INTERNET DRAFT
Category: Standards Track
Title: draft-calhoun-mobileip-proactive-fa-03.txt
Date: November 2000

Pat R. Calhoun
Sun Microsystems, Inc.
Tom Hiller
Lucent Technologies
James Kempf
Sun Microsystems, Inc.
Peter J. McCann
Lucent Technologies
Chandana Pairla
University of Illinois
Ajoy Singh
Sebastian Thalanany
Motorola

Foreign Agent Assisted Hand-off

Status of this Memo

Abstract

The Mobile IP protocol allows a Mobile Node to continue using the same home address even after changing its point of attachment to the Internet. This provides transparency to most existing applications that assume a fixed address and a fixed point of attachment. However, new applications, such as voice-over-IP, have additional real-time requirements such that a change in the point of attachment will cause a noticeable degradation of service unless additional steps are taken to reduce the latency of a handoff event.

This specification proposes extensions to the Mobile IP protocol that may be used by Foreign Agents to set up a Mobile Node's visitor entry, and forward its packets, prior to receiving a formal Registration Request from the Mobile Node. This enables a very rapid establishment of service at the new point of attachment so that the effect of the handoff on real-time applications is minimized.

Table of Contents

1.0 Introduction

This specification proposes extensions to the Mobile IP protocol that may be used by Foreign Agents to set up a Mobile Node's visitor entry, and forward its packets, prior to receiving a formal Registration Request from the Mobile Node. This enables a very rapid establishment of service at the new point of attachment so that the effect of the handoff on real-time applications is minimized. The proposed extensions make a few minimal assumptions about support available from the link layer. These assumptions are fairly broad and abstract. Although they address the kinds of link layer support available in existing radio link layers, the assumptions are not based on any specific radio link protocol.

The extensions handle both intra-domain and inter-domain handoff. While intra-domain handoff MAY make use of pre-configured security associations between Mobility Agents, inter-domain handoffs MAY make use of the AAA infrastructure. In the case of inter-technology handoff, active involvement by the mobile is necessary to switch from one network interface to another; however, the delivery of the agent advertisements, indicating the availability of a mobility agent on a new network interface, is still controlled by network assisted handoff.

In summary, this draft covers a hand-off scenario not addressed by RFC 2002: that of a pro-active, network-controlled, anchor-chained hand-off.

1.1 Requirements language

In this document, the key words "MAY", "MUST, "MUST NOT", "optional", "recommended", "SHOULD", and "SHOULD NOT", are to be interpreted as described in [4].

1.2 Terminology

This document frequently uses the following terms:

AAA
Authentication, accounting and authorization.

Anchor Foreign Agent (AFA)
A foreign agent with publicly routable IP address that acts as an anchor point when a mobile moves to a new foreign agent. Upon successful global registration (registration with home agent) of a mobile node, the anchor foreign agent supports

local registration when the mobile node changes its point of attachment to some other neighboring foreign agents.

cdma2000

This is a wide-band radio transmission technology standard, that uses CDMA(code division multiple access) technology, to meet the demands of a third-generation wireless communication system.

Connection ID

A number used to differentiate different link layer connections originated from the same device.

Dormant mode

Certain wireless technologies support dormancy, which allows the mobile to go into power saving mode. This typically occurs when the mobile has been idle for some time, but could be initiated by the network.

Foreign Agent IP Address Derivation

The derivation of the IP address of a source foreign agent or a target foreign agent based on the receipt of a link layer trigger at the target foreign agent or the source foreign agent respectively.

Gateway Foreign Agent(GFA)

A foreign agent with publicly routable IP address that acts as a concentration point for other foreign agents within an administrative domain. Upon successful global registration (registration with Home agent) of a mobile node, the GFA supports local registration when the mobile node changes its point of Attachment to some other foreign agent of the same administrative Domain.

Home Domain

The domain where the home network [1] and home agent [1] are located.

International Mobile Subscriber information (IMSI)

A number used for identifying a mobile subscriber station.

Link layer

A link layer specifies a protocol used by communicating nodes to exchange information over a physical link. A mobile node attaches itself to a mobile access network, before it can be served by a foreign agent. A mobile node's link layer address is the media access control(MAC) address of the mobile node's network interface.

Mobility Agent
A foreign agent or a home agent. The foreign agent types include an anchor foreign agent and a gateway foreign agent.

Mobility Advertisement
An advertisement message constructed by attaching a special extension to a router advertisement message.

Movement Detection
A detection of a movement in the link layer attachement of the mobile node to a mobile access network.

Ping-Pong Handoff
The rapid oscillation of a mobile node among coverage area of two or more foreign agents.

Proactive Foreign agent
A foreign agent that initiates mobile/IP registration on behalf of a mobile node due to reception of some link layer trigger event.

Source Trigger
A signal received by the source foreign agent mobile/IP stack, via the link layer, when the mobile node departs from the serving area of the source foreign agent.

Target Trigger
A signal received by the target foreign agent mobile/IP stack, via the link layer, when the mobile node arrives at the serving area of the target foreign agent.

Trigger
The link layer signal used by wireless link layer to inform inter foreign agent handoff event to Mobile/IP stack.

Visited Domain
An administrative domain, visited by a Mobile IP client, and containing the AAA infrastructure needed to carry out the necessary operations enabling Mobile IP registrations. From the point of view of the foreign agent, the foreign domain is the local domain.

1.2 Fast handoffs

MNs connect to FAs via direct, link-layer connections. Because an FA is directly connected to the link-layer, it may obtain link-layer information such as power measurements that might indicate the

necessity of a hand-off to a new FA. The FA can also gain assurance of the MN's identity through link-layer authentication, and can authenticate the stream of traffic coming from the MN, including any power measurements or other indications used for hand-off.

In this document, we will assume that the link-layer events are signaled to the Foreign Agent as "triggers". The acquisition of a "trigger" to signal that a hand-off is necessary may be more difficult when the technologies differ. We assume that any such triggers will be sufficient to derive the IP addresses of the Foreign Agents that will receive or send the hand-off. If such a trigger is not available or if the MN decides on its own that a hand-off is to take place, then one of the FAs can often still derive the identity (IP address) of the other from link-layer messages.

In order for the Mobile IP protocol to provide fast hand-off, the following problems must be addressed:

1. Reducing the latency involved in the registration process. Although optimization of the Registration process is not typically considered a Hand-Off problem, this proposal assumes that such a mechanism is in place.
2. Reducing the latency involved in the Mobile Node's movement detection process.
3. "Bi-casting" the Mobile Node's traffic to two (or more) points of attachment, ensuring that the mobile's traffic is delivered as soon as the link layer hand-off is completed.
4. Support for Reverse Tunneling, which MAY be required for private addresses.
5. The Security Relationships between the mobility entities for inter-domain hand-offs.
6. Does not increase mobile power consumption

2.0 Registration Latency

The Mobile IP protocol [1] requires that a Mobile Node registers with a Foreign Agent, and subsequently its Home Agent, in order to have its packets delivered to its current point of attachment. The Mobile IP Regional Registration [6] specification proposes optimized registration approaches using two different methods:

1. Gateway Foreign Agents (GFA), which are mobility agents that act as concentration points for Foreign Agents within an Administrative Domain.
2. Anchor Foreign Agents (AFA), where a previously used Foreign Agent becomes an anchor point when a mobile moves to a new Foreign Agent.

Both GFAs and AFAs allow a Mobile Node's registration message to be processed by a Mobility Agent in the local domain, eliminating the need to contact the Home Agent, which MAY be topologically distant.

2.1 Gateway Foreign Agents

The Mobile IP Regional Registration specification introduces the Gateway Foreign Agent (GFA), as a mobility agent that two Foreign Agents providing service to a Mobile Node have in common. Figure 1 provides an example of a Mobile's initial registration, through the GFA. Given this is the first registration message, the message MUST be forwarded to the Home Agent. All packets destined for the mobile will be delivered to the GFA, which in turn will forward the packets to the Foreign Agent servicing the Mobile Node.

```
                Reg Req   +-----+   Reg Req
             +----------->| oFA |--------------+
             |            +-----+              |
             |                                 v
          +----+                            +-----+ Reg Req +----+
          | MN |                            | GFA |<------->| HA |
          +----+                            +-----+         +----+

                           +-----+
                           | nFA |
                           +-----+
```

Figure 1 - Initial Registrations through GFA

In the event that the mobile moves to a new Foreign Agent that is serviced by a GFA that is common with oFA, the Mobile Node MAY issue a Regional Registration Request (see Figure 2). The Regional Registration message does not need to be forwarded to the Home Agent, since the mobile's traffic can still be delivered to the same GFA. This optimized approach effectively reduces the latency involved in the registration process.

```
                           +-----+
                           | oFA |
                           +-----+

          +----+                            +-----+         +----+
          | MN |                            | GFA |         | HA |
          +----+                            +-----+         +----+
             |                                 ^
             |             +-----+             |
             +------------>| nFA |-------------+
              Regional Reg +-----+ Regional Reg
```

Figure 2 - Regional Registration through GFA

2.2 Anchor Foreign Agent

The Mobile IP Regional Registration specification introduces what this document will call the Anchor Foreign Agent, which is similar to [7]. The Anchor Foreign Agent operates very similarly to the GFA, with the exception that the mobile's old Foreign Agent acts as an anchor point for the Mobile Node.

In order to minimize the latency involved in the registration process, the Mobile Node MAY issues a Regional Registration message, setting the old Foreign Agent as the GFA, as shown in Figure 3. Once completed, the Mobile Node MAY issue an additional RFC 2002 compliant Registration Messages to eliminate the routing leg through the anchor Foreign Agent.

```
                           +-----+                           +----+
                           | oFA |                           | HA |
                           +-----+                           +----+
                              ^
          +----+              |
          | MN |              | Regional
          +----+              | Reg
             |                |
             |             +-----+
             +------------>| nFA |
              Regional Reg +-----+
```

Figure 3 - Regional Registrations through an AFA

3.0 Movement Detection

The Mobile IP protocol [1] and the Regional Registration extension [6] require Mobile Nodes to listen for, or solicit, advertisements in order to detect that a movement to a new IP subnet has occurred. This

movement detection mechanism introduces significant latency into the hand-off process, which causes service degradation, especially for real-time services. Service is further impacted given the additional latency introduced through the registration process that follows the movement detection, since the mobile's traffic can only be delivered once all of the registration has completed.

There have been many solutions proposed to solve this problem, including increasing the advertisement frequency. In networks where radio spectrum is expensive or bandwidth is limited, the additional signaling required for increasing advertisement frequency is a serious issue impacting deployability.

In this document, we propose that the Foreign Agent take a pro-active approach and issue the Handoff messages on behalf of the Mobile Node (acting as a surrogate of sorts). When a Foreign Agent is aware that a hand-off is occurring at the link-layer, a trigger is sent to the Mobile IP protocol stack.

```
                                          +-----+
                                          | GFA |
                                          +-----+
                                           ^  |
                           3. Regional     |  | 4. Regional
                              Reg Request  |  |    Reg Reply
                                           |  v
               +-----+ 1. Handoff Request +-----+
               |     | -----------------> |     |
               | oFA |                    | nFA |
               |     | 2. Handoff Reply   |     |
               +-----+ <----------------- +-----+

               +-----+    Movement        +-----+
               | MN  | - - - - - - - - -> | MN  |
               +-----+                    +-----+
```

Figure 4 - Source Trigger Pro-Active Handoff

A source trigger (see Figure 4) is one that is obtained by the old Foreign Agent (oFA) once the link layer detects that the Mobile Node is departing its coverage area. A target trigger (see Figure 5), on the other hand, is one that is obtained by the new Foreign Agent (nFA) once the link layer detects that the Mobile Node is arriving in its coverage area. Note that both triggers may be available before the actual completion of the link layer handoff.

The messages depicted in both Figures 4 and 5 are very similar. The main difference is the initiator of the Handoff Request message. In both examples, an optional Gateway Foreign Agent is used, which

requires the use of the Regional Registration messages [6].

In both the source and target triggers, a Foreign Agent obtains link-layer information, such as power measurements, that indicate the necessity of a handoff to the new Foreign Agent.

In the event of a source trigger, oFA transmits a Handoff Request message to nFA. The Handoff Request MUST include the Mobile Node's Home Address, Home Agent Address, remaining registration lifetime, as well as the Link-Layer Address Extension (see Section 10). The GFA's identity MUST also be present, if one was used for the Mobile Node's registration. Upon receipt of the message, nFA MUST create the Mobile Node's visitor entry, and respond with the Handoff Reply message.

```
                           +-----+
                           | GFA |
                           +-----+
                            ^  |
            3. Regional     |  | 4. Regional
               Reg Request  |  |    Reg Reply
                            |  v
+-----+ 1. Handoff Request +-----+
|     | <----------------- |     |
| oFA |                    | nFA |
|     | 2. Handoff Reply   |     |
+-----+ -----------------> +-----+

+-----+    Movement        +-----+
| MN  | - - - - - - - - -> | MN  |
+-----+                    +-----+
```

Figure 5 - Target Trigger Pro-Active Handoff

In target triggers, the trigger occurs on nFA, which results in the transmission of a Handoff Request to oFA. The Handoff Request message MUST include the Mobile Node's Link-Layer Address (see Section 10) in order for oFA to correctly identify the Mobile Node. The request message MAY include additional Mobile Node information, if such information was provided by the link layer. Upon receipt of the request, oFA MUST respond with the Handoff Reply message, which includes the Mobile Node's Home Address, Home Agent Address, remaining registration lifetime and Link-Layer Address Extension. If a GFA was used in the Mobile Node's registration, it's address MUST be supplied.

Regardless of the direction of the Handoff Request, if nFA receives GFA information within the message from oFA, it SHOULD issue a Regional Registration Request with the GFA, which will respond with the Regional Registration Reply.

3.1 Ping-Pong effect

Some link-layers are subject to rapid motion of MNs between two FAs. For example, even though link-layer power measurements may indicate that a hand-off is necessary, the mobile may fail to attach to the new point of attachment, and return almost immediately to its old point of attachment. This event is known as a "ping-pong" effect.

```
                   Data    +-----+           Data            +----+
             +-------------| oFA |<--------------------------| HA |
             |             +-----+                           +----+
             v              ^   |
          +----+    Handoff |   | Data
          | MN |    Request |   |
          +----+            |   |
             ^              v   v
             |             +-----+
             +-------------| nFA |
                   Data    +-----+
```

Figure 6 - Bi-Casting by the Anchor Foreign Agent

Figure 6 provides an example of bi-casting a Mobile Node's through both the old and new Foreign Agents. Bi-casting is established when the oFA issues a successful Handoff Reply to nFA, or receives a successful Handoff Reply from nFA. This causes oFA to forward all of the Mobile Node's traffic to the nFA, as well as to the Mobile Node, if a link-layer channel exists.

Figure 7 provides an example where bi-casting is performed on the Gateway Foreign Agent, which is initiated by nFA setting the 'S' bit (Simultaneous Binding) in the Regional Registration Request.

```
                    Data   +-----+     Data
             +-------------| oFA |<-------------+
             |             +-----+              |
             v                                  |
          +----+                             +-----+  Data   +----+
          | MN |                             | GFA |<--------| HA |
          +----+                             +-----+         +----+
             ^                                  |
             |             +-----+              |
             +-------------| nFA |<-------------+
                    Data   +-----+     Data
```

Figure 7 - Bi-Casting by the Gateway Foreign Agent

When simultaneous bindings are in effect, and a ping-pong event

occurs, the mobile's service is guaranteed not to experience any additional latency beyond that imposed by the link-layer handoff.

4.0 Reverse Tunneling Support

In the event the Mobile Node requested Reverse Tunneling [12] support, by setting the 'T' bit in its Registration Request, the Handoff message from oFA (see Sections 8.0 and 9.0) includes the 'T' bit enabled to inform nFA to establish a bi-directional tunnel for the visitor entry.

5.0 Security Relationships

The Mobile IP Regional Registration specification [6] requires that the communicating Mobility Agents exchange authenticated messages. This imposes a requirement for Mobility Agents to share a pre-established security association. This assumption is valid for intra-domain mobility (mobility within an Administrative Domain). However, such a requirement introduces a scaling problem when the Mobility Agents are owned by separate Administrative Domains (ADs).

Given that the existing AAA infrastructure is used to establish dynamic security associations between Foreign and Home Agents in different ADs, the same infrastructure could be used to establish the required security association for the purposes of inter-domain hand-offs (see Figure 8).

```
                      +-----+               +-----+
                      | AAA |-------------->| AAA |
                      +-----+               +-----+
                         ^                     |
                         |                     |
                         | AAA                 |
                         | Hand-Off            |
                         | Req                 |
                         |                     v
                      +-----+               +-----+
                      | oFA |               | nFA |
                      +-----+               +-----+

                      +-----+    Movement   +-----+
                      | MN  | - - - - - - > | MN  |
                      +-----+               +-----+
```

Figure 8 - Inter-FA communication using AAA

Note that it is possible for geographically neighboring Foreign

Agents owned by different Administrative Domains to have a pre-established security association, which would reduce the latency introduced by the AAA infrastructure traversal. Given that such geographically neighboring FAs MAY be small in number, such an approach MAY be reasonable.

6.0 Power Consumption

An additional benefit that derives from this proposal is the potential for tracking mobile nodes while in dormant mode, if the radio link supports it, allowing significant power saving without adding additional complexity to the network layer protocol in the wired network. One of the primary innovations proposed here, namely to allow the Foreign Agents to set up visitor entries prior to the Mobile Node's registration, is also useful for power saving. Certain radio link layers allow the mobile node to enter dormant mode when idle. Allowing the network to control the handoff ensures that the mobiles do not have to be removed out of dormant mode in order to establish a Mobile IP handoff.

Limiting power consumption is a requirement for certain wireless Standards Defining Organizations (SDOs), and a Mobile IP fast handoff proposal MUST satisfy this requirement.

7.0 Operation

A Foreign Agent can receive two different types of triggers informing it of a handoff (The event that causes the trigger may be derived via link layer messaging assistance from the network or from the mobile):

- a "source trigger" is when the old FA is informed of an upcoming link-layer handoff,
- a "target trigger" occurs at the new FA when it is informed that a link layer handoff is in progress.

The method by which such triggers occur are link-layer specific, and are outside the scope of this document. It is also possible that a particular kind of link layer technology can support both source and target triggers.

7.1 Foreign Agent Considerations

Upon receipt of a trigger event, a Foreign Agent MAY issue a Handoff request message to the Foreign Agent the mobile is being handed off to/from. If the message is the result of a target trigger, the Type

Of Trigger bit MUST be set and the Link-Layer Address Extension (see Section 10) MUST be present. The message's Home Address and Home Agent Address fields MAY be set to NULL if this information is not known at the time the message is transmitted.

Upon receipt of a Handoff Request message with the Type Of Trigger bit set, a Foreign Agent MUST respond with the Handoff Reply message. The Handoff Reply MUST include both the Mobile Node's Home Address and Home Agent Address in the message header. The remaining mobile's registration lifetime MUST be included in the Reply's lifetime field. Furthermore, the Foreign Agent MAY include any security associations that were dynamically created, an example of such security associations are those described in [8]. If a Gateway Foreign Agent was used in the Mobile's registration, the GFA's identity MUST be included in the Gateway Foreign Agent Address Extension [6] MUST be present.

A Foreign Agent that issues such a Handoff Reply with the Code field set to success (zero value) MUST "bi-cast" all packets destined to the Mobile Node to both the Mobile Node and to the new Foreign Agent.

The Foreign Agent that receives a successful Handoff Reply message (one that includes a zero value in the Code field), a visitor entry is created with the information found in the message. The Foreign Agent MUST be prepared to deliver packets to the Mobile Node prior to receiving a Registration Request [1] from the Mobile Node.

Note that it is possible for the encapsulation method used between oFA and nFA to be different from the one requested by the Mobile Node during its Registration process. When this occurs, the respective Foreign Agents MUST perform encapsulation translation.

A Foreign Agent that receives a source trigger, it MUST send a Handoff Request message with the Type Of Trigger bit disabled. The message MUST also include the Mobile Node's Home Address and Home Agent Address in the message header. The remaining mobile registration lifetime MUST be included in the lifetime field. The Foreign Agent MAY also include any security associations that were dynamically created (see [8] for an example). If a Gateway Foreign Agent was used for the mobile, it's identity MUST be included in the Gateway Foreign Agent Address Extension [6].

Upon receipt of a Handoff Request with the Type Of Trigger bit disabled, a Foreign Agent MUST process the packet and respond with the Handoff Reply message. If successfully processed, the Foreign Agent MUST create a Visitor Entry for the Mobile Node, and be prepared to deliver packets received by the initiator of the Handoff Request destined for the Mobile Node. The Handoff Reply message MUST

include the Home Address, Home Agent Address, lifetime value, and the Link-Layer Address Extension (see Section 10).

A Foreign Agent that receives a Handoff Reply with the Code field set to success (zero value) MUST "bi-cast" all packets destined to the Mobile Node to both the Mobile Node and to the new Foreign Agent.

If the message received by the new Foreign Agent contained a GFA IP Address Extension [6], and it shares a security association with the GFA, it MUST issue a Regional Registration Request to the GFA. The Regional Registration Request's Care-Of address field MUST be set to the local Foreign Agent's address, while the GFA IP Address MUST be set to the address of the recipient of the request. The request's lifetime field is set to an administratively configured value. A successful Regional Registration Reply MUST cause the Foreign Agent to create a visitor entry for the Mobile Node.

If a Regional Registration Reply message is received with the code field set to DO_NOT_SERVICE_MN (Section 11), the Foreign Agent SHOULD NOT provide service to the Mobile Node. The Foreign Agent MAY enforce this by closing the Link-Layer connection (if possible), not issuing any Mobility Advertisements to the Mobile Node (assuming a point-to-point Link Layer), or simply denying all Registration Requests with the error code set to 65 (Administratively Prohibited) [1].

Once a visitor entry has been created, and the Mobile Node establishes a link layer channel with the Foreign Agent, its traffic will be immediately delivered, along with a Mobility Advertisement message [1]. A Mobile Node MUST issue a Registration Request when it receives a Mobility Advertisement from a new Foreign Agent.

Note that Foreign Agents MAY delay in sending Mobility Advertisements, especially to reduce noticeable service disruption during a ping-pong effect. However, when doing so, the Foreign Agent MAY need to re-issue a new Handoff Request to oFA (and optionally the Regional Registration message to GFA), to extend the visitor entry's lifetime.

Delaying Mobility Advertisements MAY also be done in wireless technologies that support dormant mobiles. When this is done, a Foreign Agent would typically wait to send the advertisement until the mobile is no longer in the dormant mode. When data is received by the Foreign Agent for a dormant Mobile Node, it SHOULD initiate the link-layer mechanism that causes the mobile to "wake-up" (this is typically known as paging).

The above procedures require that Foreign Agents issue Handoff Requests as a result of Link-Layer triggers. However, the discovery

of the identity of the Foreign Agents to which the Handoff messages must be sent is outside the scope of this document.

In the event that a Foreign Agent handling a particular Mobile Node's visitor entry is soon to expire, and the Mobile Node has not yet issued a Registration Request, the FA has the option to transmit a new Handoff Request message to the old Foreign Agent (and the optional Regional Registration Request to the GFA). Whether the renewal is performed on behalf of the Mobile Node is a policy decision up to the network administrator.

A Foreign Agent MAY receive packets for a Mobile Node to which it does not have a direct link layer connection. At this point, the Foreign Agent MAY:

1. Drop all packets for the Mobile Node
2. Buffer packets for the Mobile Node
3. Attempt to establish a link-layer connection with the mobile
4. Issue a Regional Registration Request with a zero lifetime

Given that a Mobile Node's packets will be delivered prior to registration, a Mobile Node is free to discard all packets received from Foreign Agents with which it hasn't registered.

When the new Foreign Agent receives the Mobile Node's Registration Request [1], its Anchor Foreign Agent changes to the new Foreign Agent. The Foreign Agent MUST transmit a Handoff Request message to the old Foreign Agent with the lifetime field set to zero. A Foreign Agent that receives a Handoff Request with the lifetime field set to zero is being informed that it is no longer the anchor point for the mobile. It MAY issue a Handoff Request to the new Foreign Agent in the future if it wishes to keep receiving the mobile's packets for possible delivery.

When a Foreign Agent determines that it is no longer servicing a Mobile Node, it SHOULD issue a Regional Registration Request message with the lifetime field set to zero (0). This will cause the visitor entry associated with the Foreign Agent's Care-Of address on the GFA to be deleted. Foreign Agents MAY decide to not issue this message immediately when a link-layer trigger is received, in order to support smooth service during a ping-pong event.

7.2 Gateway Foreign Agent Considerations

Upon receipt of a Regional Registration Request, a GFA MUST create a visitor entry indicating the Mobile Node's current point of attachment. In the event that a visitor entry already exists, the GFA SHOULD be able to create multiple visitor entries for the same

Mobile Nodes with different Care-Of addresses. If the 'S' bit was enabled in the Regional Registration Request, the GFA MUST be able to forward the mobile's packets to all Foreign Agents in the visitor entries.

When constructing the Regional Registration Reply, the GFA SHOULD include the FA-FA authentication extension [6], and set the lifetime field to the lesser of:

1. number of seconds before the Mobile Node's Registration with its Home Agent will expire.
2. The lifetime of the locally created Visitor Entry.

In the event that the Regional Registration Request's lifetime field was set to zero (0), the GFA MUST remove the visitor entry associated with the Care-Of address in the message.

Should the GFA decide that the Foreign Agent is not to provide service to the Mobile Node, it MUST issue a Regional Registration Reply message, with the code field set to DO_NOT_SERVICE_MN (see Section 11).

8.0 Handoff Request Message

The Handoff Request message is used to inform a peer that a pro-active handoff is being initiated. The Handoff Request message can be used for both source and target triggers, through the Type of Trigger 'I' bit in the message flags. When sent as a result of a target trigger, the Home Address and Home Agent fields MAY be set to zero (unless this information was communicated by the link layer, which is outside the scope of this document).

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |     Type      |S|x|I|M|G|r|T|x|          Lifetime             |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                        MN Home Address                        |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                      Home Agent Address                       |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                                                               |
    +                         Identification                        +
    |                                                               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    | Extensions ...
    +-+-+-+-+-+-+-+-
```

Type TBD (Handoff Request)

S When set, and when no GFA address extension is present, it indicates that both oFA and nFA will attempt to deliver datagrams directly to MN, if a link-layer connection exists. If a GFA address extension is present, it implies that nFA should set the 'S' bit in its regional registration.

I Type of Trigger. A value of zero is a source trigger (sent by oFA), while a value of one is a target trigger (sent by nFA).

M, G, T As defined in [1, 12]. This refers to the tunnel between oFA and nFA, or, if GFA IP address extension is present, to the parameters that should be requested in the Regional Reg Req.

Lifetime The requested Lifetime for which nFA will serve the MN on behalf of oFA, without requiring a new registration.

MN Home Address The home address of the mobile node. When using a private address, the G and T flags must be sent and a GRE Key extension must be included.

Home Agent Addr The home agent address of the mobile node.

Identification As in defined in [1].

Extensions The Message MUST include LLA (see Section 10), the FA-FA Authentication Extension [6], and MAY include GFA IP address.

9.0 Handoff Reply Message

The Handoff Reply message is sent in response to the Handoff Request message. When a source trigger caused the Handoff Request message to be sent, this message is sent with a successful code if the Visitor Entry was successfully created. When a target trigger caused the Handoff Request message, receipt of this message with a successfuly code SHOULD cause the Visitor Entry to be created.

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |     Type      |     Code      |           Lifetime            |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |S|x|I|M|G|r|T|x|                    Reserved                   |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                         MN Home Address                       |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                       Home Agent Address                      |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                                                               |
    +                          Identification                       +
    |                                                               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    | Extensions ...
    +-+-+-+-+-+-+-+-
```

Type   TBD (Handoff Reply)

Code   A value indicating the result of the Handoff Request. See below for a list of currently defined Code values.

Lifetime   If the Code field indicates that the registration was accepted, the Lifetime field is set to the number of seconds remaining before the registration is considered expired. A value of zero indicates that the mobile node has been deregistered. A value of 0xffff indicates infinity. If the Code field indicates that the registration was denied, the contents of the Lifetime field are unspecified and MUST be ignored on reception.

S   When set, and when no GFA address extension is present, it indicates that both oFA and nFA will attempt to deliver datagrams directly to MN, if a link-layer connection exists. If a GFA address extension is present, it implies that nFA should set the 'S' bit in its regional registration.

I   Type of Trigger. A value of zero is a source trigger (sent by oFA), while a value of one is a target trigger (sent by nFA).

M, G, T   As defined in [1, 12]. This refers to the

tunnel between oFA and nFA, or, if GFA IP address extension is present, to the parameters that should be requested in the Regional Reg Req.

MN Home Address
The home address of the mobile node. When using a private address, the G and T flags must be sent and a GRE Key extension must be included.

Home Agent Addr
The home agent address of the mobile node.

Lifetime
The requested Lifetime for which nFA will serve the MN on behalf of oFA, without requiring a new registration.

Identification
As in defined in [1].

Extensions
The Message MUST include LLA (see Section 10) and the FA-FA Authentication Extension [6].

10.0 Generalized Link Layer Address Extension

This section defines the Generalized Link Layer Address (LLA) Extension, used by any that needs to communicate Link Layer Addresses. The format of the extension follows MIER [13], and each sub-type of link-layer address defines its own sub-structure. This draft defines two sub-types, the cdma2000 IMSI and the Ethernet Address. Future RFCs should allocate their own sub-type and define their own address formats.

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     Type      |   Length      |   Sub-Type    |    LLA ...
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

TBD (skippable) [1]

Length

The length of the Link Layer Address + the one octet Sub-Type field

Sub-Type

This field contains the Link Layer sub-type identifier

LLA

Contains the Link Layer Address

In this document, two subtypes are defined:

1	cdma2000 International Mobile Station Identity [14]
2	Ethernet 48 bit MAC address [15]
3	64 bit Global ID, EUI-64 [19]

10.1 cdma2000 Link Layer Address Extension

The cdma2000 Link Layer Address Extension contains the International Mobile Station Identity, as defined in [14].

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |   Sub-Type    |    IMSI ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

TBD (skippable) [1]

Length

The length of the IMSI field + the one octet Sub-Type field

Sub-Type

1

IMSI

Contains the IMSI, in the form:

<IMSI>:<Connection Id>

Where the <IMSI> is an ASCII-based representation of the International Mobile Station Identifier, most significant digit first, ":" is ASCII 0x3a, and the Connection ID is the ASCII representation of a small, decimal number used for distinguishing different link-layer connections from the same device.

10.2 Ethernet Link Layer Address Extension

The Ethernet Link Layer Address Extension contains the 48 bit Ethernet MAC Address, as defined in [15].

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     Type      |    Length     |   Sub-Type    |    MAC ...
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

TBD (skippable) [1]

Length

7 (includes the Sub-Type field)

Sub-Type

2

MAC

Contains the 48 bit Ethernet MAC Address.

10.3 IEEE 64-Bit Global Identifier (EUI-64) Address Extension

The 64-Bit Global Identifier (EUI-64) Address Extension contains the 64 bit address, as defined in [19].

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     Type      |    Length     |   Sub-Type    |    MAC ...
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

TBD (skippable) [1]

Length

7 (includes the Sub-Type field)

Sub-Type

3

MAC

Contains the 64-Bit Global Identifier Address.

11.0 Error Values

The following table contains the name of Code [9] to be returned in a Registration Reply, the value for the Code, and the section in which the error is first mentioned in this specification.

Error Name	Value	Section of Document
DO_NOT_SERVICE_MN	TBD	7.1

12.0 IANA Considerations

The number for the Generalized Link Layer Address Extension in section 10 is taken from the numbering space defined for Mobile IP registration extensions defined in RFC 2002 [1]. These MUST NOT conflict with any numbers used in RFC 2002[1], RFC 2344 [12], RFC 2356 [16], RFC 2794 [17] and RFC 3012 [18].

The Code values specified for errors, listed in section 11, MUST NOT conflict with any other code values listed in RFC 2002 [1], RFC 2344 [12], RFC 2356 [16], RFC 2794 [17] and RFC 3012 [18].

Sections 8 and 9 require numbers assigned from the Mobile IP control message type address space. The numbers assigned MUST NOT conflict with [1], [6] and [7].

13.0 Security Considerations

Similar to [6] and [7], this specification assumes that the local Foreign Agent, and the GFA (or AFA) inherently trust each other. This MAY be achieved through the use of a long lived security association.

This specification introduces a new change to Mobile IP, which is the ability for a Mobile Node to receive packets from a Foreign Agent to which it has not yet registered. In the event that the Mobile Node does not wish to receive packets from unknown Foreign Agents, it MAY drop them.

Although this document does not specify how Foreign Agents can

identify, or track, Mobile Nodes, it is assumed that the wireless link layer be sufficiently secure in order to correctly identify a Mobile Node. Wireless networks that do not provide such features will be subjected to impersonation attacks, where malicious nodes could cause the Foreign Agents to believe that a Mobile Node has moved to other service areas.

14.0 References

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

[2] T. Hiller et al. "Cdma2000 Wireless Data Requirements for AAA". draft-hiller-cdma2000-AAA-00.txt (work in progress). October 1999.

[3] U. Black. "2nd Generation Wireless Networks". Prentice-Hall. New York. 1999.

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

[5] C. Perkins and D. Johnson. "Route Optimization in Mobile IP". draft-ietf-mobileip-optim-08.txt (work in progress). February 1999.

[6] E. Gustafsson, A. Jonsson, C. Perkins. "Mobile IP Regional Registration", draft-ietf-mobileip-reg-tunnel-02.txt (work in progress), March 2000.

[7] G. Dommety. "Local and Indirect Registration for Anchoring Hand-offs", draft-dommety-mobileip-anchor-handoff-00.txt (work in progress), March 2000.

[8] P. Calhoun, H. Akhtar, E. Qaddoura, N. Asokan, "Foreign Agent Keys Encoded as Opaque Tokens for use in Hand-off Process", draft-calhoun-mobileip-fa-tokens-00.txt (work in progress), March 2000.

[9] S. Hanks, T. Li, D. Farinacci, and P. Traina. Generic Routing Encapsulation (GRE). Request for Comments (Informational) 1701, Internet Engineering Task Force, October 1994.

[10] C. Perkins. Minimal Encapsulation within IP. Request for Comments (Proposed Standard) 2004, Internet Engineering Task Force, October 1996.

[11] Mohamed M.Khalil, Emad Qaddoura, Haseeb Akhtar, Pat R. Calhoun, "Generalized NAI Extension (GNAIE)", draft-ietf-mobileip-gnaie-00.txt (work in progress), February 2000.

[12] G. Montenegro, "Reverse Tunneling for Mobile IP", RFC 2344, May 1998.

[13] Khalil, and et. al. Mobile IP Extensions Rationalization (MIER) draft-ietf-mobileip-mier-00.txt, Dec 1999.

[14] TIA/EIA/IS-95-B

[15] D. Plummer, "An Ethernet Address Resolution Protocol - or - Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware", RFC 826, Symbolics, Inc., November 1982.

[16] Montenegro, G. and V. Gupta, "Sun's SKIP Firewall Traversal for Mobile IP", RFC 2356, June 1998.

[17] P. Calhoun, C. Perkins, "Mobile IP Network Access Identifier Extension", RFC 2794, March 2000.

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

[19] IEEE, "Guidelines for 64-bit Global Identifier (EUI-64) Registration Authority", http://standards.ieee.org/regauth/oui/tutorials/EUI64.html, March 1997.

15.0 Acknowledgements

The authors would like to thank Charles Perkins, George Tsirtsis and Scott Corson for their valuable feedback.

16.0 Authors' Addresses

Questions about this memo can be directed to:

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

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

Tom Hiller
Lucent Technologies
Rm 2F-218
263 Shuman Blvd
Naperville, IL 60566-7050
USA

```
Phone:  +1 630 979 7673
FAX:    +1 630 979 7673
E-Mail: tom.hiller@lucent.com
```

James Kempf
Network and Security Research Center, Sun Labs
Sun Microsystems, Inc.
15 Network Circle
Menlo Park, California, 94025
USA

```
 Phone:  +1 650 786 5890
   Fax:  +1 650 786 6445
E-mail:  james.kempf@eng.sun.com
```

Peter J. McCann
Lucent Technologies
Rm 2Z-305
263 Shuman Blvd
Naperville, IL 60566-7050
USA

```
Phone:  +1 630 713 9359
FAX:    +1 630 713 4982
E-Mail: mccap@lucent.com
```

Chandana Pairla
University of Illinois - Urbana Champaign
3315, DCL,
1304, W. Springfield Ave.,
Urbana, IL 61801
USA

Phone: +1 217 244 7117
E-mail: pairla@uiuc.edu

Sebastian Thalanany
Motorola
1475 West Shure Drive
Arlington Heights, IL - 60004
USA

Phone: +1 847 435 9296
E-mail: sthalan1@email.mot.com

Ajoy Singh
Motorola
1501 West Shure Drive
Arlington Heights, IL ô 60004
USA

Phone: +1 847 632 6941
E-mail: asingh1@email.mot.com

17.0 Full Copyright Statement