DIME Working Group   P. Calhoun
Internet Draft   Cisco Systems, Inc.
Intended Status: Standards Track   T. Johansson
Expires: May 11, 2008   Bytemobile Inc.
                                                         C. Perkins
                                                                 NSN
                                                          T. Hiller
                                                     Alcatel-Lucent
                                                          P. McCann
                                                           Motorola
                                                  November 11, 2007

                    Diameter Mobile IPv4 Application, Revised
                       draft-mccann-dime-rfc4004bis-00.txt

Status of this Memo

   By submitting this Internet-Draft, each author represents that any
   applicable patent or other IPR claims of which he or she is aware
   have been or will be disclosed, and any of which he or she becomes
   aware will be disclosed, in accordance with Section 6 of BCP 79.

   Internet-Drafts are working documents of the Internet Engineering
   Task Force (IETF), its areas, and its working groups. Note that other
   groups may also distribute working documents as Internet-Drafts.

   Internet-Drafts are draft documents valid for a maximum of six months
   and may be updated, replaced, or obsoleted by other documents at any
   time. It is inappropriate to use Internet-Drafts as reference
   material or to cite them other than as "work in progress."

   The list of current Internet-Drafts can be accessed at
   http://www.ietf.org/ietf/1id-abstracts.txt

   The list of Internet-Draft Shadow Directories can be accessed at
   http://www.ietf.org/shadow.html.

   This Internet-Draft will expire on May 11, 2008.

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-Realm 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.   **Introduction**

   Mobile IPv4 [MOBILEIP] allows a Mobile Node (MN) to change its point
   of attachment to the Internet while maintaining its fixed home
   address. Packets directed to the home address are intercepted by a
   Home Agent (HA), encapsulated in a tunnel, and forwarded to the MN at
   its current point of attachment. Optionally, a Foreign Agent (FA)
   may be deployed at this point of attachment, which can serve as the
   tunnel endpoint and may also provide access control for the visited
   network link. In this role, the FA has to authenticate each MN that
   may attach to it, whether the MN is from the same or a different
   administrative domain. The FA has to verify that the MN is
   authorized to attach and use resources in the foreign domain. Also,
   the FA must provide information to the home administrative domain
   about the resources used by the MN while it is attached in the
   foreign domain.

The Authentication, Authorization, and Accounting (AAA) requirements
for Mobile IPv4 are described in detail in other documents [MIPREQ,
CDMA2000]. This document specifies a Diameter application to meet

these requirements. This application is not applicable to the Mobile
IPv6 protocol.

Message formats (e.g., as in section 5.1) are specified as lists of
Attribute-Value Pairs (AVPs) using the syntax as described in RFC
2234 [ABNF]. This includes the use of the "*" symbol to denote zero
or more occurrences of an AVP.

Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
document are to be interpreted as described in RFC 2119 [KEYWORDS].

1.1.   Entities and Relationships

The Diameter Mobile IPv4 Application supports the HA and FA in
providing Mobile IPv4 service to MNs. Both the HA and FA act as
Diameter clients. The MNs interact with the HA and FA by using only
Mobile IPv4 and therefore do not implement Diameter.

The FA, when present, is always assumed to exist in the visited
administrative domain. The HA may be statically or dynamically
allocated to the MN in the home administrative domain or may be
dynamically allocated to the MN in a visited administrative domain.
The home domain contains a home AAA server (AAAH), and the visited
domain contains a foreign AAA server (AAAF). When the MN is "at
home" (present on its home network), the AAAH and AAAF may be the
same.

1.2.   Mobility Security Associations

The base Mobile IPv4 protocol [MOBILEIP] assumes the existence of a
Mobility Security Association (MSA) between the MN and HA (MN-HA
MSA). The MN-HA MSA is used to authenticate, by using a keyed hash-
style algorithm, the Mobile IP Registration Request that is sent from
the MN to the HA. It is important to authenticate Registration
Requests, as they inform the HA about the MN's current Care-of-
Address, which is the destination for tunneled packets from the home
network. Without authentication, malicious attackers would be able
to redirect packets to anywhere on the Internet. The MSA comprises
an agreement on a Security Parameters Index (SPI, a 32-bit number)
that will be used to refer to the MSA, an algorithm that will be used
to compute keyed hashes over messages, and a shared secret key. To
enable authentication of a message, the sender appends a Mobile IP
Authentication Extension that contains the SPI and the result of
running the keyed hash over the entire previous contents of the
message. The recipient checks the Authentication Extension by

looking up the MSA based on the SPI, re-computing the keyed hash, and
verifying that the result is equal to the contents of the received
Authentication Extension.

The base Mobile IPv4 protocol also supports an optional MSA between
the MN and FA (MN-FA MSA). If available, the MN-FA MSA is used by
the FA to authenticate each Registration Request passing through it
on the way to the HA. Although not critical to the operation of the
base protocol, the MN-FA MSA is useful when the FA has to know the
authenticity of a Registration Request; e.g., when it will be
generating accounting records for a session. The MN-FA MSA may also
be useful in future work related to handoff optimization.

Similarly, Mobile IPv4 supports an optional MSA between the FA and HA
(FA-HA MSA). The FA-HA MSA is useful for authenticating messages
between the FA and HA, such as when the HA seeks to inform the FA
that it has revoked a Mobile IP registration.

Note that configuration of MSAs that involve FAs is substantially
more difficult than configuring the one between the MN and HA,
because the MN and HA are often in the same administrative domain and
the MN will retain the same HA for long periods of time. In
contrast, the MN is likely to encounter many FAs over time and may
often find itself in foreign administrative domains.

The base Mobile IPv4 protocol assumes that MNs are identified by
their static home IP addresses and that all MSAs are statically
preconfigured. The Diameter Mobile IPv4 application, together with
extensions [MIPNAI, MIPCHAL, MIPKEYS, AAANAI] to the base Mobile IPv4
protocol, allows an MN to be dynamically assigned a home address
and/or home agent when it attaches to the Internet. This set of
specifications also supports the dynamic configuration of the MN-HA,
MN-FA, and FA-HA MSAs. The dynamic configuration of these
relationships is important to support deployments in which the MN can
attach to a visited network without having a pre-established
relationship with it.

Initially, the MN is assumed to have a long-term AAA security
association only with the AAAH. This security association is indexed
by the MN's NAI, and, like the MSAs, comprises an agreement on a SPI,
an algorithm, and a shared secret key. The MN enters a visited
network and requests service from some FA by sending a Mobile IPv4
Registration Request. The FA contacts an AAAF in its own
administrative domain to authenticate and authorize the request for
service. The AAAF and AAAH may establish a Diameter session directly
with each other, such as via a Diameter Redirect, or may pass
messages via a network of Diameter proxies. Where the AAAF and AAAH
route messages to each other through proxies, rather than a direct
connection, transitive trust is assumed. MNs can include their
Network Access Identifier (NAI) in a Mobile IPv4 Registration Request
[MIPNAI], which serves in place of the home address to identify the

MN. The NAI is used to route Diameter messages toward the correct
AAAH. This use of the NAI is consistent with the roaming model
defined by the ROAMOPS Working Group [EVALROAM, RFC2607].

The AAAH can authenticate the Registration Request with the use of the MN-AAA security association [MIPCHAL]. If authentication is successful, the AAAH then generates and distributes MSAs to the MN, HA, and FA. For each of the MSA pairs that involve the MN (i.e., MN-HA/HA-MN MSAs and MN-FA/FA-MN MSAs), the AAAH generates a nonce and then hashes it together with the MN-AAA shared key to derive the session key for the MSA pair. The nonces are sent to the HA that includes them in the Registration Reply, which enables the MN to derive the same keys [MIPKEYS]. At the same time, the AAAH must distribute the MN-HA/HA-MN MSAs and the FA-HA/HA-FA MSAs to the HA and must distribute the MN-FA/FA-MN MSAs and the FA-HA/HA-FA MSAs to the FA. These are sent in Diameter AVPs and must be independently secured by using IPSec or TLS between the AAAH and the FA and between the AAAH and the HA. See section 8 for more information on key derivation and distribution.

Note that MSAs in Mobile IP are unidirectional in that, for example, the MN-HA MSA (used to protect traffic from the MN to the HA) and the HA-MN MSA (used to protect traffic from the HA to the MN) can use different SPIs, algorithms, and shared secrets. This is true of the base Mobile IP protocol despite common existing practice during manual configuration of MSAs in which all parameters are set to the same value in both directions. This document supports the use of different SPIs in each direction; however, it only supports the distribution of a single session key for each pair of MSAs between two nodes. The security implications of this are discussed in section 13. This document sometimes names only one of the two unidirectional MSAs when referring to the distribution of the single shared secret and the pair of SPIs for the pair of MSAs between two entities.

1.3.   Handoff

In addition to supporting the derivation and transport of the MN-HA, MN-FA, and FA-HA MSAs, this application also supports MIPv4 handoff. When an MN moves from one point of attachment to another, the MN can continue the same Mobile IPv4 session by using its existing HA and home address.

The MN accomplishes this by sending a Mobile IPv4 Registration Request from its new point of attachment. To enable a single set of accounting records to be maintained for the entire session, including handoffs, it is necessary to allow the AAAH to bind the new registration to the pre-existing session. To enable the Mobile IPv4 Registration Request to be routed to the same AAAH, the MN SHOULD include the AAAH NAI [AAANAI] in such re-registrations. Also, to assist the AAAH in routing the messages to the MN's existing HA the mobile node SHOULD include the HA NAI [AAANAI] in such re-

registrations. If the mobile node does not support the Mobile IPv4
AAA NAI extension [AAANAI], this functionality is not available.

1.4.   Structure of the Document

The remainder of this document is structured as follows. Section 2
provides acronym definitions. Section 3 provides some examples and
message flows illustrating both the Mobile IPv4 and Diameter messages
that occur when a mobile node attaches to the Internet. Section 4
defines the relationship of this application to the Diameter Base
Protocol. Section 5 defines the new command codes. Section 6
defines the new result codes used by this application. Section 7
defines the set of mandatory Attribute-Value-Pairs (AVPs). Section 8
gives an overview of the key distribution capability, and Section 9
defines the key distribution AVPs. Section 10 defines the accounting
AVPs, and section 11 contains a listing of all AVPs and their
occurrence in Diameter commands. Finally, sections 12 and 13 give
IANA and security considerations, respectively.

2.   Acronyms

AAAH	Authentication, Authorization, and Accounting Home
AAAF	Authentication, Authorization, and Accounting Foreign
AMA	AA-Mobile-Node-Answer
AMR	AA-Mobile-Node-Request
ASR	Abort-Session-Request
AVP	Attribute Value Pair
CoA	Care-of-Address
FA	Foreign Agent
FQDN	Fully Qualified Domain Name
HA	Home Agent
HAA	Home-Agent-MIP-Answer
HAR	Home-Agent-MIP-Request
MN	Mobile Node
MSA	Mobility Security Association
NAI	Network Access Identifier
RRQ	Registration Request
SPI	Security Parameters Index
STR	Session-Termination-Request

3.   Scenarios and Message Flows

This section presents four scenarios illustrating Diameter Mobile
IPv4 application and describes the operation of key distribution.

In this document, the role of the "attendant" [MIPREQ] is performed
by either the FA (when it is present in a visited network) or the HA
(for co-located mobile nodes not registering via an FA), and these
terms will be used interchangeably in the following scenarios.

3.1.   Inter-Realm Mobile IPv4

When a mobile 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 7.

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.

```
            Visited Realm                     Home Realm
            +-----------+                     +-----------+
            |example.net|       AMR/AMA        |example.org|
            |   AAAF    |<------------------->|   AAAH    |
        +->|   server   |     server-server    |   server  |
        |  +-----------+    communication     +-----------+
        |        ^                                   ^
        | AMR/AMA  |      client-server        | HAR/HAA
        |          |       communication       |
        v          v                           v
   +---------+  +---------+              +---------+
   | Foreign |  | Foreign |              |  Home   |
   |  Agent  |  |  Agent  |              |  Agent  |
   +---------+  +---------+              +---------+
                    ^
                    | Mobile IP
                    |
                    v
               +--------+
               | Mobile |
               | Node   | mn@example.org
               +--------+
```
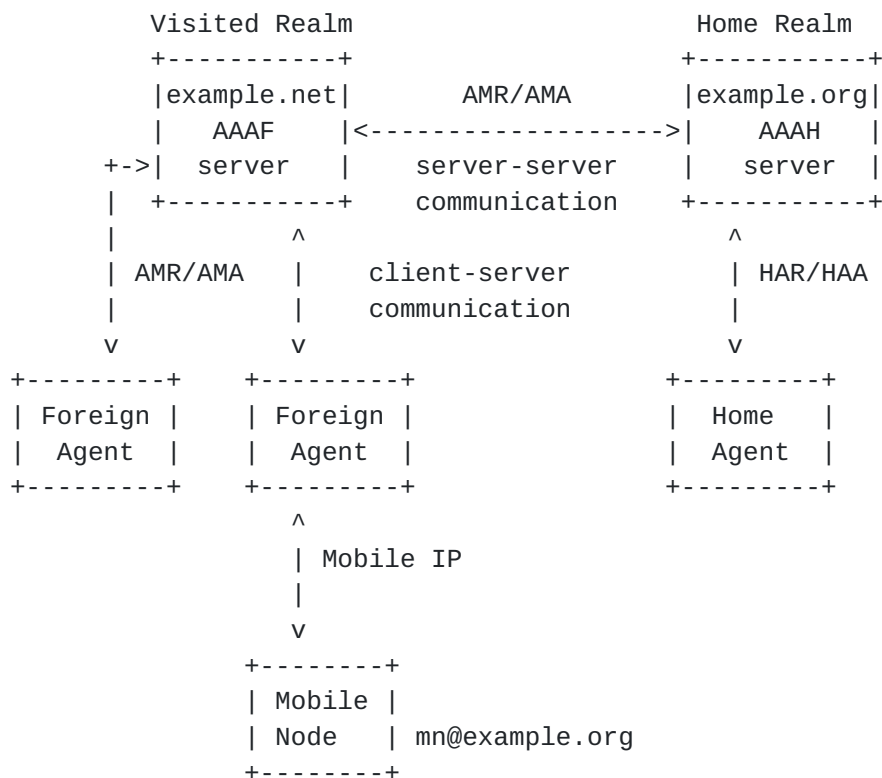
                  Figure 1. Inter-realm Mobility

Upon receiving the AMR, the AAAF follows the procedures outlined in
[DIAMBASE] to determine whether the AMR should be processed locally
or forwarded to another Diameter server known as the AAA-Home, or
AAAH. Figure 1 shows an example in which a mobile node
(mn@example.org) requests service from a foreign provider
(example.net). The request received by the AAAF is forwarded to
example.org'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 is communicated through the Authorization-Lifetime AVP
in the AA-Mobile-Node-Answer (AMA; see section 5.2) from the AAAH.
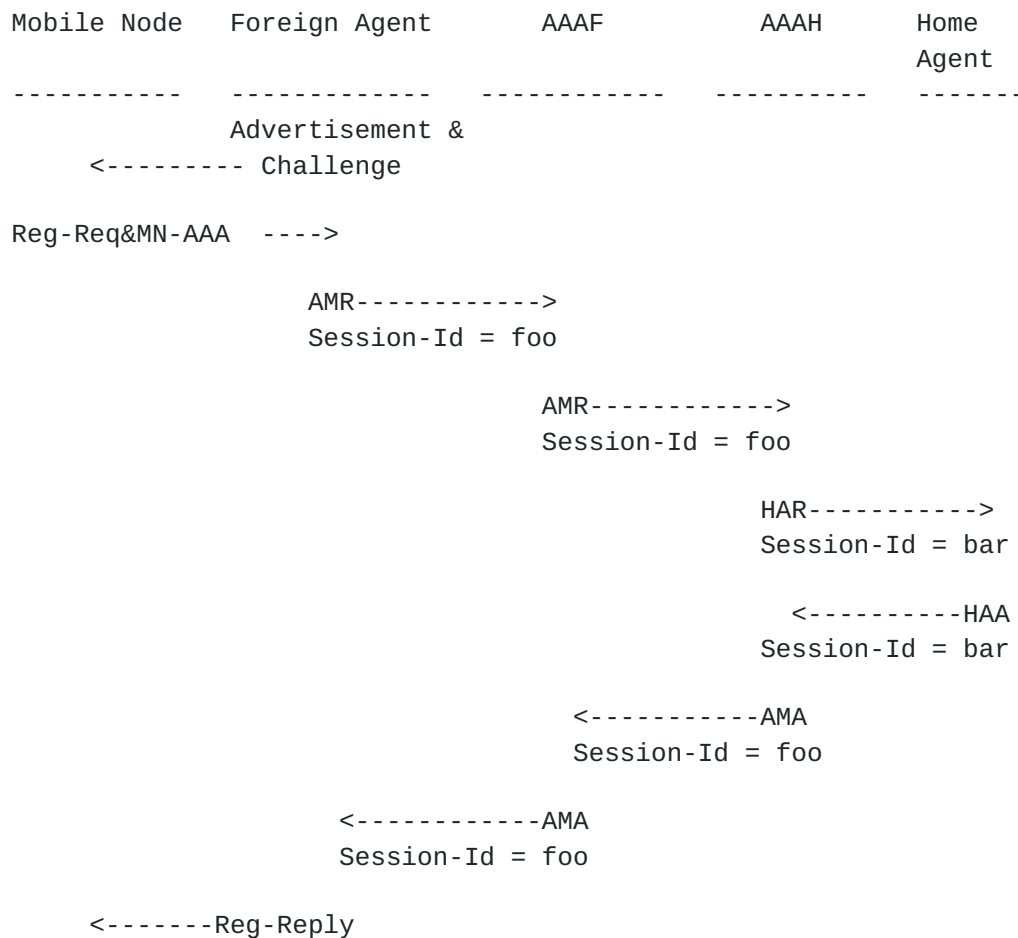
```
       Mobile Node   Foreign Agent        AAAF           AAAH        Home
                                                                     Agent
       ----------    -------------     -----------     ----------   -------
                     Advertisement &
            <--------- Challenge

       Reg-Req&MN-AAA   ---->

                          AMR------------>
                          Session-Id = foo

                                            AMR------------>
                                            Session-Id = foo

                                                            HAR----------->
                                                            Session-Id = bar

                                                            <----------HAA
                                                            Session-Id = bar

                                           <-----------AMA
                                           Session-Id = foo

                          <------------AMA
                          Session-Id = foo

            <-------Reg-Reply

               Figure 2.  Mobile IPv4/Diameter Message Exchange
```

   The foreign agent (as shown in Figure 2) MAY provide a challenge,
   which would give it direct control over the replay protection in the
   Mobile IPv4 registration process, as described in [MIPCHAL]. The
   mobile node includes the Challenge and MN-AAA authentication
   extension to enable authorization by the AAAH. If the authentication
   data supplied in the MN-AAA extension is invalid, the AAAH returns
   the response (AMA) with the Result-Code AVP set to
   DIAMETER_AUTHENTICATION_REJECTED.

   The above scenario causes the MN-FA and MN-HA keys to be exposed to
   Diameter agents all along the Diameter route. If this is a concern,
   a more secure approach is to eliminate the AAAF and other Diameter
   agents, as shown in Figure 3.

```
                               Redirect
          FA              AAAF            Agent              AAAH
                AMR
           ---------------->
                                AMR
                           ---------------->
                           AMA (Redirect)
                           <----------------
            AMA (Redirect)
           <----------------

                           Setup Security Association
           <--------------------------------------------------->

                                AMR
            --------------------------------------------------->
                           AMA (MN-FA key)
           <---------------------------------------------------
```
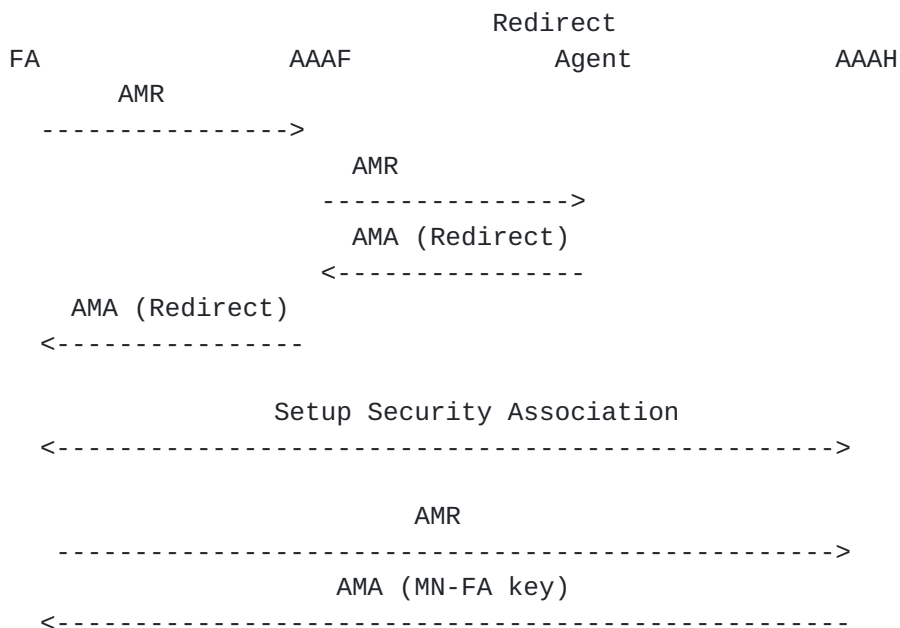
                Figure 3. Use of a Redirect Server with AMR/AMA

   In Figure 3, the FA sets up a TLS [TLS] or IPSec [IPSEC]-based
   security association with the AAAH directly and runs the AMR/AMA
   exchange over it. This provides end-to-end security for secret keys
   that may have to be distributed.

   Figure 4 shows the interaction between the AAAH and HA with the help
   of a redirect agent. When the AAAH and HA are in the same network,
   it is likely that the AAAH knows the IP address of the HA, so the
   redirect server would therefore not be needed; however, it is shown
   anyway for completeness. The redirect server will most likely be
   used in the case where the HA is allocated in a foreign network (see
   section 3.2 for more details of HA allocation in foreign networks).

```
                            Redirect
           HA               Agent                    AAAH
                                        HAR
                           <--------------------
                               HAA (Redirect)
                           -------------------->
                           Setup Security Association
           <------------------------------------------>
                           HAR (MN-HA key)
           <------------------------------------------
                               HAA
           ------------------------------------------>
```

Figure 4. Use of a Redirect Server with HAR/HAA

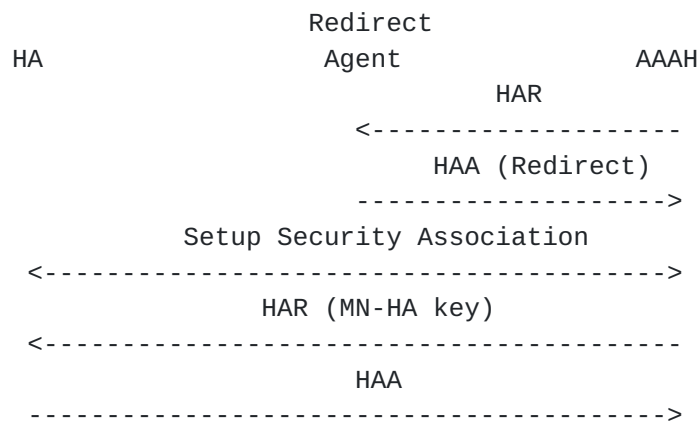As in Figure 2, the FA of Figure 3 would still provide the challenge
and the mobile sends the RRQ, etc.; however, these steps were
eliminated from Figure 3 to reduce clutter. The redirect server
eliminates the AAAF and any other Diameter agents from seeing the
keys as they are transported to the FA and HA. Note that the message
flows in Figure 3 and Figure 4 apply only to the initial
authentication and key exchange. Accounting messages would still be
sent via Diameter agents, not via the direct connection, unless
network policies dictate otherwise.

A mobile node that supports the AAA NAI extension [AAANAI], which has
been previously authenticated and authorized, MUST always include the
assigned home agent in the HA Identity subtype of the AAA NAI
extension, and the authorizing Home AAA server in the AAAH Identity
subtype of the AAA NAI extension, when re-authenticating. Therefore,
in the event that the AMR generated by the FA is for a session that
was previously authorized, it MUST include the Destination-Host AVP,
with the identity of the AAAH found in the AAAH-NAI, and the MIP-
Home- Agent-Host AVP with the identity and realm of the assigned HA
found in the HA-NAI. If, on the other hand, the mobile node does not
support the AAA NAI extension, the FA may not have the identity of
the AAAH and the identity and realm of the assigned HA. This means
that without support of the AAA NAI extension, the FA may not be able
to guarantee that the AMR will be destined to the same AAAH, which
previously authenticated and authorized the mobile node, as the FA
may not know the identity of the AAAH.

If the mobile node was successfully authenticated, the AAAH then
determines which Home Agent to use for the session. First, the AAAH
checks whether an HA has been requested by the MN by checking the
MIP-Home-Agent-Address AVP and the MIP-Home-Agent-Host AVP. The
administrative domain owning the HA may be determined from the realm
portion of the MIP-Home-Agent-Host AVP, or by checking the

Home-Agent-In-Foreign-Network flag of the MIP-Feature-Vector AVP and
the value of the MIP-Originating-Foreign-AAA AVP. If the requested
HA belongs to a permitted administrative domain, the AAAH SHOULD use

the given HA for the session. Otherwise, the AAAH returns the
response (AMA) with the Result-Code AVP set to either
DIAMETER_ERROR_NO_FOREIGN_HA_SERVICE or
DIAMETER_ERROR_HA_NOT_AVAILABLE.

If the MN has not requested any particular HA, then an HA MUST be
dynamically allocated. In this case the MIP-Feature-Vector will have
the Home-Agent-Requested flag set. If the Home-Address-Allocatable-
Only-in-Home-Realm flag is not set, and if the Foreign-Home-Agent-
Available flag is set, then the AAAH SHOULD allow the foreign realm
to allocate the HA (see section 3.2) but MAY allocate one itself in
the home realm if dictated by local policy. If the Home-Address-
Allocatable-Only-in-Home-Realm flag is set, then the AAAH MUST
allocate an HA in the home realm on behalf of the MN. Allocation of
the HA can be done in a variety of ways, including by using a load-
balancing algorithm to keep the load on all home agents equal. The
actual algorithm used and the method of discovering the home agents
are outside the scope of this specification.

The AAAH then sends a Home-Agent-MIP-Request (HAR), which contains
the Mobile IPv4 Registration Request message data encapsulated in the
MIP-Reg-Request AVP, to the assigned or requested Home Agent. Refer
to Figure 4 if the AAAH does not have a direct path to the HA. The
AAAH MAY allocate a home address for the mobile node, and the Home
Agent MUST support home address allocation. In the event that the
AAAH handles address allocation, it includes the home address in a
MIP-Mobile-Node-Address AVP within the HAR. The absence of this AVP
informs the Home Agent that it must perform the home address
allocation.

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. In the creation of the Registration Reply, the
Home Agent MUST include the HA NAI and the AAAH NAI, which will be
created from the Origin-Host AVP and Origin-Realm AVP of the HAR. If
a home address is needed, the home agent MUST also assign one and
include the address in both the Registration Reply and the
MIP-Mobile-Node-Address AVP.

Upon receipt of the HAA, the AAAH creates the AA-Mobile-Node-Answer
(AMA) message, which includes the same Acct-Multi-Session-Id
contained in the HAA and the MIP-Home-Agent-Address and MIP-Mobile-
Node-Address AVPs in the AMA message. See Figure 3 and Figure 4 for
the use of the redirect agent for the secure transport of the HAA and
AMA messages.

See section 4.1 for information on the management of sessions and

session identifiers by the Diameter Mobile IPv4 entities.

[3.2](#).   Allocation of Home Agent in Foreign Network

The Diameter Mobile IPv4 application allows a home agent to be allocated in a foreign network, as required in [MIPREQ, CDMA2000]. 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 set to 255.255.255.255, the foreign agent MUST set the Home-Address-Allocatable-Only-in-Home-Realm 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-Realm flag equal to zero.

When the AAAF receives an AMR message with the Home-Agent-Requested flag set to one and with the Home-Address-Allocatable-Only-in-Home-Realm flag equal to zero, the AAAF MAY set the Foreign-Home-Agent-Available flag in the MIP-Feature-Vector AVP in order to inform the AAAH that it is willing and able to assign a Home Agent for the mobile node. When doing so, the AAAF MUST include the MIP-Candidate-Home-Agent-Host AVP and the MIP-Originating-Foreign-AAA-AVP. The MIP-Candidate-Home-Agent-Host AVP contains the identity (i.e., a DiameterIdentity, which is an FQDN) of the home agent that would be assigned to the mobile node, and the MIP-Originating-Foreign-AAA AVP contains the identity of the AAAF. The AAAF now sends the AMR to the AAAH. However, as discussed above, the use of Diameter agents between the FA and AAAH would expose the MN-FA key. If this is deemed undesirable, a redirect server approach SHOULD be utilized to communicate the AMR to the AAAH. This causes the FA to communicate the AMR directly to the AAAH via a security association.

If the mobile node with AAA NAI extension support [AAANAI] has been previously authorized by the AAAH, now has to be re-authenticated, and requests to keep the assigned home agent in the foreign network, the mobile node MUST include the HA NAI and the AAAH NAI in the registration request to the FA. Upon receipt, the FA will create the AMR, including the MIP-Home-Agent-Address AVP and the Destination-Host AVP based on the AAAH NAI, and include the MIP-Home-Agent-Host AVP based on the home agent NAI. If the AAAF authorizes the use of the requested home agent, the AAAF MUST set the Home-Agent-In-Foreign-Network bit in the MIP-Feature-Vector AVP.

If the mobile node has to be re-authenticated but does not support the AAA NAI extension, it sends a registration request without the AAA NAI and the HA NAI, even though it has previously been authorized by the AAAH and requests to keep the assigned home agent in the foreign network. Upon receipt, the FA will create the AMR, including the MIP-Home-Agent-Address AVP. If the AAAF authorizes the use of the requested home agent, and if it knows that the agent is in its own domain, the AAAF MUST set the Home-Agent-In-Foreign-Network bit in the MIP-Feature-Vector AVP.

When the AAAH receives an 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 (i.e., the
Foreign-Home-Agent-Available is set in the MIP-Feature-Vector AVP),
or if the AMR indicates that the AAAF has offered a previously
allocated Home Agent for the mobile node (i.e., the Home-Agent-In-
Foreign-Network is set in the MIP-Feature-Vector AVP), then the AAAH
must decide whether its local policy would allow the user to have or
keep a home agent in the foreign network. Assuming that the mobile
node is permitted to do so, the AAAH determines the IP address of the
HA based upon the FQDN of the HA by using DNS or learns it via an
MIP-Home-Agent-Address AVP in a redirect response to an HAR (i.e., if
the redirect server adds this AVP to the HAA). Then it sends an HAR
message to Home Agent by including the Destination-Host AVP set to
the value found in the AMR's MIP-Candidate-Home-Agent-Host AVP or
MIP-Home-Agent-Host AVP. If DNS is used to determine the HA IP
address, it is assumed that the HA has a public address and that it
can be resolved by DNS.

Security considerations may require that the HAR be sent directly
from the AAAH to the HA without the use of intermediary Diameter
agents. This requires that a security association between the AAAH
and HA be established, as in Figure 4. If no security association
can be established, the AAAH MUST return an AMA with the Result-Code
AVP set to DIAMETER_ERROR_END_TO_END_MIP_KEY_ENCRYPTION.

If Diameter agents are being used (e.g., if there is no redirect
server) the AAAH sends the HAR to the originating AAAF. In this HAR
the Destination-Host AVP is set to the value found in the AMR's MIP-
Originating-Foreign-AAA AVP, and the MIP-Home-Agent-Host AVP or the
MIP-Candidate-Home-Agent-Host AVP found in the AMR is copied into the
HAR.

Therefore, the AAAH MUST always copy the MIP-Originating-Foreign-AAA
AVP from the AMR message to the HAR message. In cases when another
AAAF receives the HAR, this new AAAF will send the HAR to the HA.

```
                     Visited                         Home
                      Realm                         Realm
                   +--------+ ------- AMR -------> +--------+
                   |  AAAF  | <------ HAR -------- |  AAAH  |
                   |        |                      |        |
               +--->| server | ------- HAA -------> | server |
               |    +--------+ <------ AMA ------- +--------+
               |         ^  |
               |         |  |
          HAR/HAA |     AMR |  | AMA
               v         |  v
          +---------+      +---------+
          |  Home   |      | Foreign |
          |  Agent  |      |  Agent  |
          +---------+      +---------+
                               ^
             +--------+        |
             | Mobile |<----------+
             | Node   |  Mobile IP
             +--------+
```
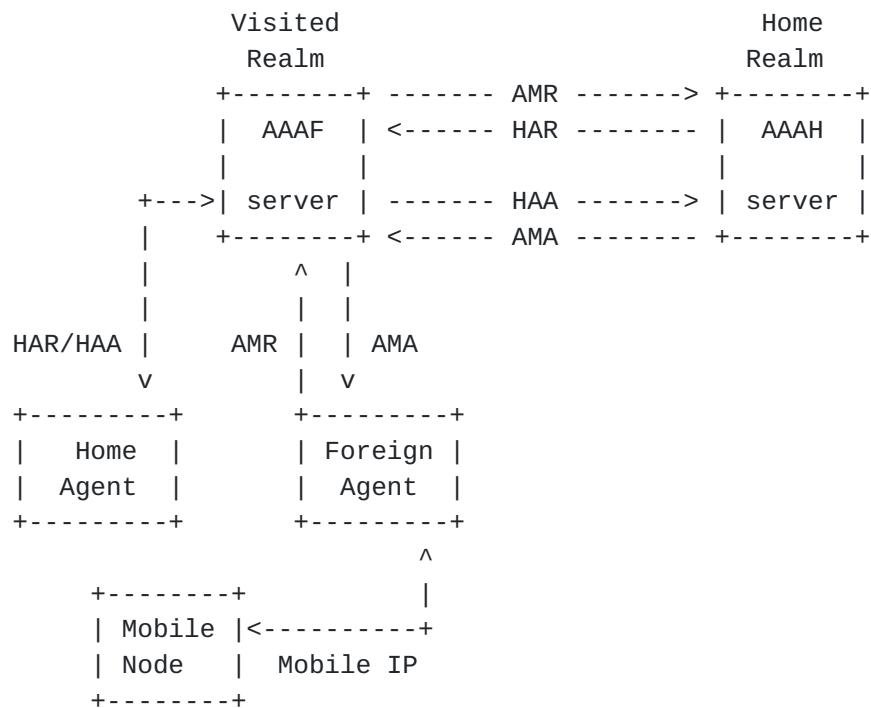
Figure 5. Home Agent Allocated in Visited Realm

Upon receipt of an HAA from the Home Agent in the visited realm, the
AAAF forwards the HAA to the AAAH in the home realm. The AMA is then
constructed and issued to the AAAF and, finally, to the FA. If the
Result-Code indicates success, the HAA and AMA MUST include the MIP-
Home-Agent-Address and the MIP-Mobile-Node-Address AVPs.

If exposing keys to the Diameter Agents along the way represents an
unacceptable security risk, then the redirect approach depicted in
Figure 3 and Figure 4 MUST be used instead.

```
     Mobile Node   Foreign Agent    Home Agent      AAAF        AAAH
     -----------   -------------   ------------- ---------- ----------

     <----Challenge----
     Reg-Req (Response)->
                         ------------AMR------------->
                                                      -----AMR---->
                                                      <----HAR-----
                                       <-----HAR------
                                       ------HAA------>

                                                      -----HAA---->
                                                      <----AMA-----
                         <------------AMA------------
         <---Reg-Reply----


         Figure 6.  MIP/Diameter Exchange for HA Is Allocated in
                            Visited Realm
```

   If the mobile node moves to another foreign Network, it MAY either
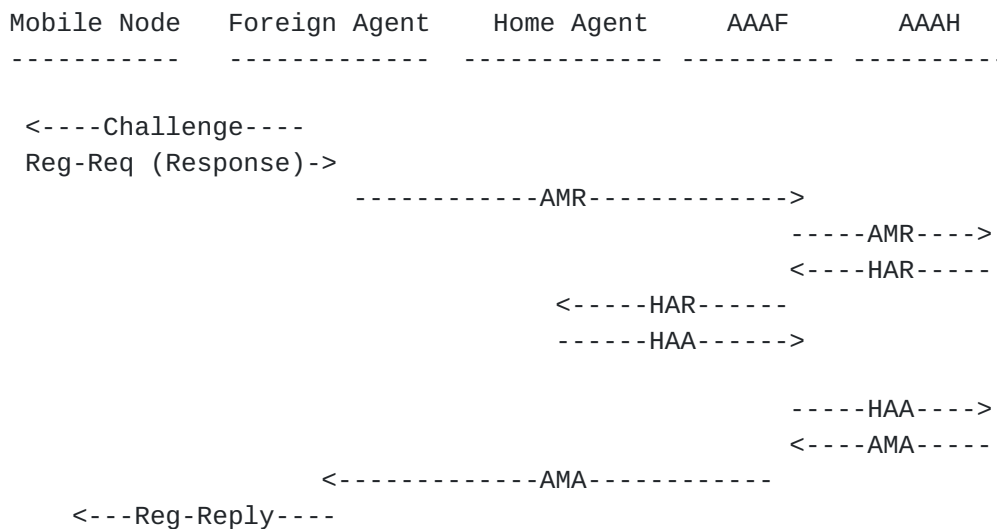   request to keep the same Home Agent within the old foreign network or
   request to get a new one in the new foreign network. If the AAAH is
   willing to provide the requested service, the AAAH will have to
   provide services for both visited networks; e.g., key refresh.

3.3.   Co-located Mobile Node

   If a mobile node registers with the Home Agent as a co-located mobile
   node, no foreign agent is 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. The Home Agent also includes the Acct-Multi-
   Session-Id AVP (see sections 4.1.1 and 4.1.2) in the AMR sent to the
   AAAH, as the AAAH may find this piece of session-state or log entry
   information useful.

```
                                      Home
                                      Realm
                                   +--------+
                                   |  AAAH  |
                                   |        |
                                   | server |
                                   +--------+
                                      ^  |
                                      |  |
                                  AMR |  | AMA
                                      |  v
          +--------+               +---------+
          | Mobile | Registration  |  Home   |
          | Node   |-------------->|  Agent  |
          +--------+     Request   +---------+
```
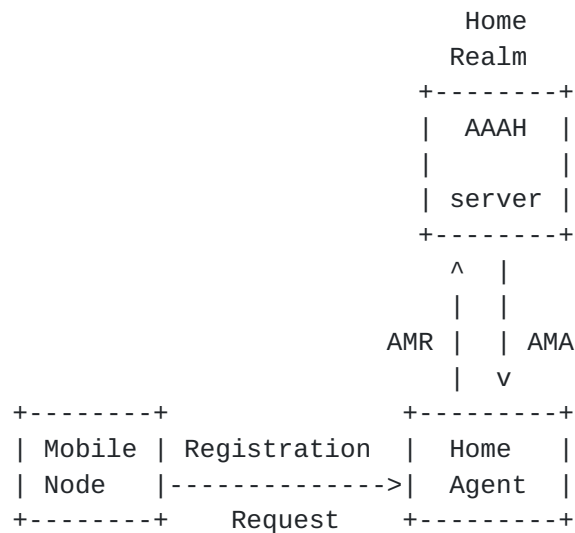
                 Figure 7. Co-located Mobile Node

   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.

   Figure 8 shows a signaling diagram that indicates a secure way to set
   up the necessary security associations when using redirect servers.
   The Proxy AAA represents any AAA server or servers that the HA may
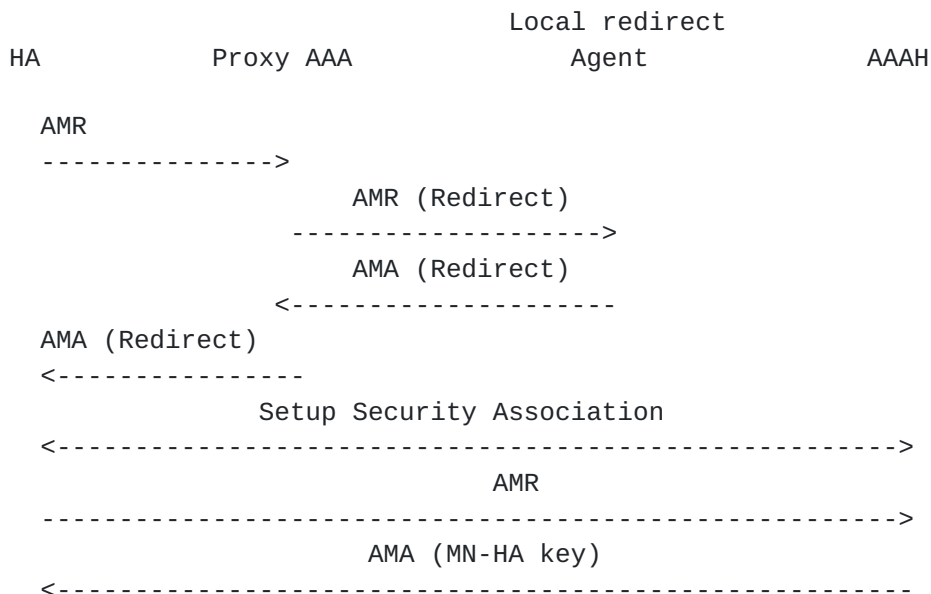   use. This applies to the visited or home network.


```
                              Local redirect
        HA            Proxy AAA            Agent               AAAH

        AMR
        --------------->
                          AMR (Redirect)
                        -------------------->
                          AMA (Redirect)
                        <--------------------
        AMA (Redirect)
        <----------------
                      Setup Security Association
        <----------------------------------------------------->
                                   AMR
        ------------------------------------------------------->
                            AMA (MN-HA key)
        <-------------------------------------------------------
```

        Figure 8. Use of Redirect Server for Co-located CoA
                           and AMR/AMA

[3.4](#).   Key Distribution

   To allow the scaling of wireless data access across administrative
   domains, it is necessary to minimize the number of pre-existing
   Mobility Security Associations (MSAs) required. This means that each
   Foreign Agent should not be required to have a pre-configured MSA
   with each Home Agent on the Internet, nor should the mobile node be
   required to have a pre-configured MSA (as defined in [MOBILEIP]) with
   any specific foreign agent. Furthermore, when the mobile node
   requests a dynamically allocated home agent, it is likely to receive
   the address of a home agent for which it has no available mobility
   security association.

   The Diameter Mobile IPv4 application solves this by including key
   distribution functionality, which means that after a Mobile Node is
   authenticated the authorization phase includes the generation of
   session keys and nonces. Specifically, three session keys and two
   nonces are generated:

     - K1: The MN-HA Session Key, which will be part of the MSA between
            the Mobile Node and the Home Agent. The MN-HA Session Key
            is derived from a nonce generated by AAA. The mobile node
            obtains that nonce in the Registration Reply and generates
            this key using the same formula that AAA uses.

     - K2: The MN-FA Key, which will be part of the MSA between the
            Mobile Node and the Foreign Agent. The MN-FA Key is derived
            from a nonce generated by AAA. The mobile node obtains that
            nonce in the Registration Reply and generates the MN-FA key
            using the same formula that AAA uses.

     - K3: The FA-HA Key, which will be part of the MSA between the
            Foreign Agent and the Home Agent.

   The same session key is used in both directions between two entities;
   e.g., the Mobile Node and the Foreign Agent use the same session key
   for the MN-FA and the FA-MN authentication extensions. The security
   implications of this are examined in section 13. However, the SPIs
   may be different for the MN-FA and the FA-MN authentication
   extensions. The SPI for the MN-FA MSA is used on messages sent from
   the MN to the FA, and the SPI for the FA-MN MSA is used on messages
   sent from the FA to the MN.

   All keys and nonces are generated by the AAAH, even if a Home Agent
   is dynamically allocated in the foreign network.

Figure 9 depicts the MSAs used for Mobile-IPv4 message integrity
using the keys created by the DIAMETER server.

```
                  +--------+                      +--------+
                  |Foreign |          K3          | Home   |
                  |Agent   |<-------------------->| Agent  |
                  |        |                      |        |
                  +--------+                      +--------+
                       ^                              ^
                       | K2                      K1 |
                       |          +--------+          |
                       |          | Mobile |          |
                  +------>| Node     |<------+
                                  |        |
                                  +--------+
```

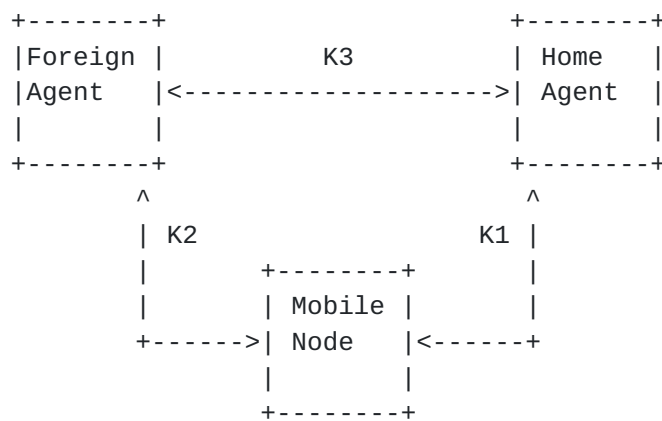   Figure 9.   Mobility Security Associations after Session
                            Key and Nonce Distribution

   The keys destined for the foreign and home agent are propagated to
   the mobility agents via the Diameter protocol. If exposing keys to
   the Diameter Agents along the way represents an unacceptable security
   risk, then the keys MUST be protected either by IPSec or TLS security
   associations that exist directly between the HA and AAAH or the FA
   and AAAF, as explained above.

   The keys destined for the mobile node MUST also be propagated via the
   Mobile IPv4 protocol and therefore MUST follow the mechanisms
   described in [MIPKEYS] instead. In [MIPKEYS], the mobile node
   receives a nonce for each key it needs, and the mobile node will use
   the nonce and the long-term shared secret to create the keys (see
   section 8).

   Once the session keys have been established and propagated, the
   mobility devices can exchange registration information directly, as

defined in [MOBILEIP], without the need of the Diameter

infrastructure. However, the session keys have a lifetime, after
which the Diameter infrastructure MUST be invoked again if new
session keys and nonces are to be acquired.

4.   Diameter Protocol Considerations

This section details the relationship of the Diameter Mobile IPv4
application to the Diameter base protocol.

This document specifies Diameter Application-ID 2. Diameter nodes
conforming to this specification MAY advertise support by including
the value of two (2) in the Auth-Application-Id or the Acct-
Application-Id AVP of the Capabilities-Exchange-Request and
Capabilities-Exchange-Answer commands [DIAMBASE]. The value of two
(2) MUST be used as the Application-Id in all AMR/AMA and HAR/HAA
commands. The value of two (2) MUST be used as the Application-Id in
all ACR/ACA commands, as this application defines new, mandatory AVPs
for accounting. The value of zero (0) SHOULD be used as the
Application-Id in all STR/STA and ASR/ASA commands, as these are
defined in the Diameter base protocol and no additional mandatory
AVPs for those commands are defined in this document.

Given the nature of Mobile IPv4, re-authentication can only be
initiated by a mobile node, which does not participate in the
Diameter message exchanges. Therefore, Diameter server initiated
re-auth does not apply to this application, and RAR/RAA commands MUST
NOT be sent for Diameter Mobile IPv4 sessions.

4.1.   Diameter Session Management

The AAAH and AAAF MAY maintain session-state or MAY be session-
stateless. AAA redirect agents and AAA relay agents MUST NOT
maintain session-state. The AAAH, AAAF, proxies and relays agents
MUST maintain transaction state.

A mobile node's session is identified via its identity in the User-
Name AVP and the MIP-Mobile-Node-Address, and the MIP-Home-Agent-
Address AVPs. This is necessary in order to allow the session state
machine, defined in the base protocol [DIAMBASE], to be used without
modification for this application. However, as the MN may interact
with more than one FA during the life of its session, it is important
for the Diameter Mobile IPv4 application to distinguish the two
pieces of the session (some state at the FA, some state at the HA)
and to manage them independently. The following sub-sections give
further details.

4.1.1.   Session Identifiers

   During creation of the AMR, the FA will choose a session identifier.
   During the creation of the HAR, the AAAH MUST use a different session
   identifier than that used in the AMR/AMA. If the AAAH is session-
   stateful, it MUST send the same session identifier for all HARs
   initiated on behalf of a given mobile node's session. Otherwise, if
   the AAAH is session-stateless, it will manufacture a unique session-
   id for every HAR.

   When the HA is first allocated, it MUST create and include an Acct-
   Multi-Session-Id AVP in the HAA returned to the AAAH. This
   identifier will be kept constant for the life of the Mobile IPv4
   session, as detailed in the next subsection.

4.1.2.   Managing Sessions During Mobile IPv4 Handoffs

   Given the nature of Mobile IPv4, a mobile node MAY receive service
   from many foreign agents during a period of time. However, the home
   realm should not view these handoffs as different sessions, as this
   could affect billing systems. Furthermore, foreign agents usually do
   not communicate between each other, which implies that AAA
   information cannot be exchanged between these entities.

   A handoff registration request from a mobile node will cause the FA
   to send an AMR to its AAAF. The AMR will include a new session
   identifier and MAY be sent to a new AAAF (i.e., a AAAF different from
   that used by the previous FA). However, the AMR shall be received by
   the AAAH to which the user is currently registered (possibly via the
   redirect mechanism depicted in Figure 3).

   As the AAAH may be session-stateless, 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 an existing service, then the HA MUST be able to
   modify its internal session state information to reflect the new
   session identifier.

   For correlation to occur, accounting records must have some
   commonality across handoffs. Therefore, the home agent MUST send the
   same Acct-Multi-Session-Id AVP value in all HAAs for the mobile's
   session. That is, the HA generates a unique Acct-Multi-Session-Id
   when receiving an HAR for a new session and returns this same value
   in every HAA for the session. This Acct-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 Acct-Multi-Session-Id in the
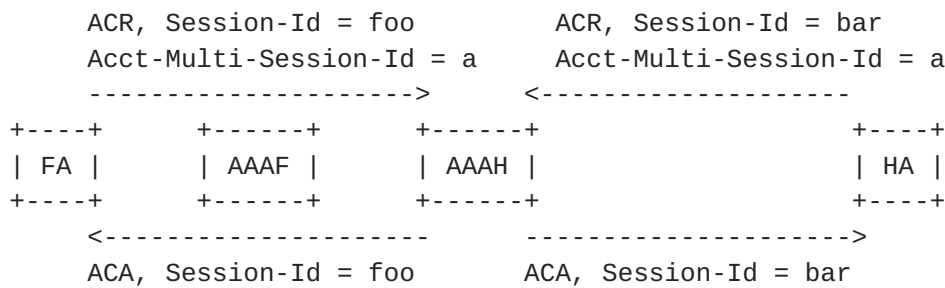   accounting messages, as depicted in Figure 10.

```
          ACR, Session-Id = foo         ACR, Session-Id = bar
          Acct-Multi-Session-Id = a   Acct-Multi-Session-Id = a
          -------------------->     <--------------------
    +----+       +------+       +------+                 +----+
    | FA |       | AAAF |       | AAAH |                 | HA |
    +----+       +------+       +------+                 +----+
       <---------------------     -------------------->
        ACA, Session-Id = foo       ACA, Session-Id = bar
```

            Figure 10: Accounting messages w/ Mobile IPv4
                            Application

[4.1.3]. 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. For a Diameter
   Server to release any resources allocated to a specific mobile node,
   that server has to receive a Session-Termination-Request (STR) from a
   mobility agent. The mobility agents MUST issue the Session-
   Termination-Request (STR) if the Authorization Lifetime has expired
   and no subsequent MIP registration request has been received.

   The AAAH 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 (for example, as a result of
   a handover) does not cause the Home Diameter Server to free all
   resources for the mobile node. Therefore, an STR from a foreign
   agent would free the session from the foreign agent, but not the
   session state associated with the home agent (see Figure 11).

```
          STR, Session-Id = foo       STR, Session-Id = bar
          -------------------->     <--------------------
    +----+       +------+       +------+                 +----+
    | FA |       | AAAF |       | AAAH |                 | HA |
    +----+       +------+       +------+                 +----+
       <---------------------     -------------------->
        STA, Session-Id = foo       STA, Session-Id = bar
```
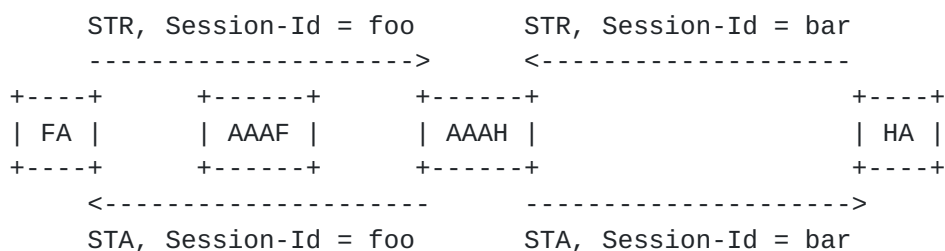
            Figure 11. Session Termination and Session Identifiers

   When deallocating all of the mobile node's resources, the home
   Diameter server (and the foreign Diameter server in the case of an HA
   allocated in foreign network) MUST destroy all session keys that may
   still be valid.

   In the event that the AAAF wishes to terminate a session, its Abort-

Session-Request (ASR) [DIAMBASE] message SHOULD be sent to the FA.
Similarly, the AAAH SHOULD send its message to the Home Agent.

5. Command-Code Values

This section defines Command-Code [DIAMBASE] 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-Request       AMR          260        5.1
     AA-Mobile-Node-Answer        AMA          260        5.2
     Home-Agent-MIP-Request       HAR          262        5.3
     Home-Agent-MIP-Answer        HAA          262        5.4
```

5.1.   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 (i.e., the Foreign Agent), acting as a Diameter client,
to a AAAF 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, 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 [DIAMBASE])
        MN-HA Key Request (MIP-Feature-Vector AVP)
        MN-FA Key Request (MIP-Feature-Vector AVP)
        MN-AAA Authentication Extension (MIP-MN-AAA-Auth AVP)
        Foreign Agent Challenge Extension (MIP-FA-Challenge AVP)
        Home Agent NAI (MIP-Home-Agent-Host AVP)
        Home AAA server NAI (Destination-Host AVP [DIAMBASE])
        Home Agent to Foreign Agent SPI (MIP-HA-to-FA-SPI AVP)
```

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 home 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 realm.

If the mobile node's home address is all ones, the foreign or home
agent MUST include a MIP-Mobile-Node-Address AVP, set to all ones.

If the mobile node includes the home agent NAI and the home AAA
server NAI [AAANAI], the foreign agent MUST include the MIP-Home-
Agent-Host AVP and the Destination-Host AVP in the AMR.

   Message Format

       <AA-Mobile-Node-Request> ::= < Diameter Header: 260, REQ, PXY >
                                    < Session-ID >
                                    { Auth-Application-Id }
                                    { User-Name }
                                    { Destination-Realm }
                                    { Origin-Host }
                                    { Origin-Realm }
                                    { MIP-Reg-Request }
                                    { MIP-MN-AAA-Auth }
                                    [Acct-Multi-Session-Id]
                                    [Destination-Host]
                                    [Origin-State-Id]
                                    [MIP-Mobile-Node-Address]
                                    [MIP-Home-Agent-Address]
                                    [MIP-Feature-Vector]
                                    [MIP-Originating-Foreign-AAA]
                                    [Authorization-Lifetime]
                                    [Auth-Session-State]
                                    [MIP-FA-Challenge]
                                    [MIP-Candidate-Home-Agent-Host]
                                    [MIP-Home-Agent-Host]
                                    [MIP-HA-to-FA-SPI]
                                    [MIP-MN-to-FA-SPI]
                                  * [Proxy-Info]
                                  * [Route-Record]
                                  * [AVP]

5.2.   AA-Mobile-Node-Answer

   The AA-Mobile-Node-Answer (AMA), indicated by the Command-Code field
   set to 260 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 User-Name MAY be included in the AMA if it is present in the AMR.
   The Result-Code AVP MAY contain one of the values defined in section
   6, in addition to the values defined in [DIAMBASE].

   An AMA message with the Result-Code AVP set to DIAMETER_SUCCESS MUST
   include the MIP-Home-Agent-Address AVP, MUST include the MIP-Mobile-
   Node-Address AVP, and includes the MIP-Reg-Reply AVP if and only if
   the Co-Located-Mobile-Node bit was not set in the MIP-Feature-Vector
   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-MSA and MIP-FA-to-MN-MSA if they were requested in the
AMR and were present in the HAR. The MIP-MN-to-HA-MSA and MIP-HA-to-

MN-MSA 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.

   Message Format

       <AA-Mobile-Node-Answer> ::= < Diameter Header: 260, PXY >
                                   < Session-Id >
                                   { Auth-Application-Id }
                                   { Result-Code }
                                   { Origin-Host }
                                   { Origin-Realm }
                                   [Acct-Multi-Session-Id]
                                   [User-Name]
                                   [Authorization-Lifetime]
                                   [Auth-Session-State]
                                   [Error-Message]
                                   [Error-Reporting-Host]
                                   [Re-Auth-Request-Type]
                                   [MIP-Feature-Vector]
                                   [MIP-Reg-Reply]
                                   [MIP-MN-to-FA-MSA]
                                   [MIP-MN-to-HA-MSA]
                                   [MIP-FA-to-MN-MSA]
                                   [MIP-FA-to-HA-MSA]
                                   [MIP-HA-to-MN-MSA]
                                   [MIP-MSA-Lifetime]
                                   [MIP-Home-Agent-Address]
                                   [MIP-Mobile-Node-Address]
                                 * [MIP-Filter-Rule]
                                   [Origin-State-Id]
                                 * [Proxy-Info]
                                 * [AVP]

5.3.   Home-Agent-MIP-Request

The AAA sends 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, 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 to the HA if no redirect servers are involved. If any are,
the HAR is sent directly to the HA via a security association. If
the HAR message does not include a MIP-Mobile-Node-Address AVP, the
Registration Request has 0.0.0.0 for the home address, and the HAR is
successfully processed, the Home Agent MUST allocate the mobile nodes
address. If, on the other hand, the home agent's local AAA server

allocates the mobile node's home address, the local AAA server MUST
include the assigned address in a MIP-Mobile-Node-Address AVP.

When session keys are requested for use by the mobile node, the AAAH
MUST create them and include them in the HAR message. When a FA-HA
session key is requested, it will be created and distributed by the
AAAH server.

    Message Format

        <Home-Agent-MIP-Request> ::= < Diameter Header: 262, REQ, PXY >
                                     < Session-Id >
                                     { Auth-Application-Id }
                                     { Authorization-Lifetime }
                                     { Auth-Session-State }
                                     { MIP-Reg-Request }
                                     { Origin-Host }
                                     { Origin-Realm }
                                     { User-Name }
                                     { Destination-Realm }
                                     { MIP-Feature-Vector }
                                     [Destination-Host]
                                     [MIP-MN-to-HA-MSA]
                                     [MIP-MN-to-FA-MSA]
                                     [MIP-HA-to-MN-MSA]
                                     [MIP-HA-to-FA-MSA]
                                     [MIP-MSA-Lifetime]
                                     [MIP-Originating-Foreign-AAA]
                                     [MIP-Mobile-Node-Address]
                                     [MIP-Home-Agent-Address]
                                   * [MIP-Filter-Rule]
                                     [Origin-State-Id]
                                   * [Proxy-Info]
                                   * [Route-Record]
                                   * [AVP]

5.4.   Home-Agent-MIP-Answer

In response to a Home-Agent-MIP-Request, the Home Agent sends 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, to its
local AAA server. The User-Name MAY be included in the HAA if it is
present in the HAR. 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 6 instead of the values defined in [DIAMBASE].

Message Format

```
<Home-Agent-MIP-Answer> ::= < Diameter Header: 262, PXY >
                            < Session-Id >
                            { Auth-Application-Id }
                            { Result-Code }
                            { Origin-Host }
                            { Origin-Realm }
                            [ Acct-Multi-Session-Id ]
                            [ User-Name ]
                            [ Error-Reporting-Host ]
                            [ Error-Message ]
                            [ MIP-Reg-Reply ]
                            [ MIP-Home-Agent-Address ]
                            [ MIP-Mobile-Node-Address ]
                            [ MIP-FA-to-HA-SPI ]
                            [ MIP-FA-to-MN-SPI ]
                            [ Origin-State-Id ]
                          * [ Proxy-Info ]
                          * [ AVP ]
```

6. Result-Code AVP Values

This section defines new Result-Code [DIAMBASE] values that MUST be
supported by all Diameter implementations that conform to this
specification.

6.1.   Transient Failures

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

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 IPv4
    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.

          DIAMETER_ERROR_MIP_FILTER_NOT_SUPPORTED 4008
             This error code is used by a mobility agent to indicate to
             the home Diameter server that the requested packet filter
             Rules cannot be supported.

6.2.   Permanent Failures

   Errors in 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 5024
             This error is used by the AAAF to inform the AAAH that
             allocation of a home agent in the foreign domain is not
             permitted at this time.

          DIAMETER_ERROR_END_TO_END_MIP_KEY_ENCRYPTION 5025
             This error is used by the AAAF/AAAH to inform the peer
             that the requested Mobile IPv4 session keys could not be
             delivered via a security association.

7.   Mandatory AVPs

   The following table describes the Diameter AVPs defined in the Mobile
   IPv4 application; their AVP Code values, types, and possible flag
   values; and whether the AVP MAY be encrypted.

   Due to space constraints, the short form IPFiltrRule is used to
   represent IPFilterRule, and DiamIdent is used to represent
   DiameterIdentity.

```
                                     +--------------------------+
                                     |      AVP Flag rules       |
                                     |----+-----+----+-----|----+
                     AVP   Section   |    |     |SHLD| MUST|MAY |
    Attribute Name   Code Defined   Value Type |MUST| MAY | NOT| NOT|Encr|
    ----------------------------------------|----+-----+----+-----|----|
    MIP-Reg-Request  320  7.1       OctetString| M  |  P  |    |  V  | Y  |
    MIP-Reg-Reply    321  7.2       OctetString| M  |  P  |    |  V  | Y  |
    MIP-MN-AAA-Auth  322  7.6       Grouped    | M  |  P  |    |  V  | Y  |
    MIP-Mobile-Node- 333  7.3       Address    | M  |  P  |    |  V  | Y  |
       Address
    MIP-Home-Agent-  334  7.4       Address    | M  |  P  |    |  V  | Y  |
       Address
    MIP-Candidate-   336  7.9       DiamIdent  | M  |  P  |    |  V  | N  |
       Home-Agent-Host
    MIP-Feature-     337  7.5       Unsigned32 | M  |  P  |    |  V  | Y  |
       Vector
    MIP-Auth-Input-  338  7.6.2     Unsigned32 | M  |  P  |    |  V  | Y  |
       Data-Length
    MIP-             339  7.6.3     Unsigned32 | M  |  P  |    |  V  | Y  |
       Authenticator-Length
    MIP-             340  7.6.4     Unsigned32 | M  |  P  |    |  V  | Y  |
       Authenticator-Offset
    MIP-MN-AAA-SPI   341  7.6.1     Unsigned32 | M  |  P  |    |  V  | Y  |
    MIP-Filter-Rule  342  7.8       IPFiltrRule| M  |  P  |    |  V  | Y  |
    MIP-FA-Challenge 344  7.7       OctetString| M  |  P  |    |  V  | Y  |

    MIP-Originating- 347  7.10      Grouped    | M  |  P  |    |  V  | Y  |
    Foreign-AAA
    MIP-Home-Agent-  348  7.11      DiamIdent  | M  |  P  |    |  V  | N  |
       Host
```

7.1.   MIP-Reg-Request AVP

   The MIP-Reg-Request AVP (AVP Code 320) is of type OctetString and
   contains the Mobile IPv4 Registration Request [MOBILEIP] sent by the
   mobile node to the foreign agent.

7.2.   MIP-Reg-Reply AVP

   The MIP-Reg-Reply AVP (AVP Code 321) is of type OctetString and
   contains the Mobile IPv4 Registration Reply [MOBILEIP] sent by the
   home agent to the foreign agent.

7.3.   MIP-Mobile-Node-Address AVP

The MIP-Mobile-Node-Address AVP (AVP Code 333) is of type Address and
contains the mobile node's home IP address.

7.4.   MIP-Home-Agent-Address AVP

The MIP-Home-Agent-Address AVP (AVP Code 334) is of type Address and
contains the mobile node's home agent IP address.

7.5.   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 the following:

           1   Mobile-Node-Home-Address-Requested
           2   Home-Address-Allocatable-Only-in-Home-Realm
           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., one not equal
to 0.0.0.0 or 255.255.255.255) in its Registration Request, the
foreign agent sets the Mobile-Node-Home-Address-Requested flag in the
MIP-Feature-Vector AVP to zero.

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-
Realm 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-
Realm flag in the MIP-Feature-Vector AVP.

Whenever the foreign agent sets either the
Mobile-Node-Home-Address-Requested flag or the Home-Agent-Requested
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 Generation Nonce Request" [MIPKEYS] extension,
with the subtype set to AAA.

If the mobile node includes a "Generalized MN-FA Key Generation Nonce
Request" [MIPKEYS] extension with the AAA subtype (1) 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 AAAF is willing and able to assign a home agent in the foreign
network, the AAAF sets the Foreign-Home-Agent-Available flag 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 FA-HA key with the home agent,
the foreign agent 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 both 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 and Home-Agent-In-Foreign-
Network flags 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.

7.6.   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 IPv4 Registration Request [MOBILEIP, MIPCHAL] 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 ]
```

7.6.1.   MIP-MN-AAA-SPI AVP

The MIP-MN-AAA-SPI AVP (AVP Code 341) is of type Unsigned32 and
indicates the MSA by which the targeted AAA server (AAAH) should

attempt to validate the Authenticator computed by the mobile node
over the Registration Request data.

7.6.2.   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, as indicated by the MN-AAA-SPI AVP,
used to determine whether the Authenticator Data supplied by the
mobile node is valid.

7.6.3.   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).

7.6.4.   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).

7.7.   MIP-FA-Challenge AVP

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 [MIPCHAL].

7.8.   MIP-Filter-Rule AVP

The MIP-Filter-Rule AVP (AVP Code 342) is of type IPFilterRule and
provides filter rules that have to be configured on the foreign or
home agent for the user. The packet filtering rules are set by the
AAAH by adding one or more MIP-Filter-Rule AVPs in the HAR if
destined for the home agent and/or in the AMA if destined for the
foreign agent.

7.9.   MIP-Candidate-Home-Agent-Host

The MIP-Candidate-Home-Agent-Host AVP (AVP Code 336) is of type
DiameterIdentity and contains the identity of a home agent in the
foreign network that the AAAF proposes to be dynamically assigned to
the mobile node.

7.10.   MIP-Originating-Foreign-AAA AVP

The MIP-Originating-Foreign-AAA AVP (AVP Code 347) is of type Grouped
and contains the identity of the AAAF, which issues the AMR to the

AAAH. The MIP-Originating-Foreign-AAA AVP MUST only be used in cases
when the home agent is or may be allocated in a foreign domain. If
the MIP-Originating-Foreign-AAA AVP is present in the AMR, the AAAH
MUST copy it into the HAR.

```
MIP-Originating-Foreign-AAA ::= < AVP Header: 347 >
                                { Origin-Realm }
                                { Origin-Host }
                              * [ AVP ]
```

7.11.   MIP-Home-Agent-Host AVP

The MIP-Home-Agent-Host AVP (AVP Code 348) is of type Grouped and
contains the identity of the assigned Home Agent. If the MIP-Home-
Agent-Host AVP is present in the AMR, the AAAH MUST copy it into the
HAR.

```
MIP-Home-Agent-Host ::= < AVP Header: 348 >
                            { Destination-Realm }
                            { Destination-Host }
                          * [ AVP ]
```

8.   Key Distribution

The mobile node and mobility agents use session keys (i.e., the MN-
FA, FA-HA, and MN-HA session keys) to compute authentication
extensions applied to MIP registration messages, as defined in
[MOBILEIP]. If session keys are requested, the AAAH MUST return the
keys and nonces after the mobile node is successfully authenticated
and authorized.

The SPI values are used as key identifiers, and each session key has
its own SPI value; nodes that share a key can have multiple different
SPIs all referring to the same key. In all cases, the entity that
receives an authentication extension (i.e., that verifies the
authentication extension) is providing the entity that sends the
authentication extension (i.e., that computes the authentication
extension) the value of the SPI to use for that computation. Note
that the keys in this model are symmetric in that they are used in
both directions, even though the SPIs do not have to be symmetric.

The mobile node allocates SPIs for use in the FA-MN and HA-MN
mobility security associations, via the Mobile IPv4 AAA Key Request
extensions [MIPKEYS]. The home agent allocates SPIs for the MN-HA
and FA-HA mobility security association. The foreign agent chooses
SPIs for the MN-FA and HA-FA mobility security associations.

Once the session keys and nonces have been distributed, subsequent

Mobile IPv4 registrations need not invoke the AAA infrastructure until the keys expire. As mandated by Mobile IPv4, these registrations MUST include the MN-HA authentication extension.

Likewise, subsequent registrations MUST also include MN-FA
authentication extension if the MN-FA session key was generated and
distributed by AAA. The same holds true for subsequent use of the
FA-HA authentication extensions.

8.1.   Authorization Lifetime vs. MIP Key Lifetime

The Diameter Mobile IPv4 application makes use of two timers: the
Authorization-Lifetime AVP [DIAMBASE] and the MIP-MSA-Lifetime AVP.

The Authorization-Lifetime contains the number of seconds before the
mobile node must issue a subsequent MIP registration request. The
content of the Authorization-Lifetime AVP corresponds to the Lifetime
field in the MIP header [MOBILEIP].

The MIP-MSA-Lifetime AVP contains the number of seconds before
session keys destined for the mobility agents and the mobile node
expire. A value of zero indicates infinity (no timeout). If not zero,
the value of the MIP-MSA-Lifetime AVP MUST be at least equal to the
value in the Authorization Lifetime AVP.

8.2.   Nonce vs. Session Key

As described in section 3.4, the AAAH generates session keys and
transmits them to the home agent and foreign agent. The AAAH
generates nonces that correspond to the same keys and transmits them
to the mobile node. When it is necessary to protect the session keys
and SPIs from un-trusted Diameter agents, end-to-end security
mechanisms such as TLS or IPSec are required to eliminate all
Diameter Agents between the FA or HA and the AAAH, as outlined above.

In [MIPKEYS], the mobility security associations are established via
nonces transmitted to the mobile node via Mobile IPv4. To provide the
nonces, the AAAH must generate a random [RANDOM] value of at least
128 bits [MIPKEYS]. The mobile node then uses the nonce to derive the
MN-HA and MN-FA session keys.

More details of the MN-HA and the MN-FA session key creation
procedures are found in [MIPKEYS].

The hashing algorithm used by the mobile node to construct the
session key has to be the same as that used by the AAAH in the
session key generation procedure. The AAAH therefore indicates the
algorithm used along with the nonce by including a AAA SPI.

The FA-HA and HA-FA session key is shared between the FA and HA. The
AAAH generates a random [RANDOM] value of at least 128 bits for use
as this session key.

See sections [9](#) for details about the format of the AVPs used to transport the session keys.

8.3.   **Distributing the Mobile-Home Session Key**

   If the mobile node does not have an MN-HA session key, then the AAAH
   is likely to be the only trusted entity that is available to the
   mobile node. Thus, the AAAH has to generate the MN-HA session key.

   The distribution of the HA-MN (session) key to the HA is specified in
   sections 1.2 and 3.4. The HA and AAAH establish a security
   association (IPSec or TLS) and transport the key over it. If no
   security association exists between the AAAH and the home agent and a
   security association cannot be established, the AAAH MUST return a
   Result-Code AVP with DIAMETER_ERROR_END_TO_END_MIP_KEY_ENCRYPTION.

   The AAAH also has to arrange for the key to be delivered to the
   mobile node. Unfortunately, the AAAH only knows about Diameter
   messages and AVPs, and the mobile node only knows about Mobile IPv4
   messages and extensions [MOBILEIP]. For this purpose, AAAH includes
   the MN-HA MIP-nonce AVP into a MIP-MN-to-HA-MSA AVP, which is added
   to the HAR (for FA COA style Mobile IPv4) or to the AMA (for
   collocated COA-style Mobile IPv4 messages) and delivered either to a
   local home agent or a home agent in the visited network. Note that
   the mobile node will use the nonce to create the MN-HA session key
   by using the MN-AAA key it shares with the AAAH [MIPKEYS]. The AAAH
   has to rely on the home agent (which also understands Diameter) to
   transfer the nonce into a Mobile IPv4 "Generalized MN-HA Key
   Generation Nonce Reply" extension [MIPKEYS] in the Registration Reply
   message. The HA includes the SPIs proposed by the mobile node and the
   home agent in the "Generalized MN-HA Key Generation Nonce Request"
   extension. 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 HAA's MIP-Reg-Reply AVP.

   The AAAH parses the HAA message, transforms it into an AMA message
   containing an MIP-Reg-Reply AVP, and sends the AMA message to the
   foreign agent. The foreign agent then uses that AVP to recreate a
   Registration Reply message containing the "Generalized MN-HA Key
   Generation Nonce Reply" extension for delivery to the mobile node.

   In summary, the AAAH generates the MN-HA nonce, which is added to the
   MIP-MN-to-HA-MSA AVP, and a session key, which is added to the
   MIP-HA-to-MN-MSA AVP. These AVPs are delivered to the home agent in
   HAR or AMA messages. The home agent retains the session key for its
   own use and copies the nonce from the MIP-MN-to-HA-MSA AVP into a
   "Generalized MN-HA Key Generation Nonce Reply" extension, which is
   appended to the Mobile IPv4 Registration Reply message. This
   Registration Reply message MUST also include the HA-MN authentication
   extension, which is created by using the newly allocated HA-MN

session key. The home agent then includes the Registration Reply
message and extensions into a MIP-Reg-Reply AVP as part of the HAA
message to be sent back to the AAA server.

The key derived by the MN from the MN-HA session nonce is identical
to the HA-MN session key provided to the HA.

8.4.   Distributing the Mobile-Foreign Session Key

The MN-FA session nonce is also generated by AAAH (upon request) and
added to the MIP-MN-to-FA-MSA AVP, which is added to the HAR and
copied by the home agent into a "Generalized MN-FA Key Generation
Nonce Reply" extension [MIPKEYS] of the Mobile IPv4 Registration
Reply message. The HA also includes the SPI proposed by the FA in
the "Generalized MN-FA Key Generation Nonce Reply" extension. The
AAAH includes the FA-MN session key in the MIP-FA-to-MN-MSA AVP in
the AMA, to be used by the foreign agent in the computation of the
FA-MN authentication extension.

The key derived by the MN from the MN-FA session nonce is identical
to the FA-MN session key provided to the FA.

8.5.   Distributing the Foreign-Home Session Key

If the foreign agent requests an FA-HA session key, it also includes
a MIP-HA-to-FA-SPI AVP in the AMR to convey the SPI to be used by the
home agent for this purpose. The AAAH generates the FA-HA session
key, which is identical to the HA-FA session key, and distributes
that to both the HA and the FA over respective security associations
by using the MIP-HA-to-FA-MSA and MIP-FA-to-HA-MSA AVPs. The HA
conveys the SPI that the FA MUST use in the HAA; this is similar to
the way in which the FA conveys the SPI that the HA MUST use in the
AMR. The AAAH later includes these SPIs in the MIP-FA-HA-MSA and
MIP-HA-FA-MSA AVPs, respectively, along with the session key.

Refer to Figure 2, Figure 3, Figure 4 and Figure 6 for the messages
involved.

Note that if multiple MNs are registered on the same FA and HA pair,
then multiple mobility security associations would be distributed.
However, only one is required to protect the Mobile IP control
traffic between FA and HA. This creates an unacceptable level of
state (i.e., to store the two SPIs and shared key for each FA-HA
mobility security association). To improve scalability, the FA and HA
may discard FA-HA mobility security associations prior to the time
when they actually expire. However, if a proper discard policy is
not chosen, this could cause Mobile IP messages in transit or waiting
in queues for transmission to fail authentication.

The FA MUST always use the FA-HA security association with the latest
expiry time when computing authentication extensions on outgoing

messages. The FA MAY discard HA-FA mobility security associations 10
seconds after a new HA-FA mobility security association arrives with
a later expiry time.

The HA SHOULD use the HA-FA mobility security association that has
the latest expiry time when computing authentication extensions in
outgoing messages. However, when the HA receives a new HA-FA
mobility security association with a later expiry time, the HA SHOULD
wait 4 seconds for the AMA to propagate to the FA before using the
new association. Note that the HA always uses the mobility security
association from the HAR when constructing the Mobile IP Registration
Reply in the corresponding HAA. The HA MAY discard an FA-HA mobility
security association once it receives a message authenticated by a
FA-HA mobility security association with a later expiry time.

9.   Key Distribution AVPs

The Mobile-IP protocol defines a set of mobility security
associations shared between the mobile node, foreign agent, and home
agent. These three mobility security associations (MN-HA, MN-FA, and
FA-HA) are dynamically created by the AAAH and have previously been
described in section 3.4 and section 8. AAA servers supporting the
Diameter Mobile IP Application MUST implement the key distribution
AVPs defined in this document.

The names of the key distribution AVPs indicate the two entities
sharing the mobility security association. The first named entity in
the AVP name will use the mobility security association to create
authentication extensions using the given SPI and key. The second
named entity in the AVP name will use the mobility security
association to verify the authentication extensions of received
Mobile IP messages.

For instance, the MIP-MN-to-HA-MSA AVP contains the MN-HA nonce,
which the mobile node will use to derive the MN-HA Key, and the
MIP-HA-to-MN-MSA AVP contains the MN-HA key for the home agent. Note
that mobility security associations are unidirectional; however, this
application delivers only one key that is shared between both
unidirectional security associations that exist between two peers.
The security considerations of using the same key in each direction
are given in section 13. The SPIs are, however, unique to each
unidirectional security association and are chosen by the peer that
will receive the Mobile IP messages authenticated with that security
association.

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

```
                                       +-------------------------+
                                       |      AVP Flag Rules      |
                                       |----+-----+----+-----|----+
                     AVP   Section     |    |     |SHLD| MUST|MAY |
    Attribute Name  Code Defined  Value Type |MUST| MAY | NOT|  NOT|Encr|
    ---------------------------------------|----+-----+----+-----|----|
    MIP-FA-to-HA-SPI 318  9.11    Unsigned32 | M  |  P  |    |   V | Y  |
    MIP-FA-to-MN-SPI 319  9.10    Unsigned32 | M  |  P  |    |   V | Y  |
    MIP-HA-to-FA-SPI 323  9.14    Unsigned32 | M  |  P  |    |   V | Y  |
    MIP-MN-to-FA-SPI TBD  9.16    Unsigned32 | M  |  P  |    |   V | Y  |
    MIP-MN-to-FA-MSA 325  9.5     Grouped    | M  |  P  |    |   V | Y  |
    MIP-FA-to-MN-MSA 326  9.1     Grouped    | M  |  P  |    |   V | Y  |
    MIP-FA-to-HA-MSA 328  9.2     Grouped    | M  |  P  |    |   V | Y  |
    MIP-HA-to-FA-MSA 329  9.3     Grouped    | M  |  P  |    |   V | Y  |
    MIP-MN-to-HA-MSA 331  9.6     Grouped    | M  |  P  |    |   V | Y  |
    MIP-HA-to-MN-MSA 332  9.4     Grouped    | M  |  P  |    |   V | Y  |
    MIP-Nonce        335  9.12    OctetString| M  |  P  |    |   V | Y  |
    MIP-Session-Key  343  9.7     OctetString| M  |  P  |    |   V | Y  |
    MIP-Algorithm-   345  9.8     Enumerated | M  |  P  |    |   V | Y  |
      Type
    MIP-Replay-Mode  346  9.9     Enumerated | M  |  P  |    |   V | Y  |
    MIP-MSA-Lifetime 367  9.13    Unsigned32 | M  |  P  |    |   V | Y  |
    MIP-AAA-SPI      TBD  9.15    Unsigned32 | M  |  P  |    |   V | Y  |
```

9.1.   MIP-FA-to-MN-MSA AVP

The MIP-FA-to-MN-MSA AVP (AVP Code 326) is of type Grouped and
contains the FA-MN session key. This AVP is conveyed to the FA in an
AMA message. The MN allocates the MIP-FA-to-MN-SPI. The FA creates
an FA-MN authentication extension by using the session key and
algorithm, and the MN verifies that extension by using the same
session key and algorithm. The data field of this AVP has the
following ABNF grammar:

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

9.2.   MIP-FA-to-HA-MSA AVP

The MIP-FA-to-HA-MSA AVP (AVP Code 328) is of type Grouped and
contains the FA-HA session key. This AVP is conveyed to the FA in an
AMA message. The HA allocates the MIP-FA-to-HA-SPI. The FA creates
the FA-HA authentication extension by using the session key and

algorithm, and the HA verifies that extension by using the same key
and algorithm. The AVP's data field has the following ABNF grammar:

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

9.3.   MIP-HA-to-FA-MSA AVP

The MIP-HA-to-FA-MSA AVP (AVP Code 329) is of type Grouped and
contains the Home Agent's session key, which it shares with the
foreign agent. This AVP is conveyed to the HA in an HAR message.
The FA allocates the MIP-HA-to-FA-SPI. The HA creates the HA-FA
authentication extension by using the session key and algorithm, and
the FA verifies that extension by using the same session key and
algorithm. The AVP's data field has the following ABNF grammar:

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

9.4.   MIP-HA-to-MN-MSA AVP

The MIP-HA-to-MN-MSA AVP (AVP Code 332) is of type Grouped and
contains the HA-MN session key. This AVP is conveyed to the HA in an
HAR for FA COA Mobile IPv4 and in an AMA for collocated COA Mobile
IPv4. The MN allocates the MIP-HA-to-MN-SPI. The HA creates the HA-
MN authentication extension by using the session key and algorithm,
and the MN verifies that extension by using the same key and
algorithm. The AVP's field has the following ABNF grammar:

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

9.5.   MIP-MN-to-FA-MSA AVP

The MIP-MN-to-FA-MSA AVP (AVP Code 325) is of type Grouped and
contains the MN-FA session nonce, which the mobile node uses to
derive the MN-FA session key. This AVP is conveyed to the HA in an
HAR message. The FA allocates the MIP-MN-to-FA-SPI. The MN creates
the MN-FA session key by using the nonce and an algorithm indexed by
the AAA SPI.

The home agent uses this AVP in the construction of the Mobile IP

"Generalized MN-FA Key Generation Nonce Reply" extension [MIPKEYS].

    MIP-MN-to-FA-MSA ::= < AVP Header: 325 >

```
                              { MIP-MN-FA-SPI }
                              { MIP-Algorithm-Type }
                              { MIP-nonce }
                            * [ AVP ]
```

9.6.   MIP-MN-to-HA-MSA AVP

The MIP-MN-to-HA-MSA AVP (AVP Code 331) is of type Grouped and
contains the MN-HA session nonce, which the mobile node uses to
derive the MN-HA session key. This AVP is conveyed to the HA in an
HAR message for FA COA Mobile IPv4 and in an AMA for collocated
Mobile IPv4. The HA allocates the MIP-MN-to-HA-SPI. The MN creates
the MN-HA session key using the nonce and an algorithm indexed by the
AAA SPI.

The Home Agent uses this AVP in the construction of the Mobile IP
"Generalized MN-HA Key Generation Nonce Reply" extension [MIPKEYS].

```
        MIP-MN-to-HA-MSA ::= < AVP Header: 331 >
                             { MIP-Algorithm-Type }
                             { MIP-Replay-Mode }
                             { MIP-nonce }
                           * [ AVP ]
```

9.7.   MIP-Session-Key AVP

The MIP-Session-Key AVP (AVP Code 343) is of type OctetString and
contains the Session Key for the associated Mobile IPv4
authentication extension. The HAAA selects the session key.

9.8.   MIP-Algorithm-Type AVP

The MIP-Algorithm-Type AVP (AVP Code 345) is of type Enumerated and
contains the Algorithm identifier for the associated Mobile IPv4
authentication extension. The HAAA selects the algorithm type. The
following values are currently defined:

```
        2   HMAC-SHA-1 [HMAC]
```

9.9.   MIP-Replay-Mode AVP

The MIP-Replay-Mode AVP (AVP Code 346) is of type Enumerated and
contains the replay mode the Home Agent for authenticating the mobile
node. The HAAA selects the replay mode.

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

                1   None
                2   Timestamps
                3   Nonces

9.10.   MIP-FA-to-MN-SPI AVP

   The MIP-FA-to-MN-SPI AVP (AVP Code 319) is of type Unsigned32 and
   contains the Security Parameter Index that the FA and MN use to refer
   to the FA-MN mobility security association. The MN allocates the
   SPI, and it MUST NOT have a value between zero (0) and 255, which is
   the reserved namespace defined in [MOBILEIP].

9.11.   MIP-FA-to-HA-SPI AVP

   The MIP-FA-to-HA-SPI AVP (AVP Code 318) is of type Unsigned32 and
   contains the Security Parameter Index the FA and HA   use to refer to
   the FA-HA mobility security association. The HA allocates the SPI,
   and it MUST NOT have a value between zero (0) and 255, which is the
   reserved namespace defined in [MOBILEIP].

9.12.   MIP-Nonce AVP

   The MIP-Nonce AVP (AVP Code 335) is of type OctetString and contains
   the nonce sent to the mobile node for the associated authentication
   extension. The mobile node follows the procedures in [MIPKEYS] to
   generate the session key used to authenticate Mobile IPv4
   registration messages. The HAAA selects the nonce.

9.13.   MIP-MSA-Lifetime AVP

   The MIP-MSA-Lifetime AVP (AVP Code 367) is of type Unsigned32 and
   represents the period of time (in seconds) for which the session key
   or nonce is valid. The associated session key or nonce, as the case
   may be, MUST NOT be used if the lifetime has expired; if the session
   key or nonce lifetime expires while the session to which it applies
   is still active, either the session key or nonce MUST be changed or
   the association Mobile IPv4 session MUST be terminated.

9.14.   MIP-HA-to-FA-SPI AVP

   The MIP-HA-to-FA-SPI AVP (AVP Code 323) is of type Unsigned32 and
   contains the Security Parameter Index the HA and FA use to refer to
   the HA-FA mobility security association. The FA allocates the SPI,

and it MUST NOT have a value between zero (0) and 255, which is the
reserved namespace defined in [MOBILEIP].

9.15.   MIP-AAA-SPI AVP

The MIP-AAA-SPI AVP (AVP Code TBD) is of type Unsigned32 and contains the Security Parameter Index the AAA and MN use to indicate the algorithm used to generate a Mobile IP Session Key from a Mobile IP Nonce. It appears in registration replies according to [MIPKEYS].

9.16.   MIP-MN-to-FA-SPI AVP

The MIP-MN-to-FA-SPI AVP (AVP Code TBD) is of type Unsigned32 and contains the Security Parameter Index the MN and FA use to refer to the MN-FA mobility security association. The FA allocates the SPI, and it MUST NOT have a value between zero (0) and 255, which is the reserved namespace defined in [MOBILEIP].

10.   Accounting AVPs

10.1.   Accounting-Input-Octets AVP

The Accounting-Input-Octets AVP (AVP Code 363) is of type Unsigned64, and contains the number of octets in IP packets received from the user. This AVP MUST be included in all Accounting-Request messages and MAY be present in the corresponding Accounting-Answer messages as well.

10.2.   Accounting-Output-Octets AVP

The Accounting-Output-Octets AVP (AVP Code 364) is of type Unsigned64 and contains the number of octets in IP packets sent to the user. This AVP MUST be included in all Accounting-Request messages and MAY be present in the corresponding Accounting-Answer messages as well.

10.3.   Acct-Session-Time AVP

The Acct-Time AVP (AVP Code 46) is of type Unsigned32 and indicates the length of the current session in seconds. This AVP MUST be included in all Accounting-Request messages and MAY be present in the corresponding Accounting-Answer messages as well.

10.4.   Accounting-Input-Packets AVP

The Accounting-Input-Packets (AVP Code 365) is of type Unsigned64 and contains the number of IP packets received from the user. This AVP

MUST be included in all Accounting-Request messages and MAY be present in the corresponding Accounting-Answer messages as well.

10.5.   **Accounting-Output-Packets AVP**

   The Accounting-Output-Packets (AVP Code 366) is of type Unsigned64
   and contains the number of IP packets sent to the user. This AVP MUST
   be included in all Accounting-Request messages and MAY be present in
   the corresponding Accounting-Answer messages as well.

10.6.   **Event-Timestamp AVP**

   The Event-Timestamp (AVP Code 55) is of type Time and MAY be included
   in an Accounting-Request message to record the time at which this
   event occurred on the mobility agent, in seconds since January 1,
   1970, 00:00 UTC.

11.   **AVP Occurrence Tables**

   The following tables present the AVPs defined in this document and
   their occurrences in Diameter messages. 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.

11.1.   **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 | 0-1 | 1   | 0   |
   Auth-Application-Id              | 1   | 1   | 1   | 1   |
   Auth-Session-State              | 0-1 | 0-1 | 1   | 0   |
   Acct-Multi-Session-Id           | 0-1 | 0-1 | 0   | 0-1 |
   Destination-Host                | 0-1 | 0   | 0-1 | 0   |
   Destination-Realm               | 1   | 0   | 1   | 0   |
   Error-Message                   | 0   | 0-1 | 0   | 0-1 |
   Error-Reporting-Host            | 0   | 0-1 | 0   | 0-1 |
   MIP-Candidate-Home-Agent-Host   | 0-1 | 0   | 0-1 | 0   |
   MIP-Home-Agent-Host             | 0-1 | 0   | 0-1 | 0   |
   MIP-Originating-Foreign-AAA     | 0-1 | 0   | 0-1 | 0   |
   MIP-FA-Challenge                | 0-1 | 0   | 0   | 0   |
   MIP-FA-to-MN-MSA                | 0   | 0-1 | 0   | 0   |
   MIP-FA-to-HA-MSA                | 0   | 0-1 | 0   | 0   |
   MIP-HA-to-FA-MSA                | 0   | 0   | 0-1 | 0   |
   MIP-HA-to-MN-MSA                | 0   | 0-1 | 0-1 | 0   |
   MIP-MN-to-FA-MSA                | 0   | 0   | 0-1 | 0   |
   MIP-MN-to-HA-MSA                | 0   | 0-1 | 0-1 | 0   |
   MIP-FA-to-HA-SPI                | 0   | 0   | 0   | 0-1 |
   MIP-HA-to-FA-SPI                | 0   | 0   | 0   | 0-1 |

   MIP-FA-to-MN-SPI                | 0   | 0   | 0   | 0-1 |
   MIP-MN-to-FA-SPI                | 0   | 0   | 0   | 0-1 |

   MIP-HA-to-MN-SPI                | 0   | 0   | 0   | 0-1 |
   MIP-MN-to-HA-SPI                | 0   | 0   | 0   | 0-1 |
   MIP-Feature-Vector              | 0-1 | 0-1 | 1   | 0   |
   MIP-Filter-Rule                 | 0   | 0+  | 0+  | 0   |
   MIP-Home-Agent-Address          | 0-1 | 0-1 | 0-1 | 0-1 |
   MIP-MSA-Lifetime                | 0   | 0-1 | 0-1 | 0   |
   MIP-MN-AAA-Auth                 | 1   | 0   | 0   | 0   |
   MIP-Mobile-Node-Address         | 0-1 | 0-1 | 0-1 | 0-1 |
   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   |
   Origin-State-Id                 | 0-1 | 0-1 | 0-1 | 0-1 |
   Proxy-Info                      | 0+  | 0+  | 0+  | 0+  |
```

```
Redirect-Host                  | 0   | 0+  | 0   | 0+  |
Redirect-Host-Usage            | 0   | 0-1 | 0   | 0-1 |
Redirect-Max-Cache-Time        | 0   | 0-1 | 0   | 0-1 |
Result-Code                    | 0   | 1   | 0   | 1   |
```

```
      Re-Auth-Request-Type            | 0   | 0-1 | 0   | 0   |
      Route-Record                    | 0+  | 0   | 0+  | 0   |
      Session-Id                      | 1   | 1   | 1   | 1   |
      User-Name                       | 1   | 0-1 | 1   | 0-1 |
      -----------------------------|-----+-----+-----+-----|
```

11.2.   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, as
   defined in [DIAMBASE].

```
                                      +-------------+
                                      | 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 |
      Acct-Multi-Session-Id           |  1   | 0-1 |
      Acct-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 |
      Event-Timestamp                 | 0-1  |  0  |
      -------------------------------|------+------+
```

12.   IANA Considerations

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

12.1.   Command Codes

   This specification assigns the values 260 and 262 from the Command
   Code namespace defined in [DIAMBASE]. See section 5 for the
   assignment of the namespace in this specification.

12.2.   AVP Codes

   This specification assigns the values 318 - 348 and 363 - 367 from
   the AVP Code namespace defined in [DIAMBASE]. See sections 7, 9, and

10 for the assignment of the namespace in this specification.

12.3.   **Result-Code AVP Values**

   This specification assigns the values 4005 - 4008 and 5024 - 5025
   from the Result-Code AVP (AVP Code 268) value namespace defined in
   [DIAMBASE]. See section 6 for the assignment of the namespace in
   this specification.

12.4.   **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 7.5. The remaining bits should only be assigned
   via Standards Action [IANA].

12.5.   **MIP-Algorithm-Type AVP Values**

   As defined in section 9.8, the MIP-Algorithm-Type AVP (AVP Code 345)
   defines the value 2. All remaining values, except zero, are
   available for assignment via Designated Expert [IANA].

12.6.   **MIP-Replay-Mode AVP Values**

   As defined in section 9.9, the MIP-Replay-Mode AVP (AVP Code 346)
   defines the values 1-3. All remaining values, except zero, are
   available for assignment via Designated Expert [IANA].

12.7.   **Application Identifier**

   This specification uses the value two (2) in the Application
   Identifier namespace defined in [DIAMBASE]. See section 4 for more
   information.

13.   **Security Considerations**

   This specification describes a Mobile IPv4 Diameter Application for
   authenticating and authorizing a Mobile IPv4 mobile node. The
   authentication algorithm used is dependent on the transforms used
   within the Mobile IPv4 protocol, and [MIPCHAL]. This specification,
   in conjunction with [MIPKEYS], also defines a method by which the
   home Diameter server can create and distribute session keys and
   nonces for use in authenticating and integrity-protecting Mobile IPv4
   registration messages [MOBILEIP]. The key distribution is
   asymmetric, as communication with the mobile node occurs via the
   Mobile IPv4 protocol [MIPKEYS, MOBILEIP], where as communication to

the Home Agent and Foreign Agent occurs via the Diameter protocol.
Where untrusted Diameter agents are present, end-to-end security MUST
be used. The end-to-end security takes the form of TLS or IPSec

security associations between the AAAH and the FA and between the
AAAH and the HA. These connections will be authenticated with the
use of public keys and certificates; however, the identities that
appear in the certificates must be authorized and bound to a
particular Mobile IPv4 Diameter session before the AAAH can safely
begin distribution of keys.

Note that the direct connections are established as a result of
Diameter redirect messages. For example, in Figure 3, the FA gets a
redirect response containing the Redirect-Host AVP of the AAAH. This
is the identity that should be matched against the certificate
presented by the AAAH when the secure connection is established. In
this case, the network of Diameter proxies and redirect agents is
trusted with the task of returning the correct AAAH identity to the
FA.

The AAAH must also make an authorization decision when the FA
establishes the connection. If the AAAH and the redirect server are
one and the same, then the AAAH may have observed and noted the
original AMR message that contained the identity of the FA and so may
authorize the establishment of a TLS or IPSec connection from the
same entity. Otherwise, the AAAH would need to maintain a list of
all authorized visited domains (roaming partners) and authorize TLS
or IPSec connections based on this list. Note that establishment of
the connection is only the first step, and the AAAH has another
opportunity to deny service upon receipt of the AMR message itself.
At this step, the AAAH can check the internal AVPs of the AMR to
ensure that the FA is valid; for example, it can check that the
Mobile IP COA is equal to the IP address used as the endpoint of the
TLS or IPSec connection. However, such a policy would prevent the FA
from using different interfaces for AAA and Mobile IP tunnel packets
and may not be desirable in every deployment situation.

A similar set of considerations applies to the connection between
AAAH and HA when those entities are in different administrative
domains. However, here the roles are reversed because it is the AAAH
that contacts the HA via the HAR. The identity of the candidate HA
is given to the AAAH in the AMR, and the AAAH should expect to
receive the same identity in the public key certificates during TLS
or IPSec negotiation. The HA may authorize individual connections by
acting as its own redirect server, or it may maintain a list of
trusted roaming partners.

This application creates and distributes a single session key for
each pair of MSAs between two entities; e.g., the same session key is
used for the MN-HA MSA and the HA-MN MSA. This is safe to do from a
security perspective, as the session keys are only used with keyed
hash functions to generate authenticator values that protect the

integrity of each Mobile IP control message. Mobile IP messages have
built-in replay protection with the use of timestamps or nonces
[MOBILEIP], and, due to the nature of the protocol, requests are
always different bitwise from responses, at least in the message type
code. This avoids problems that might arise in other situations

where an attacker could mount a replay or reflection attack if the
same key were used (for example) to encrypt otherwise unprotected
traffic on more than one connection leg in the network.

Nonces are sent to the mobile node, which are used to generate the
session keys via the HMAC-SHA-1 one-way function. Because the nonces
and authentication extensions may be observed by anyone with access
to a clear-text copy of the Registration Reply, the pre-shared key
between the mobile node and the home Diameter server would be
vulnerable to an offline dictionary attack if it did not contain
enough entropy. To prevent this, the pre-shared key between the
mobile node and the home Diameter server SHOULD be a randomly chosen
quantity of at least 96 bits.

Because the session key is determined by the long-term secret and the
nonce, the nonce SHOULD be temporally and globally unique; if the
nonce were to repeat, then so would the session key. To prevent
this, a nonce is strongly recommended to be a random [RANDOM] value
of at least 128 bits. The long-term secret between the MN and AAAH
MUST be refreshed periodically, to guard against recovery of the
long-term secret due to nonce reuse or other factors. This is
accomplished by using out-of-band mechanisms, which are not specified
in this document.

Note that it is not recommended to set the MIP-MSA-Lifetime AVP value
to zero, as keeping session keys for a long time (no refresh)
increases the level of vulnerability.

14. References

14.1.   Normative References

   [ABNF]   Crocker, D. and P. Overell, "Augmented BNF for Syntax
                 Specifications: ABNF", RFC 2234, November 1997.

   [DIAMBASE]   Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and
                 J. Arkko, "Diameter Base Protocol", RFC 3588,
                 September 2003.

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

   [MOBILEIP]   Perkins, C., "IP Mobility Support for IPv4", RFC 3344,
                 August 2002.

   [MIPCHAL]   Perkins, C. and P. Calhoun, "Mobile IPv4
                    Challenge/Response Extensions", RFC 3012, November
                    2000.

   [NAI]   Aboba, B. and M. Beadles, "The Network Access
                  Identifier", RFC 2486, January 1999.

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

   [MIPKEYS]   Perkins, C. and P. Calhoun, "Authentication,
                  Authorization, and Accounting (AAA) Registration Keys
                  for Mobile IP", RFC 3957, March 2005.

   [AAANAI]   Johansson, F. and T. Johansson, "Mobile IPv4 Extension
                  for Carrying Network Access Identifiers", RFC 3846,
                  June 2004.

   [IPSEC]   Kent, S. and R. Atkinson, "Security Architecture for
                  the Internet Protocol", RFC 2401, November 1998.

   [TLS]   Blake-Wilson, S., Nystrom, M., Hopwood, D., Mikkelsen,
                  J., and T. Wright, "Transport Layer Security (TLS)
                  Extensions", RFC 3546, June 2003.

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

14.2.   Informative References

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

   [CDMA2000]   Hiller, T., Walsh, P., Chen, X., Munson, M., Dommety,
                  G., Sivalingham, S., Lim, B., McCann, P., Shiino, H.,
                  Hirschman, B., Manning, S., Hsu, R., Koo, H., Lipford,
                  M., Calhoun, P., Lo, C., Jaques, E., Campbell, E., Xu,
                  Y., Baba, S., Ayaki, T., Seki, T., and A. Hameed,
                  "CDMA2000 Wireless Data Requirements for AAA", RFC
                  3141, June 2001.

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

   [MIPNAI]   Calhoun, P. and C. Perkins, "Mobile IP Network Access
                  Identifier Extension for IPv4", RFC 2794, March 2000.

[RANDOM]   Eastlake, D., 3rd, Schiller, J., and S. Crocker,
               "Randomness Requirements for Security", BCP 106, RFC
               4086, June 2005.

[15](#). Acknowledgements

The authors would like to thank Nenad Trifunovic, Haseeb Akhtar, and
Pankaj Patel for their participation in the pre-IETF Document Reading
Party; Erik Guttman for his very useful proposed text; and Fredrik
Johansson, Martin Julien, and Bob Kopacz for their very useful
contributed text.

The authors would also like to thank the participants of 3GPP2's
TSG-X working group for their valuable feedback, and the following
people for their contribution in the development of the protocol:
Kevin Purser, Thomas Panagiotis, Mark Eklund, Paul Funk, Michael
Chen, Henry Haverinen, and Johan Johansson. General redirect server
text due to Pasi Eronen was borrowed from Diameter-EAP.

Pat Calhoun would like to thank Sun Microsystems, as most of the
effort put into this document was done while he was in their employ.

Authors' Addresses

Questions about this memo can be directed to:

Pat Calhoun
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134
USA

Phone: +1 408-853-5269
EMail: pcalhoun@cisco.com

Tony Johansson
Bytemobile, Inc.
2029 Stierlin Court
Mountain View, CA 94043

Phone: +1 650-641-7817
Fax: +1 650-641-7701
EMail: tony.johansson@bytemobile.com

Charles E. Perkins
Nokia Siemens Networks
323 Fairchild Dr.
Mountain View, CA 94043

USA

   Email: charles.perkins@nsn.com

Tom Hiller
Alcatel-Lucent
1960 Lucent Lane
Naperville, IL 60566
USA

Phone: +1 630-979-7673
EMail: tomhiller@alcatel-lucent.com

Peter J. McCann
Motorola
MD 2240
1301 E. Algonquin Rd
Schaumburg, IL 60196
USA

Phone: +1 847-576-3440
EMail: pete.mccann@motorola.com

Full Copyright Statement

Intellectual Property

Acknowledgement