INTERNET-DRAFT
Expires August 05, 2003

Subrata Goswami
Independent Consultant

February 4, 2003

Simultaneous Handoff of Mobile-IPv4 and 802.11

<draft-goswami-mobileip-simultaneous-handoff-v4-02.txt>

Status of this Memo

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 [RFC 2119].

Abstract

This document describes a way to perform simultaneous Mobile-IPv4 handoff and 802.11 Access Point Association/Reassociation. Mobile-IPv4 Registration messages are carried as Information Elements in 802.11 frames. This way Mobile-IPv4 can perform handoff at the same time as 802.11 handoffs. The Foreign Agent can be a part of the Access Point or may serve a number of Access Points. The implications to existing mobility entities such as Access Point, Mobile Node, and Foreign Agent are discussed. Also pointed out are potential issues with 802.1x and the emerging 802.11i standards.

1. Overview and Rationale

In the 802.11 wireless lan [WiFi] network an 802.11 client connects to an **802.11 Access Point (AP) at the link level. 802.11 provides a mechanism to** achieve handoffs between AP's and the client. A 802.11 client first authenticates and then associates with one AP. When the 802.11 client decides that it is better to move to a second AP, it can do a pre-authentication and re-association with the second AP.

Similarly when a Mobile-IPv4 (MIP4) client move from subnet to subnet it seeks a Foreign Agent (FA) situated in the subnet and registers with the FA. The IP packet sent in Registration Message has the Home IP address as the source, and the destination address can be the FA's IP address or the "All Mobility Agents" multicast address (224.0.0.11). The FA then responds with Registration Reply message. The Registration Message also includes Authentication Extensions.

There is no obvious reason why the Mobile Node (MN) has to go through the authentication and association/registration twice. It would be beneficial to subsume the authentication and registration of MIPv4 to be completed during the 802.11 Authentication and Association exchanges.

The situation of non co-located FA is primarily considered, although a discussion of co-located FA is also provided.

2. 802.11 Network Architecture.

A hypothetical IP over 802.11 network is shown in the following figure. The mobile client MN can move from subnet X1 to X2 and from AP2 to AP3.

```
                        [FA1]
                          |
        ...     [AP1]-------[X1]--|
[MN]...           |             |
                [AP2]----               |----[X]----->  [HA]
                                        |
                [AP3/FA3]---[X3]--|


[MN] - Mobile Node
[FA] - Foreign Agent
[HA] - Home Agent
[AP] - Access Point
[X]  - IP Router
...  - 802.11 link
---  - 802.3  link
```

Figure 1: 802.11 Network

Here when the MN moves from AP1 to AP2, it first Associates with AP2 and then Dissociates with AP1. As the move from AP1 to AP2 occurs within the same subnet, hence the MN is still served by the same FA.

3. Message Sequence

The following figure shows the what happens when MN move from AP1 to AP2 to AP3. During the AP1 to AP2 handoff, the MN is in same subnet, hence MIPv4 registration is not required. The MN has no good way to figure that out, so it sends a MIPv4 Registration Request Message Information Element in every **802.11 Association Request Message. AP2 constructs a MIPv4 Registration** Request message from the 802.11 Information Element and send it to FA1. FA1 responds with MIPv4 Registration Reply message, which can be generated without doing a FA to HA message sequence.

```
MN                                  AP1         AP2              AP3
FA1             FA3

 ----- 802.11 Authentication Request------>

 <---- 802.11 Authentication Response------

.
.

 -------802.11 Reassociation  Request ----->
          (MIPv4 Registration IE included but not reqd.)

                                                         ----MIPv4
Registration-->
                                                         <---MIPv4
Reply----------

 <------802.11 Reassociation  Response-----
          (MIPv4 Reply IE included)

 --802.11 Dissociation Request->
 .
 .

 ------ 802.11 Reassociation  Request------------------>
          (MIPv4 Registration IE included)
                                                         ----MIPv4
Registration------------>
                                                         <---MIPv4
Reply--------------------

 <------802.11 Reassociation  Response------------------
          (MIPv4 Reply IE included)
```

Figure 2. 802.11/MIPv4 Message Sequence

When the MN moves from AP2 to AP3 there is a change of the serving FA, hence FA3 now needs to do a FA-HA message sequence.

4. New Information Elements in 802.11 Management Frames

The 802.11 Association/Reassociation frames are shown in the following figure. The Association/Reassociation frames can carry an optional MIPv4 information element. The MIPv4 Registration Request message is contained in the 802.11 Association/Reassociation Request messages. Similarly, the MIPv4 Registration Reply message is contained in the 802.11 Association/Reassociation Response messages.

```
    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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |        Frame Control          |         Duration              |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                          Destination Address                  |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                               |         Source Address        |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                          Source Address                       |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                          Basic Service Set ID                 |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                               |         Sequence Control      |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  Capability Information       |     Listen Interval           |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                          Current AP Address                   |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  Current AP Address           |     SSID (2-34 octets)        |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                          Supported Rates (3-7 octets)         |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   .                                                               .
   +                MIPv4-802.11 Registration Request IE           +
   .                                                               .
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                           Frame Check Sequence                |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 3. 802.11 (Re) Association Request Frame

In Figure 3., 802.11 Association Reassociation frames differ primarily in the absence of the Current AP address field from the first.

The MIPv4-802.11 element is an 802.11 Information Element (IE) with a unique Element ID (say 128) (see page 55 of [WiFi]). The 802.11 Information Element consists of the following fields: Element ID, Length ID, and Information. The length field is 1 octet long and specifies the length of the Information field in number of octets. Thus the MIPv4-802.11 can be at most 255 octets, and as such it would be a waste to put the full IP and UDP header. Hence a psuedo-IP and psuedo-UDP header is used. The pseudo-IP header is composed of Source and Destination IP addresses. The destination address can be the FA's IP address or the "All Mobility Agents" multicast address (224.0.0.11). The Source IP address is the Home Address of the MN. The pseudo-UDP header is composed of Source Port and Destination Port. The rest of the MIPv4-802.11 IE contains the MIPv4 fields. Figure 4 below shows the MIPv4-802.11 IE. The AP uses the Source IP Address from the IE for the source address of the Registration Request message it sends out.

The FA determines (from the ICMP packet itself) the L2 address of where the Request message came from and after receiving a reply from the HA, sends the reply to this L2 address. The FA MUST not use the ARP response for this L2 address (see section 5.3 for a more detailed description of this requirement).

```
    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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                   |Element ID     | Length        |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                       Source IP Address                       |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                       Destination IP Address                  |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                       UDP Source Port                         |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                       UDP Destination Port                    |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     Type      |S|B|D|M|G|V|rsv|          Lifetime             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                          Home Address                         |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                           Home Agent                          |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                        Care-of Address                        |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   +                         Identification                        +
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   | Extensions ...
   +-+-+-+-+-+-+-+-
```

Figure 4. MIPv4-802.11 Registration Request Information Element

Similarly a MIPv4-802.11 Registration Reply IE is defined as shown in Figure 5. The Source IP Address is the unicast IP address of the FA. The Destination IP Address is copied from the IP Source Address of the corresponding Registration Request IE. The UDP ports are also copied from the Registration Request IE, with the destination and source exchanged.

```
    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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                   |Element ID     | Length        |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                       Source IP Address                       |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                       Destination IP Address                  |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                       UDP Source Port                         |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                       UDP Destination Port                    |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     Type      |   Code        |          Lifetime             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                          Home Address                         |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                           Home Agent                          |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   +                         Identification                        +
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   | Extensions ...
   +-+-+-+-+-+-+-+-
```

Figure 5. MIPv4-802.11 Registration Reply Information Element

5. Mobile Entity Implications

There are some implications for the different mobile entities involved.

5.1 Implications for MN

The MN should be capable of passing the MIPv4 information to the 802.11 driver and vice-versa. At the instant the MN is ready to send an Association Request it should be able to access the MN's Mobile-IPv4 attributes. Similarly, when the MN receives an Association Response there should be a mechanism to change the Mobile-IPv4 attributes in MN.

5.2 Implications for 802.11 AP

The 802.11 AP should be able to extract/include the MIPv4-802.11 IE's. Its relation to the FA depends on whether the FA is a separate entity or an embedded entity.

When the FA is an embedded entity in the AP, then the mechanism of how the FA interacts with AP functions is an implementation issue.

When the FA is an independent entity with its own IP address, the situation is more complicated. The AP behaves as a proxy for the MN here, and constructs ICMP Registration Request packets with the source IP address copied from the MIPv4-802.11 IE. Thus the ICMP Reply packets relayed by the FA would be destined to the IP address of the MN. The link layer address used by the FA is that of the AP, hence the AP receive ICMP Registration Reply packets (from the HA via the FA). The AP then extracts IP address information from the ICMP Registration Reply packet and places them in the MIPv4-802.11 IE of the **802.11 Association Response message.**

After registration is complete, the MN would send periodic ICMP Registration Request directly to the FA which would be carried by regular 802.11 Data Frames.

5.3 Implications for FA

The FA listens on UDP port 434, which remains same for both the embedded and independent FA entity.

When the FA is an independent entity from the AP with its own IP address, the FA MUST use the MAC source address of the ICMP Registration Request packets it receives when sending out an ICMP Registration Reply message (This makes sure that the AP receives the response rather than the MN). The FA is required to have the link layer address of the MN (Section 3.7.1 of [MIPv4]). The AP in a way "proxies" for the MN for the ICMP Registration messages. After the MIPv4 registration is completed, the AP no longer proxies for the MN. Hence, the FA MUST be able to handle a change of link-layer address for IP address, as the link-layer addresses used by ICMP Registration Request messages are different when MIPv4-802.11 IE is involved and when MN generated ICMP Registration Request are used. Thus, the FA MUST extract the link-layer addresses from the ICMP Registration Request messages.

It should be noted that the acrobatics in the previous paragraph can be easily avoided if the Source IP Address requirement (section 3.6.1.1 in [MIPv4]) is relaxed so that the Source IP Address and the Home Address of the MN does not need to be same.

If the FA is an embedded entity in the AP, then there might be alternative ways to exchange information with the AP.

6. Co-located FA

When the FA is co-located on the MN, then MN first has to get a co-located Care of Address (CoA). MN's registers by setting the 'D' bit if it is registering with a co-located care-of address. There are several ways of obtaining CoA, of which one of the most popular method is DHCP. Although, for DHCP to work the 802.11 Authentication and Association should have been already completed. Thus it looks impossible for normal Mobile-IP registration to be simultaneous with 802.11 Associations.

There is actually a way to handle this. In this case the same MIPv4-802.11 Request/Response IE's are used. The MN makes the Source IP Address **0.0.0.0 in the MIPv4-802.11 Request IE.** The AP (through the DHCP server) then assigns an IP address for the CoA and send a Registration Request packet with that IP address as the Source IP Address to the MN's Home Agent. The AP temporarily responds to ARP for the IP address. The HA replies to this CoA, the AP then constructs the IE and sends a MIPv4-802.11 Response IE to the MN with the 802.11 Association Response. After this, the AP no longer responds to ARP for the CoA. The MN MUST use the Source IP Address in the MIPv4-802.11 Response IE as the CoA.

There could be situations when even if the MN wants to do co-located registration, the network may not allow that. Also, unlike regular MIPv4 operations, the MN does not receive any Mobility Agent advertisements, hence a new code (201) called Registration Required is defined. An Mobile-IE Extension can also be defined that lists the available Foreign Agents. After this the MN can do a regular MIPv4 registration or can do another 802.11 Association.

7. Working with 802.1x and 802.11i

When 802.1x authentication is done after the 802.11 associations, although registration with the IE would proceed smoothly, the MN would not be able to receive any IP traffic till 802.1x authentication is completed successfully.

The 802.11i is a draft standard at IEEE 802.11 Working Group [WiFiTGi]. It is supposed to handle all the problems that WEP-1 (as defined in [WiFi]) has and more. It is both an encryption and authentication method as is IPSec. Unlike IPSec, it is not meant to be end-to-end.   The unapproved standard as of now supports 4 different schemes: Open Text, Temporal Key Integrity Protocol (TKIP), Wireless Robust Authenticated Protocol (WRAP), and CCM (AES Counter Mode Encryption and CBC-MAC Authentication). The draft supports pre-authentication through 802.1x and then 802.11 Association. Thus in this case MIPv4 registration can be performed simultaneously with 802.11 Associations. The encryption supported by 802.11i is transparent to any MIPv4 traffic.

The following message sequence diagram, Figure 6, shows how 802.11i pre-authentication and encryption is done and how it does not effect MIPv4. Depending on the specific algorithm used, the 802.1x pre-authentication message sequence may consists of 10+ messages.

```
MN                                  AP1         AS                 AP3
FA3

 --EAPOL Start---------------->(802.11 Class 1  frame)

 <-EAPOL Request Identity-----

 --EAPOL Response Identity---->

                              --RADIUS Req->

 <  EAPOL Authentication Message Exchange  >

                              <-RADIUS Rep--

 <-EAPOL Success --------------
```

```
.
.
   <EAP Cipher Suite and Key  Exchanges>
.
.
   <Normal data exchanges>
.
.
 --802.1x pre-auth Request----->(802.11 Class 3  frame)

                               - 802.1x pre-auth Request->

                                           <-RADIUS Req--

                                           --RADIUS Rep->

                                         <-802.1x pre-auth Response-
 <-802.1x pre-auth Response-----
.
.
 -------802.11 Reassociation  Request ----------------->
          (MIPv4 Registration included but not reqd.)

                                                         ----MIPv4
Registration-->
                                                         <---MIPv4
Reply----------

 <------802.11 Reassociation  Response-----------------
          (MIPv4 Reply included)

 .
 .


[MN] - Mobile Node, 802.1x supplicant
[AP] - Access Node, 802.1x authenticator
[AS] - 802.1x Authentication Server, typically a RADIUS server.
[FA] - Foreign Agent
```

Figure 6. 802.11i, 802.1x pre-authentication and Mobile-IP v4

8. MN Returning Home

To be added

9. IETF and IEEE Issues

As mentioned previously, the Source IP Address requirement (section 3.6.1.1 in [MIPv4]) needs to be relaxed so that the Source IP Address and the Home Address of the MN does not need to be same.

>From the IEEE side, a new optional Information Element needs to be defined that can carry all MIPv4 registration related payload between the MN and the AP.

10. Acknowledgments

All the RFC's, IDÆs, freely available 802.11 standards, and Linux web-sites.

11. References

[WiFi] IEEE, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", 1999.

[MIPv4] Perkins, C., "IP Mobility Support", RFC 3220, January 2002.

[WiFiTGi] IEEE, "802.11i Draft 2.3", 2002.

12. Author's Address

Subrata Goswami, Ph.D.
Independent Consultant
Newark, CA 94560
sgoswami@umich.edu

This document expires August 05, 2003.