { Origin-Host }
                             { Origin-Realm }
                             { MIP-Reg-Request }
                             { MIP-MN-AAA-Auth }
                             [ MIP-Mobile-Node-Address ]
                             [ MIP-Home-Agent-Address ]
                             [ MIP-Feature-Vector ]
                             [ Authorization-Lifetime ]
                             [ MIP-FA-MN-Preferred-SPI ]
                             [ MIP-FA-HA-Preferred-SPI ]
                             [ MIP-Previous-FA-Host ]
                             [ MIP-Previous-FA-Addr ]
                             [ MIP-FA-Challenge ]
                             [ Destination-Host ]
                             [ Origin-State-Id ]
                           * [ AVP ]
                           * [ Proxy-Info ]
                           * [ Route-Record ]
```

2.2 AA-Mobile-Node-Answer

The AA-Mobile-Node-Answer (AMA), indicated by the Command-Code field set to 261 and the 'R' bit cleared in the Command Flags field, 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].

A successful AMA message MUST include the MIP-Home-Agent-Address, MIP-Home-Mobile-Node-Address AVP and MIP-Reg-Reply AVPs. 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 if they were requested in the AMR, and they were present in the HAR.

The MIP-MN-to-HA-Key and MIP-HA-to-MN-Key AVPs MUST be present if the session keys were requested in the AMR, and the Co-Located-Mobile-Node bit was set in the MIP-Feature-Vector AVP.

An AMA message with the Result-Code set to DIAMETER_MULTI_ROUND_AUTH MAY include mobile node registration key AVPs (see Section 6.1) such as the MIP-MN-to-FA-Key AVP and the MIP-MN-to-HA-Key AVP. If such an AVP is present in the AMA message, the foreign agent MUST include the corresponding Mobile IP key distribution extension in the Registration Reply it sends to the mobile node. This is to support multi-roundtrip authentication mechanisms.

Message Format

```
<AA-Mobile-Node-Answer> ::= < Diameter Header: 260 >
                            < Session-Id >
                            { Auth-Application-Id }
                            { Authorization-Lifetime }
                            { Result-Code }
                            { Origin-Host }
                            { Origin-Realm }
                            { Destination-Host }
                            { Accounting-Multi-Session-Id }
                            [ Error-Reporting-Host ]
                            [ MIP-Reg-Reply ]
                            [ MIP-MN-to-FA-Key ]
                            [ MIP-MN-to-HA-Key ]
                            [ MIP-FA-to-MN-Key ]
                            [ MIP-FA-to-HA-Key ]
                            [ MIP-HA-to-MN-Key ]
                            [ MIP-Home-Agent-Address ]
                            [ MIP-Mobile-Node-Address ]
                          * [ Filter-Rule ]
                            [ Session-Timeout ]
                            [ Origin-State-Id ]
                          * [ AVP ]
                          * [ Proxy-Info ]
                          * [ Route-Record ]
```

2.3 Home-Agent-MIP-Request

The Home-Agent-MIP-Request (HAR), indicated by the Command-Code field set to 262 and the 'R' bit set in the Command Flags field, 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 the AAAH and forwarded by the 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.

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, REQUEST >
                             < Session-Id >
                             { Auth-Application-Id }
                             { Authorization-Lifetime }
                             { MIP-Reg-Request }
                             { Origin-Host }
                             { Origin-Realm }
                             { User-Name }
                             { Destination-Realm }
                             { Accounting-Multi-Session-Id }
                             { MIP-Foreign-Agent-Host }
                             [ Destination-Host ]
                             [ 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 ]
                             [ MIP-Home-Agent-Address ]
                           * [ Filter-Rule ]
                             [ Session-Timeout ]
                             [ Origin-State-Id ]
                           * [ AVP ]
                           * [ Proxy-Info ]
                           * [ Route-Record ]
```

2.4 Home-Agent-MIP-Answer

The Home-Agent-MIP-Answer (HAA), indicated by the Command-Code field set to 262 and the 'R' bit cleared in the Command Flags field, 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: 262 >
                            < Session-Id >
                            { Auth-Application-Id }
                            { Session-Timeout }
                            { Authorization-Lifetime }
                            { Result-Code }
                            { Origin-Host }
                            { Origin-Realm }
                            { Destination-Host }
                            { Accounting-Multi-Session-Id }
                            { MIP-Foreign-Agent-Host }
                            [ Error-Reporting-Host ]
                            [ MIP-Reg-Reply ]
                            [ MIP-Home-Agent-Address ]
                            [ MIP-Mobile-Node-Address ]
                            [ MIP-FA-to-MN-Key ]
                            [ MIP-FA-to-HA-Key ]
                            [ Filter-Rule ]
                            [ Origin-State-Id ]
                          * [ AVP ]
                          * [ Proxy-Info ]
                          * [ Route-Record ]
```

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 Transient Failures

Errors that fall within the transient failures category are used to inform a peer that the request could not be satisfied at the time it was received, but MAY be able to satisfy the request in the future.

DIAMETER_ERROR_AUTH_FAILURE 4004
This error code is used by AAAH to inform the attendant that the authentication data in the MN-AAA authentication extension is invalid.

DIAMETER_ERROR_MIP_REPLY_FAILURE 4005
This error code is used by the Home Agent when processing of the Registration Request has failed.

DIAMETER_ERROR_HA_NOT_AVAILABLE 4006
This error code is used to inform the Foreign Agent that the requested Home Agent cannot be assigned to the Mobile Node at this time. The Foreign Agent MUST return a Mobile IP Registration Reply to the Mobile Node with an appropriate error code.

DIAMETER_ERROR_BAD_KEY 4007
This error code is used by the Home Agent to indicate to the local Diameter server that the key generated is invalid.

3.2 Permanent Failures

Errors that fall within the permanent failures category are used to inform the peer that the request failed, and should not be attempted again.

DIAMETER_ERROR_NO_FOREIGN_HA_SERVICE 5016
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 application, 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
Filter-Rule	400	4.10	OctetString	M	P		V	Y
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-FA-Challenge	344	4.9	OctetString	M	P		V	Y
MIP-Feature-Vector	337	4.7	Unsigned32	M	P		V	Y
MIP-Foreign-Agent-Host	330	4.10	OctetString	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-Host	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-Host AVP

The MIP-Previous-FA-Host AVP (AVP Code 335) is of type OctetString and contains the identity of the Mobile Node's old Foreign Agent, encoded in the UTF-8 [12] format, according to the Diameter identity rules defined in [1]. 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 User-Name 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 User-Name 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
256	Co-Located-Mobile-Node

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.

If the mobile node sets the home agent field equal to 255.255.255.255 in its Registration Request, the Foreign Agent sets both the Home-Agent-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, and zeroes the Home-Address-Allocatable-Only-in-Home-Domain flag in the MIP-Feature-Vector AVP.

Whenever the Foreign Agent sets either the Mobile-Node-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 either by setting the home address field to all ones, or by specifying a home agent in the foreign network, and the AAAF authorizes the request, the AAAF MUST set the Home-Agent-In-Foreign-Network bit to one.

If the Home Agent receives a Registration Request from the Mobile Node indicating that the MN is acting as a Co-Located Mobile Node, the Home Agent sets the Co-Located-Mobile-Node 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 ::= < AVP Header: 322 >
                    { MIP-MN-AAA-SPI }
                    { MIP-Auth-Input-Data-Length }
                    { MIP-Authenticator-Length }
                    { MIP-Authenticator-Offset }
```

```
* [ AVP ]
```

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).

4.9 MIP-FA-Challenge

The MIP-FA-Challenge AVP (AVP Code 344) is of type OctetString and contains the challenge advertised by the Foreign Agent to the Mobile Node. This AVP MUST be present in the AMR if the Mobile Node used the RADIUS-style MN-AAA computation algorithm.

4.10 MIP-Foreign-Agent-Host AVP

The MIP-Foreign-Agent-Host AVP (AVP Code 330) is of type OctetString and contains the identity of the foreign agent, encoded in the UTF-8

[12] format, according to the Diameter identity rules defined in [1]. This AVP is copied from the value of the Origin-Host AVP in the AMR.

4.10 Filter-Rule AVP

The Filter-Rule AVP (AVP Code 400) is of type OctetString, encoded in the UTF-8 [29] format, and provides filter rules that need to be configured on the Foreign or Home Agent for the user. One or more such AVPs MAY be present in an authorization response.

Each packet can be filtered based on the following information that is associated with it:

Direction	(in or out)
Source and destination IP address	(possibly masked)
Protocol	
Source and destination port	(lists or ranges)
TCP flags	
IP fragment flag	
IP options	
ICMP types	

Rules for the appropriate direction are evaluated in order, with the first matched rule terminating the evaluation. Each packet is evaluated once. If no rule matches, the packet is dropped if the last rule evaluated was a permit, and passed if the last rule was a deny.

The filters in the Filter-Rule AVP MUST follow the format:

```
action dir proto from src to dst [options]

action       permit - Allow packets that match the rule.
             deny - Drop packets that match the rule.

dir          "in" is from the terminal, "out" is to the terminal.

proto        An IP protocol specified by number.  The "ip" keyword
             means any protocol will match.

src and dst  <address/mask> [ports]

             The <address/mask> may be specified as:
             ipno       An IPv4 or IPv6 number in dotted-quad or
                        canonical IPv6 form. Only this exact IP
                        number will match the rule.
             ipno/bits  An IP number as above with a mask width of
                        the form 1.2.3.4/24.  In this case all IP
```

numbers from 1.2.3.0 to 1.2.3.255 will match. The bit width MUST be valid for the IP version and the IP number MUST NOT have bits set beyond the mask.

The sense of the match can be inverted by preceding an address with the not modifier, causing all other addresses to be matched instead. This does not affect the selection of port numbers.

The keyword "any" is 0.0.0.0/0 or the IPv6 equivalent. The keyword "assigned" is the address or set of addresses assigned to the terminal. The first rule SHOULD be "deny in ip !assigned".

With the TCP and UDP protocols, optional ports may be specified as:

{port|port-port}[,port[,...]]

The `-' notation specifies a range of ports (including boundaries).

Fragmented packets which have a non-zero offset (i.e. not the first fragment) will never match a rule which has one or more port specifications. See the frag option for details on matching fragmented packets.

options:

frag Match if the packet is a fragment and this is not the first fragment of the datagram. frag may not be used in conjunction with either tcpflags or TCP/UDP port specifications.

ipoptions spec
Match if the IP header contains the comma separated list of options specified in spec. The supported IP options are:

ssrr (strict source route), lsrr (loose source route), rr (record packet route) and ts (timestamp). The absence of a particular option may be denoted with a `!'.

tcpoptions spec
Match if the TCP header contains the comma separated list of options specified in spec. The supported TCP options are:

mss (maximum segment size), window (tcp window advertisement), sack (selective ack), ts (rfc1323 timestamp) and cc (rfc1644 t/tcp connection count). The absence of a particular option may be denoted with a `!'.

established
TCP packets only. Match packets that have the RST or ACK bits set.

setup TCP packets only. Match packets that have the SYN bit set but no ACK bit.

tcpflags spec
TCP packets only. Match if the TCP header contains the comma separated list of flags specified in spec. The supported TCP flags are:

fin, syn, rst, psh, ack and urg. The absence of a particular flag may be denoted with a `!'. A rule which contains a tcpflags specification can never match a fragmented packet which has a non-zero offset. See the frag option for details on matching fragmented packets.

icmptypes types
ICMP packets only. Match if the ICMP type is in the list types. The list may be specified as any combination of ranges or individual types separated by commas. The supported ICMP types are:

echo reply (0), destination unreachable (3), source quench (4), redirect (5), echo request (8), router advertisement (9), router solicitation (10), time-to-live exceeded (11), IP header bad (12), timestamp request (13), timestamp reply (14), information request (15), information reply (16), address mask request (17) and address mask reply (18).

There is one kind of packet that the FA MUST always discard, that is an IP fragment with a fragment offset of one. This is a valid packet, but it only has one use, to try to circumvent firewalls.

An FA that is unable to interpret or apply a deny rule MUST terminate the session. An FA that is unable to interpret or apply a permit rule MAY apply a more restrictive rule. An FA MAY apply deny rules of its own before the supplied rules, for example to protect the FA owner's infrastructure.

The rule syntax is a modified subset of ipfw(8) from FreeBSD, and the ipfw.c code may provide a useful base for implementations.

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.

If the AAAH does not communicate directly with the foreign agent, and it does not wish for intermediate proxies to have access to the session keys, they SHOULD be protected using the CMS security application [9].

The Authorization-Lifetime AVP contains the number of seconds before registration keys destined for the Home Agent and/or Foreign Agent expire. 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 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 generated 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, but instead transmits the HAR to the AAAF. When the AAAF receives the HAR, it first allocates a home agent, and then issues the HAR for that home agent.

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]. 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, which is added to the HAR message, and delivered either to a local home agent, or to the AAAF in the case where the home agent is in the visited network. The AAAH has to rely on the home agent (that also understands Diameter) to transfer the key into a Mobile IP Generalized MN-HA Key Reply extension in the Registration Reply message. The home agent can format the Reply message and extensions correctly for eventual delivery to the mobile node. The resulting Registration Reply is added to the MIP-Reg-Reply AVP and added to the AMA.

After the HAA message is parsed by the AAAH, and transformed into an AMA, the AMA message containing the MIP-Reg-Reply AVP will eventually be received by the the foreign agent. The foreign agent can then use that AVP to recreate a Registration Reply message, containing the Generalized 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 Generalized 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, which is added to the HAR, and copied by the home agent into a Generalized MN-FA Key Reply Extension [15] to the Mobile IP Registration Reply message. Most of the considerations for distributing the Mobile-Foreign registration key are similar to the distribution of the Mobile-Home Registration Key.

If the MIP-FA-to-MN-Key AVP is present in the HAR, the home agent MUST ensure that the same AVP is present in the HAA. The AAAH MUST ensure that this AVP is present in the AMA, which is sent to the foreign agent. The foreign agent MUST include the FA-MN Authentication extension to the Registration Reply, using the decoded session key found in MIP-FA-to-MN-Key.

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 either case, the AAA server 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.

If the MIP-FA-to-HA-Key AVP was present in the HAR, the same AVP MUST be present in the corresponding HAA, which is eventually transformed by the AAAH into an AMA message that is transmitted back to the foreign agent.

Upon receipt of the HAR, the home agent recovers the Foreign-Home registration key, and uses this key to create a Foreign-Home authentication extension to the Registration Reply message.

5.4 Key Distribution Example

Figure 9 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.

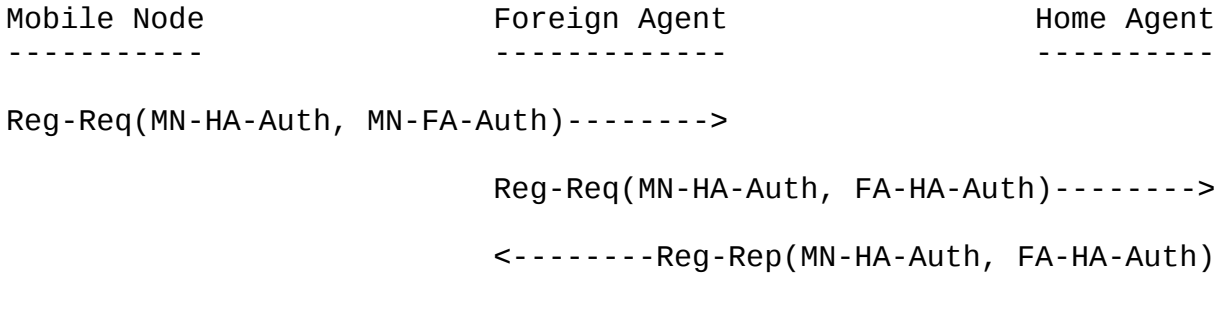

Figure 9: Mobile IP Message Exchange

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 Application 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.

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 CMS security application [9] be used.

The following table describes the Diameter AVPs defined in the Mobile IP application, 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-Algorithm-Type	345	6.2.7	Unsigned32	M	P		V	Y
MIP-FA-HA-Preferred-SPI	327	6.4	Unsigned32	M	P		V	Y
MIP-FA-MN-Preferred-SPI	324	6.3	Unsigned32	M	P		V	Y
MIP-FA-to-HA-Key	328	6.2.2	Grouped	M	P		V	Y
MIP-FA-to-MN-Key	326	6.2.1	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-Replay-Mode	346	6.2.8	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 MIP-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 MIP-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 a Diameter clients. The lifetime of the generated keys MUST be the same as the value of the Authorization-Lifetime AVP.

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. The Algorithm-Type AVP identifies the cryptographic function to be used in the creation of the relevant Mobile IP authentication extension. The Replay-Mode AVP specifies the replay method used in the generation of the Mobile IP registration messages.

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 Data field has the following ABNF grammar:

```
MIP-FA-to-MN-Key ::= < AVP Header: 326 >
                     { MIP-Peer-SPI }
                     { MIP-Algorithm-Type }
                     { MIP-Session-Key }
                   * [ AVP ]
```

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 Data field has the following ABNF grammar:

```
MIP-FA-to-HA-Key ::= < AVP Header: 328 >
                     { MIP-Peer-SPI }
                     { MIP-Algorithm-Type }
                     { MIP-Session-Key }
                   * [ AVP ]
```

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 Data field has the following ABNF grammar:

```
MIP-HA-to-FA-Key ::= < AVP Header: 329 >
                     { MIP-Peer-SPI }
                     { MIP-Algorithm-Type }
                     { MIP-Replay-Mode }
                     { MIP-Session-Key }
                   * [ AVP ]
```

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 Data field has the following ABNF grammar:

```
MIP-HA-to-MN-Key ::= < AVP Header: 332 >
                     { MIP-Peer-SPI }
                     { MIP-Algorithm-Type }
                     { MIP-Replay-Mode }
                     { MIP-Session-Key }
                   * [ AVP ]
```

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.

6.2.7 MIP-Algorithm-Type AVP

The MIP-Algorithm-Type AVP (AVP Code 345) is of type Unsigned32, and contains the Algorithm identifier used to generate the associated Mobile IP authentication extension. The following values are currently defined:

0 Prefix+Suffix MD5
1 HMAC-MD5

6.2.8 MIP-Replay-Mode AVP

The MIP-Replay-Mode AVP (AVP Code 346) is of type Unsigned32 and contains the replay mode the Home Agent should use when authenticating the Mobile Node.

The following values are supported (see [4] for more information):

0 None
1 Timestamps
2 Nonces

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 AVPs

This section will define the Accounting AVPs that are specific to Mobile IP, and MUST be included in all Accounting-Request messages. These AVPs MAY be present in the corresponding Accounting-Answer messages as well.

7.1 Accounting-Input-Octets AVP

The Accounting-Input-Octets AVP (AVP Code 42) is of type Unsigned64, and contains the number of octets in IP packets received from the user.

7.2 Accounting-Output-Octets AVP

The Accounting-Output-Octets AVP (AVP Code 43) is of type Unsigned64, and contains the number of octets in IP packets sent to the user.

7.3 Accounting-Session-Time AVP

The Accounting-Session-Time AVP (AVP Code 46) is of type Unsigned32, and indicates the length of the current session in seconds.

7.4 Accounting-Input-Packets AVP

The Accounting-Input-Packets (AVP Code 47) is of type Unsigned64, and contains the number of IP packets received from the user.

7.5 Accounting-Output-Packets AVP

The Accounting-Output-Packets (AVP Code 48) is of type Unsigned64, and contains the number of IP packets sent to the user.

8.0 AVP Occurrence Tables

The following tables 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.

8.1 Mobile IP Command AVP Table

The table in this section is limited to the Command Codes defined in this specification.

	Command-Code			
Attribute Name	AMR	AMA	HAR	HAA
Authorization-Lifetime	0-1	1	1	1
Destination-Host	0-1	1	0-1	1
Destination-Realm	1	0	1	0
Error-Reporting-Host	0	0-1	0	0-1
Auth-Application-Id	1	1	1	1
Filter-Rule	0	0+	0+	0
MIP-FA-Challenge	0-1	0	0	0
MIP-FA-to-HA-Key	0	0-1	0-1	0-1
MIP-FA-to-MN-Key	0	0-1	0-1	0-1
MIP-FA-HA-Preferred-SPI	0-1	0	0	0
MIP-FA-MN-Preferred-SPI	0-1	0	0	0
MIP-Feature-Vector	0-1	0	0	0
MIP-Foreign-Agent-Host	0	0	1	1
MIP-HA-to-FA-Key	0	0	0-1	0
MIP-HA-to-MN-Key	0	0	0-1	0
MIP-Home-Agent-Address	0-1	0-1	0-1	0-1
MIP-MN-AAA-Auth	1	0	0	0
MIP-MN-to-FA-Key	0	0	0-1	0
MIP-MN-to-HA-Key	0	0-1	0-1	0
MIP-Mobile-Node-Address	0-1	0-1	0-1	0-1
MIP-Previous-FA-Address	0-1	0	0	0
MIP-Previous-FA-Host	0-1	0	0	0
MIP-Reg-Reply	0	0-1	0	0-1
MIP-Reg-Request	1	0	1	0
Origin-Host	1	1	1	1
Origin-Realm	1	1	1	1
Original-State-Id	0-1	0-1	0-1	0-1
Proxy-Info	0+	0+	0+	0+
Result-Code	0	1	0	1
Route-Record	0+	0+	0+	0+
Session-Id	1	1	1	1
Session-Timeout	0	1	1	1
User-Name	1	0	1	0

8.2 Accounting AVP Table

The table in this section is used to represent which AVPs defined in this document are to be present in the Accounting messages, defined in [1].

	Command-Code	
Attribute Name	ACR	ACA
Accounting-Input-Octets	1	0-1
Accounting-Input-Packets	1	0-1
Accounting-Output-Octets	1	0-1
Accounting-Output-Packets	1	0-1
Accounting-Session-Time	1	0-1
MIP-Feature-Vector	1	0-1
MIP-Home-Agent-Address	1	0-1
MIP-Mobile-Node-Address	1	0-1
MIP-Previous-FA-Address	0-1	0-1
MIP-Previous-FA-Host	0-1	0-1

9.0 Acknowledgements

The following people have contributed text to this document: Fredrik Johansson, Martin Julien

The authors would like to thank Nenad Trifunovic, Haseeb Akhtar 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.

10.0 IANA Considerations

This section contains the namespaces that have either been created in this specification, or the values assigned to existing namespaces managed by IANA.

10.1 Command Codes

This specification assigns the values 260 and 262 from the Command Code namespace defined in [1]. See section 2.0 for the assignment of the namespace in this specification.

10.2 AVP Codes

This specification assigns the values 320-322, 324-346 from the AVP Code namespace defined in [1]. See sections 4.0 and 6.0 for the assignment of the namespace in this specification.

This specification also makes use of AVP Code 400, which is assigned in [14].

10.3 Result-Code AVP Values

This specification assigns the values 4004-4007, and 5016 from the Result-Code AVP (AVP Code 268) value namespace defined in [1]. See section 3.0 for the assignment of the namespace in this specification.

10.4 DSI-Event AVP Values

This specification assigns the values 4002-4003 and 5009 from the DSI-Event AVP (AVP Code 297) value namespace defined in [1]. See section 4.0 for the assignment of the namespace in this specification.

10.5 MIP-Feature-Vector AVP Values

There are 32 bits in the MIP-Feature-Vector AVP (AVP Code 337) that are available for assignment. This document assigns bits 1-9, as listed in section 4.7. The remaining bits should only be assigned via Standards Action [2].

10.6 MIP-Algorithm-Type AVP Values

As defined in Section 6.2.7, the MIP-Algorithm-Type AVP (AVP Code 345) defines the values 0-1. All remaining values are available for assignment via Designated Expert [2].

10.7 MIP-Replay-Mode AVP Values

As defined in Section 6.2.8, the MIP-Replay-Mode AVP (AVP Code 346) defines the values 0-2. All remaining values are available for assignment via Designated Expert [2].

10.8 Application Identifier

This specification assigns the value four (4) to the Application Identifier namespace defined in [1]. See section 1.7 for more information.

11.0 Security Considerations

This specification describes the Diameter Application 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 SHOULD be be protected using the methods defined in [9].

12.0 References

[1] P. Calhoun, H. Akhtar, J. Arkko, E. Guttman, A. Rubens, "Diameter Base Protocol", draft-ietf-aaa-diameter-05.txt, IETF work in progress, June 2001.

[2] Narten, Alvestrand,"Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998

[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 CMS Security

Application", draft-ietf-aaa-diameter-cms-sec-00.txt, IETF work in progress, June 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] F. Yergeau, "UTF-8, a transformation format of ISO 10646", RFC 2279, January 1998.

[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 Application", draft-ietf-aaa-diameter-nasreq-05.txt, IETF work in progress, June 2001.

[15] C. Perkins, P. Calhoun, "AAA Registration Keys for Mobile IP", draft-ietf-mobileip-aaa-key-05.txt, IETF work in progress, May 2001.

[16] T. Hiller and al, "CDMA2000 Wireless Data Requirements for AAA", draft-hiller-cdma2000-aaa-01.txt, IETF work in progress, June 2000.

13.0 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

14.0 Full Copyright Statement

15.0 Expiration Date

This memo is filed as <draft-ietf-aaa-diameter-mobileip-05.txt> and expires in December 2001.