Mobile IP Working Group Eva Gustafsson
INTERNET DRAFT Ericsson
25 August 1999 Annika Jonsson
Ericsson
Charles E. Perkins
Sun Microsystems Laboratories

Mobile IP Regional Tunnel Management

draft-ietf-mobileip-reg-tunnel-01.txt

Status of This Memo

Abstract

In Mobile IP a mobile node registers with its home agent each time it changes care-of address. If the distance between the visited network and the home network of the mobile node is large, the signaling delay for these registrations may be long. We propose a solution for performing registrations locally in the visited domain: regional registrations. Regional registrations reduce the number of signaling messages to the home network, and reduce the signaling delay when a mobile node moves from one foreign agent to another, within the same visited domain. This may, for instance, improve the performance of handover.

Contents

1. Introduction

This document adds to the Mobile IP protocol, by proposing a means for mobile nodes to register locally in a visited domain. By registering locally, via regional registrations, the signaling delay is reduced, and this may improve the performance when the mobile node changes foreign agent.

In Mobile IP, as specified in RFC 2002 [9], a mobile node registers with its home agent each time it changes care-of address. If the distance between the visited network and the home network of the mobile node is large, the signaling delay for these registrations may be long. We propose a solution for performing registrations locally in the visited domain: regional registrations. Regional registrations reduce the number of signaling messages to the home network, and reduce the signaling delay when a mobile node moves from one foreign agent to another, within the same visited domain. This may, for instance, improve the performance of handover.

When a mobile node first arrives at a visited domain, it performs a registration with its home network. At this registration, we assume that the home network generates a registration key for the mobile node. This registration key is distributed to the mobile node and to the visited domain, and can be used for authentication of regional registrations.

At registration with the home network, the home agent registers the care-of address of the mobile node. In case the visited domain supports regional tunnel management, the care-of address that is registered at the home agent is the publicly routable address of a Gateway Foreign Agent (GFA). This care-of address will not change when the mobile node changes foreign agent under the same GFA. When changing GFA, a mobile node must perform registration at its home network; when changing foreign agent under the same GFA, the mobile node MAY perform a regional registration within the visited domain.

The proposed regional tunnel management protocol supports one level of foreign agent hierarchy beneath the GFA. The protocol may be extended to support several levels of hierarchy. Such a hierarchy is discussed in the appendix.

Foreign agents that support regional registrations are also required to support registrations according to RFC 2002 [9]. If the mobile node chooses not to employ regional registrations, it may register a co-located care-of address directly with its home agent, according to [9], or, if there is a foreign agent address announced in the Agent Advertisement, the mobile node may register that foreign agent care-of address with its home agent [9].

2. Terminology

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 [2].

In addition, this document frequently uses the following terms:

Mobile Node (MN)
As defined in [9].

Home Agent (HA)
As defined in [9].

Foreign Agent (FA)
As defined in [9].

Home network
As defined in [9].

Mobility Agent (MA)
As defined in [9].

Visited network
As defined in [9].

Home domain
The domain where the home network and home agent are located.

Visited domain
The domain where the visited network, the current foreign agent and the GFA are located.

Gateway Foreign Agent (GFA)
A Foreign Agent which has a publicly routable IP address. A GFA may, for instance, be placed in or near a firewall.

Local Care-of Address
A Care-of Address which is either assigned to a mobile node, or to a foreign agent offering local connectivity to a mobile node. A registration message from the mobile node is subsequently sent to a GFA via the local care-of address.

Home Registration
A registration, processed by the home agent and the GFA, using the specification in RFC 2002 possibly with additional extensions defined in this document.

Regional Registration
A mobile node performs registration locally at the visited domain, by sending a Regional Registration Request to a GFA, and receiving a Regional Registration Reply in return.

Registration Key
A key used by mobile nodes and mobility agents to secure certain control messages related to Mobile IP.

AAA server
Authentication, authorization and accounting server.

3. Description of the Protocol

This section provides an overview of the regional tunnel management protocol.

3.1. General Assumptions

Our general model of operation is illustrated in figure 1, showing a visited domain with foreign agent and GFA, and a home network with a home agent.

```
+----------------------------+                +-----------------+
|       Visited Domain       |                |      Home       |
|                            |   +----------+ |     Network     |
|                            |   |          | |                 |
|  +------+      +-------+   |   | Public   | |    +------+     |
|  |  FA  |------|  GFA  |-------------------------|  HA  |     |
|  +--+---+      +-------+   |   | Network  | |    +------+     |
|     |                      |   |          | |                 |
+-----|----------------------+   +----------+ +-----------------+
      |
   +--+---+
   |  MN  |
   +------+
```

Figure 1: Visited domain with a GFA, and a home network with HA.

3.1.1. Visited Domain

We assume two hierarchy levels of foreign agents in the visited domain. At the top level of the hierarchy, there is at least one GFA, which is a foreign agent with additional features. A GFA must have a publicly routable address. Beneath a GFA, there are one or more foreign agents. We assume that there exist established security associations among a GFA and the foreign agents beneath it. Multiple hierarchy levels of foreign agents are discussed in the Appendix. When designing a domain supporting regional registrations, the foreign agents and their GFA must be compatible. That is, they should support the same encapsulation types, compression mechanisms etc.

When a mobile node changes care-of address under the same GFA, it MAY perform a regional registration. If the mobile node changes GFA, within a visited domain or between visited domains, it MUST register with its home network.

3.1.2. Registration Key Distribution

We assume that when a mobile node performs registration at its home network, registration keys are distributed to the mobile node and to the visited domain, for example according to [3, 7]. When regional tunnel management is employed, the GFA is the agent within the visited domain which receives the registration keys. This is because the GFA address is the registered care-of address of the mobile node at its home network.

These registration keys are subsequently used to enable proper authentication for regional registration messages (see sections 5.1 and 5.2).

3.1.3. Network Access Identifier

We provide additional features that rely on the ability of the the mobile node and the foreign agent to use the Network Access Identifier (NAI) [1]. For mobile nodes and mobility agents that do not have a NAI, regional registration will still work but the lack of certain features will result in less than optimal results.

3.1.4. Authentication Extensions

With regional tunnel management, a GFA address is registered at the home agent as the care-of address of the mobile node. We assume that if a Mobile-Foreign Authentication extension is present in a Registration Request message, the GFA will perform the authentication. Similarly, we assume that if a Foreign-Home Authentication extension is present in a Registration Request message, the authentication is performed between the GFA and the home agent.

3.2. Protocol Overview

When a mobile node first arrives at a visited domain, it performs a registration with its home network. At this registration, the home agent registers the care-of address of the mobile node. In case the visited domain supports regional registrations, the care-of address that is registered at the home agent is the address of a GFA. The GFA keeps a visitor list of all the mobile nodes currently registered with it.

At this registration, the home network distributes a registration key for the mobile node and the GFA. It can be used for authentication of regional registrations.

Since the care-of address registered at the home agent is the GFA address, it will not change when the mobile node changes foreign agent under the same GFA. Thus, the home agent does not need to be informed of any mobile node movements beneath the GFA.

```
    MN                     FA1                     GFA              HA
    |                       |                       |                |
    | Registration Request  |                       |                |
    |---------------------->|  Reg. Request w/ext.  |                |
    |                       |---------------------->|  Reg. Request  |
    |                       |                       |--------------->|
    |                       |                       |   Reg. Reply   |
    |                       |  Reg. Reply w/ext.    |<---------------|
    |  Registration Reply   |<----------------------|                |
    |<----------------------|                       |                |
    |                       |                       |                |
```

Figure 2: Registration at the GFA and the home agent.

Figure 2 illustrates the signaling message flow for registration with the home network. After the registration at the home agent, the home agent records the GFA address as the care-of address of the mobile node.

```
    MN                     FA2                            GFA       HA
    |                       |                              |         |
    | Regional Reg. Request |                              |         |
    |---------------------->| Regional Reg. Request w/ext. |         |
    |                       |----------------------------->|         |
    |                       | Regional Reg. Reply w/ext.   |         |
    | Regional Reg. Reply   |<-----------------------------|         |
    |<----------------------|                              |         |
    |                       |                              |         |
```

Figure 3: Regional registration at the GFA.

Figure 3 illustrates the signaling message flow for regional registration. Even though the mobile node's local care-of address changes, the home agent continues to record the GFA address as the care-of address of the mobile node.

DISCUSSION:

Should regional registration use different message types, or extensions to the existing message types?

3.3. Advertising Foreign Agent and GFA

A foreign agent MAY announce its presence via an Agent Advertisement message [9]. If the domain to which a foreign agent belongs supports regional registrations, the following applies to the Agent Advertisement message.

The `I' flag MUST be set to indicate that the domain supports regional tunnel management, and that a GFA address is advertised in the Agent Advertisement message. If the `I' bit is set, there MUST be at least one care-of address in the Agent Advertisement message.

If the `I' bit is set, and there is only one care-of address, it is the address of the GFA. The FA-NAI SHOULD also be present to enable the mobile node to be able to determine whether or not it has changed foreign agents (so that a new regional registration may be initiated). The mobile node also uses the foreign agent NAI to decide whether or not it is in its home domain.

If the `I' bit is set, and there are multiple care-of addresses, the first care-of address is the local FA, and the last care-of address is the GFA. In this case, if the FA-NAI is present, the first care-of address SHOULD be treated as a private address; further handling for such addresses is not specified in this document. In this latter case, the mobile node MUST match the FA-NAI before using the local care-of address. Moreover, the mobile node MUST insert its own MN-NAI in any registration request sent to the foreign agent with the private address.

3.4. Home Registration

This section describes registration at the home network. Registration at the home network is performed when a mobile node first arrives at a visited domain, when it requests a new home agent, or when it changes GFA. Registration at the home network is also performed to renew bindings which would otherwise expire soon.

3.4.1. Mobile Node Considerations

Suppose the mobile node receives an Agent Advertisement from the foreign agent. If the `I' flag in the Agent Advertisement is set, if the mobile node determines that it is in a visited domain, and if the mobile node registers via a foreign agent, it SHOULD either use the advertised GFA address in the care-of address field in the Registration Request message, or set this field to zero to request to be assigned a GFA. The home agent will then register the GFA address as the care-of address of the mobile node. If the mobile node is assigned a GFA, it learns the address of that GFA from the GFA IP address extension in the Registration Reply. If the mobile node, when receiving an Agent Advertisement, determines that it is in its home domain, it acts according to [9]. The mobile node may also find the GFA address by some other means, not considered in this draft.

Suppose a mobile node with a co-located care-of address wishes to use the address of GFA as its care-of address in a Registration Request message. The mobile node MAY then generate a Registration Request message, with the GFA address in the care-of address field, and send it directly to the GFA (not via a foreign agent). In this case, the mobile node MUST add a Hierarchical Foreign Agent extension, including its co-located care-of address, to the Registration Request before sending it.

Mobility agents send out Agent Advertisements. Upon receipt of an Agent Advertisement message with the `I' flag set and a FA-NAI extension, the mobile node compares the domain part of the foreign agent NAI with the domain part of its own NAI, to help in the determination about whether it is in its home domain or in a visited domain. If the NAIs do not match, the mobile node MUST assume it is in a foreign domain. Otherwise, if the mobile node determines that it is in its home domain, and furthermore that it is attached to its home network, it acts as defined in [9]. If the mobile node determines that it is in its home domain, but not on its home network, the mobile node SHOULD behave as defined in [9], and not register via a GFA.

DISCUSSION (for multiple levels, as in appendix):

How does regional registration work on the home network, where the mobile node should NOT have to go through a GFA?

If the mobile node determines that it is in a visited domain, and if it registers via a foreign agent, the mobile node SHOULD register the GFA address as its care-of address. This can be done either by (i) putting the GFA address in the care-of address field in the Registration Request message; or (ii) setting the care-of address field in the Registration Request message to zero, thereby requesting to be assigned a GFA care-of address.

All of these operations are still possible if the mobile node receives an Agent Advertisement with the `R' bit set. In that case, the mobile node, even though it has a co-located care-of address, still formulates the same Registration Request message with extensions, but it sends the message to the advertising foreign agent (not, for example, the GFA).

If the mobile node had requested to be assigned a GFA, it learns the address of that GFA from the GFA IP address extension in the Registration Reply.

3.4.2. Foreign Agent Considerations

When the foreign agent receives a Registration Request message from a mobile node, it reads the care-of address field in the Registration Request message, to find the GFA to which the message shall be relayed. If the care-of address field is set to zero, the foreign agent assigns a GFA to the mobile node, by some means not described in this draft. The foreign agent assigns a GFA to the mobile node, by some means not considered in this draft, and adds a GFA IP Address extension to the Registration Request message. The foreign agent cannot insert the GFA address directly in the care-of address field in the Registration Request message, since that would cause the Mobile-Home authentication to fail.

If the care-of address in the Registration Request is the address of a GFA, the foreign agent adds a Hierarchical Foreign Agent extension, including its own address, to the Registration Request message, and relays it to the GFA. If the care-of address in the Registration

Request is the address of the foreign agent, the foreign agent relays the message directly to the home agent, as described in [9].

If the care-of address in the registration request has the `T' bit set, the mobile node is requesting Reverse Tunneling [5]. In this case, the foreign agent has to tunnel packets from the mobile node to the GFA for further handling. The GFA will then decapsulate the packet from the foreign agent and re-encapsulate them for further delivery back to the home agent. It is required that the home agent receive such packets from the expected care-of address (i.e., that of the GFA) instead of the local care-of address.

3.4.3. GFA Considerations

For each pending or current registration, the GFA maintains a visitor list entry as described in [9]. In addition to the list entry contents required in [9], the list entry MUST contain:

- the current care-of address of the mobile node, i.e., the foreign agent address in the Hierarchical Foreign Agent extension.
- the remaining Lifetime of the regional registration.
- the style of replay protection in use

If the Registration Request message contains a Replay Protection extension (see section 6.3) requesting a style of replay protection not supported by the GFA, the GFA MUST reject the registration request and send a Registration Reply with the value in the Code field set to UNSUPPORTED_REPLAY_PROTECTION.

If the Hierarchical Foreign Agent extension comes after the MN-FA authentication extension, the GFA MUST then remove it from the Registration Request message. The GFA then sends the request to the home agent, possibly via AAA servers as described in [3].

Upon receipt of the Registration Reply message, the GFA consults its pending registration record to find the care-of address within its domain that is currently used by the mobile node, and sends the Registration Reply to that care-of address. When a Registration Reply arrives, the GFA relays the Registration Reply message to the foreign agent, according to the information from the cached Hierarchical Foreign Agent extension.

3.4.4. Home Agent Considerations

The Registration Request is processed by the home agent as described in [9], with additional processing for extensions specified in this document. If a home agent receives a Registration Request message with the care-of address set to zero, and a GFA IP Address extension, it MUST register the IP address of the GFA as the care-of address of the mobile node in its mobility binding list. If the registration request is accepted, the home agent MUST include the GFA IP Address extension in the Registration Reply, before the Mobile-Home Authentication extension. If the home agent does not support regional tunnel management, upon receipt of a Registration Request message with a GFA IP Address extension, it MUST deny the request.

The home agent then generates a Registration Reply message, including the GFA IP Address extension, and sends it back to the GFA. As with the Registration Request, the message may be relayed directly, or via AAA servers.

3.5. Regional Registration

This section describes regional registration. Once the home agent has registered the GFA address as the care-of address of the mobile node, the mobile node may perform regional registrations. When performing regional registrations, the mobile node may either register a foreign agent care-of address or a co-located address with the GFA. In the following, we assume that a registration at the home network has already occurred, and that the GFA has a registration key for the mobile node. All Regional registration messages MUST include a Mobile-Foreign Authentication extension. By contrast, regional registration messages MUST NOT include a Mobile-Home Authentication extension nor a Foreign-Home Authentication extension.

Assume that the mobile node moves from one foreign agent to another foreign agent within the same visited domain. It will then receive an Agent Advertisement from the new foreign agent. If the Agent Advertisement indicates that the visited domain supports regional registrations, and if the advertised GFA address is the same as the one the mobile node has registered as its care-of address with its home agent, the mobile node can perform a regional registration with this GFA, using the registration keys for authentication.

The mobile node issues a Regional Registration Request message to the new foreign agent. The request is authenticated using the registration key that was distributed to the GFA and to the mobile node from the home network.

The foreign agent adds a Hierarchical Foreign Agent extension to the message and relays it to the GFA. Based on the information in the Hierarchical Foreign Agent extension, the GFA updates the mobile node's current point of attachment in its visitor list. The GFA then issues a Regional Registration Reply to the mobile node via the foreign agent.

If the advertised GFA is not the same as the one the mobile node has registered as its care-of address, and if the mobile node is still within the same domain as it was when it registered that care-of address, the mobile node MAY try to perform a regional registration with its registered GFA. If the foreign agent cannot support regional registration to a GFA, other than advertised, the foreign agent denies the regional registration with code `unknown GFA'.

3.5.1. Mobile Node Considerations

For each pending or current registration, that is, registration with the home network or regional registration, the mobile node maintains the information described in [9]. In addition to that, the mobile node MUST maintain the following information, if present:

- the GFA address
- the style of replay protection in use

It is essential for the mobile node to be able to distinguish regional registrations from registrations with the home network, since it needs to know that when using regional registration, the nonces are not synchronized with its home agent. Further, in order to renew bindings before the lifetime expires, registrations MUST be directed to the home network. This is why we introduce a new message type for the Regional Registration Request message.

The replay protection for registrations and regional registrations is performed as described in [9]. Since the mobile node may perform regional registrations at the GFA in parallel with registrations at its home network, the mobile node MUST keep one replay protection mechanism and sequence for the GFA, and a separate mechanism and sequence for the home agent.

When a mobile node, which has already registered a GFA care-of address with its home agent, changes foreign agent within the same domain and receives an Agent Advertisement which advertises another GFA address, it MAY still generate a Regional Registration Request message destined to its old GFA.

3.5.2. Foreign Agent Considerations

When the foreign agent receives a Regional Registration Request message from a mobile node, it processes the message according the rules of processing a Registration Request message (see section 3.5.2), except that the care-of address field is presumed to be that of a GFA. If that care-of address belongs to an known GFA, the FA forwards the request to the indicated GFA. Otherwise, the foreign agent MUST generate a Regional Registration Reply with error code `unknown GFA'.

3.5.3. GFA Considerations

The GFA MUST NOT accept a Regional Registration Request if the lifetime of the mobile node's registration with its home agent has expired. If the GFA accepts a Regional Registration Request, it MUST set the lifetime to be no greater than the remaining lifetime of the mobile node's registration with its home agent, and put this lifetime into the corresponding Regional Registration Reply.

If the GFA receives a tunneled packet from a foreign agent in its domain, then after decapsulation the GFA looks to see whether it has an entry in its visitor list for the source IP address of the inner IP header after decapsulation. If so, then it checks the visitor list to see whether reverse tunneling has been requested; if requested, then the GFA re-encapsulates the packet with its own address as the source IP address, and the address of the home agent as the destination IP address.

4. Router Discovery Extensions

This section specifies an optional extension to the ICMP Router Discovery Protocol [4], and a new flag within the Mobile IP Agent Advertisement.

4.1. Regional Tunnel Management Flag

The Agent Advertisement message SHOULD include a flag indicating whether the domain, to which the foreign agent generating the Agent Advertisement belongs, supports regional tunnel management. The flag is inserted in one of the reserved fields, after the flags defined in [9].

The flag is defined as follows:

```
   I          Regional tunnel management.  This domain supports
              regional registrations.
```

4.2. Foreign Agent NAI Extension

The FA NAI extension is defined as follows:

```
 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     |        FA NAI ....
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 4: Foreign Agent NAI Extension

Type   TBD

Length   The length in bytes of the FA NAI field

FA NAI   A string in the NAI format defined in [1].

The foreign agent SHOULD include its NAI in the Agent Advertisement message. If present, the Foreign Agent NAI extension MUST appear in the Agent Advertisement message after any of the advertisement extensions defined in [9].

By comparing the domain part of the foreign agent NAI with the domain part of its own NAI, the mobile node can determine whether it is in its home domain or in a visited domain, and whether it has changed domain since it last registered.

5. Regional Registration Messages

This section specifies two new registration message types: Regional Registration Request and Regional Registration Reply. These messages are sometimes to be used instead of the existing Registration Request and Registration Reply, in order to reduce network load for Mobile IP registration.

Regional registration messages are protected by requiring authentication extensions, in the same way as the existing Mobile IP registration messages are protected. The following rules apply to authentication extensions which follow the fixed portion of the regional registration messages.

- The Mobile-Home Authentication extension [9] MUST NOT be included in any regional registration message.

- The Mobile-Foreign Authentication extension [9] MUST be included in all regional registration messages.
- The Foreign-Home Authentication extension [9] MUST NOT be included in any regional registration message.

5.1. Regional Registration Request

The Regional Registration Request is used by a mobile node to register with its current GFA.

The Regional Registration Request message is defined as the Registration Request message in [9], but with the following changes:

```
   Type        TBD (Regional Registration Request)

   GFA IP Address The IP address of the Gateway Foreign Agent.
               (Replaces Home Agent field in Registration Request
               message in [9].)

   Care-of Address MAY be set to zero.

   Extensions ...
```

5.2. Regional Registration Reply

The Regional Registration Reply is used by the GFA to indicate regional registration accept or denial to a mobile node.

The Regional Registration Reply message is defined as the Registration Reply message in [9], but with the following changes:

```
   Type        TBD (Regional Registration Reply)

   GFA IP Address The IP address of the Gateway Foreign Agent.
               (Replaces Home Agent field in Registration Reply
               message in [9].)

   Extensions ...
```

The values to use within the Code field of the Registration Reply are defined in [9]. In addition, the following values are defined:

Registration denied by the GFA:

- TBD requested replay protection unavailable (see section 6.3)

For a Regional Registration Reply, the following additional values are defined:

Registration denied by the FA:

TBD unknown GFA
TBD GFA unreachable (ICMP error received)
TBD GFA host unreachable (ICMP error received)
TBD GFA port unreachable (ICMP error received)
TBD GFA unreachable (other ICMP error received)

6. Regional Extensions to Registration Messages

In this section we specify new Mobile IP registration extensions for the purpose of managing regional registrations.

6.1. GFA IP Address Extension

If a foreign agent receives a Registration Request message from a mobile node, where the care-of address field is zero, the mobile node is requesting to be assigned a GFA. The foreign agent assigns a GFA to the mobile node, and adds a GFA IP Address extension to the Registration Request before relaying it to the GFA in question. The GFA IP Address extension MUST appear in the Registration Request message before the Foreign-Home Authentication extension, if present.

If a home agent receives a Registration Request message with the care-of address set to zero, and a GFA IP Address extension, it registers the IP address of the GFA as the care-of address of the mobile node. When generating a Registration Reply message, the home agent MUST include the GFA IP Address extension from the Registration Request in the Registration Reply message. The GFA IP Address extension MUST appear in the Registration Reply message before the Mobile-Home Authentication extension.

The GFA IP Address extension is defined as follows:

Type   TBD

Length   4

GFA IP Address   The GFA IP Address field contains the Gateway Foreign Agent's publicly routable address.

```
    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     |        GFA IP Address ....
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
            GFA IP Address         |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 5: The GFA IP Address extension

6.2. Hierarchical Foreign Agent Extension

One or more Hierarchical Foreign Agent extensions MAY be present in a Registration Request or in a Regional Registration Request. When these extensions are added to a registration request by a foreign agent, the receiving foreign agent sets up a pending registration record for the mobile node, using the IP address in the Hierarchical Foreign Agent extension as the care-of address for the mobile node. Furthermore, in this case, the extension MUST be appended at the end of all of the extensions that had been included by the mobile node as part of its registration message. When the receiving foreign agent receives the registration message, it MUST remove the Hierarchical Mobility Agent extension added by the sending foreign agent.

The Hierarchical Foreign Agent extension is defined as follows:

```
    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     |       FA IP Address ....
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
           FA IP Address ....      |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 6: The Hierarchical Foreign Agent Extension

Type   TBD (Hierarchical Foreign Agent)

Length   4

FA IP Address The IP Address of the foreign agent relaying the
            Registration Request.

6.3. Replay Protection

When a mobile node uses Mobile IP to register a care-of address with its home agent, the style of replay protection used for the registration messages is assumed to be known by way of a Mobility Security Association that is required to exist between the mobile node and the home agent receiving the request. No such pre-existing security association between the mobile node and the GFA is likely to be available. By default, the mobile node SHOULD treat replay protection for Regional Registration messages exactly as specified in RFC 2002 [9] for timestamp-based replay protection.

If the mobile node requires nonce-based replay protection, also as specified in RFC 2002, it MAY append a Replay Protection extension to the Registration Request message (see section 5.1). The format of this extension is shown in figure 7.

```
    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     |    Replay Protection Style    |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   +                    Initial Identification                     +
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 7: The Replay Protection Extension

Type   TBD (Replay Protection)

Length   2

Replay Protection Style
            An integer specifying the style of replay protection desired by the mobile node.

Initial Identification
            The timestamp or nonce to be used for initial synchronization for the replay mechanism.

Admissible values for the Replay Protection Style are as follows:

0 timestamp [9]
1 nonce [9]

7. Security Considerations

This document proposes a method for a mobile node to register locally in a visited domain. A authentication extensions are expected to be those defined either in [9], [8], or [3]. Furthermore, it assumes key distribution to be performed according to, for instance, [3] or [7].

8. Acknowledgements

This draft is a logical successor to drafts written with Pat Calhoun and Gabriel Montenegro; thanks to them and their many efforts to help explore this problem space. Many thanks also to Jari Malinen at the Helsinki University of Technology for his commentary on a rough version of this draft, and providing motivation for section dereg.

References

[1] B. Aboba and M. Beadles. RFC 2486: The Network Access Identifier, January 1999. Status: PROPOSED STANDARD.

[2] S. Bradner. Key Words for Use in RFCs to Indicate Requirement Levels. RFC 2119, March 1997.

[3] P. Calhoun and C. E. Perkins. DIAMETER Mobile IP Extensions. draft-calhoun-diameter-mobileip-01.txt, November 1998. (work in progress).

[4] Stephen E. Deering, Editor. ICMP Router Discovery Messages. RFC 1256, September 1991.

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

[6] Charles E. Perkins and Pat R. Calhoun. Aaa registration keys for mobile IP. draft-ietf-mobileip-aaa-key-00.txt, June 1999. (work in progress).

[7] Charles E. Perkins and David B. Johnson. Registration Keys for Route Optimization. draft-ietf-mobileip-regkey-00.txt, November 1997. (work in progress).

[8] Charles E. Perkins and David B. Johnson. Route Optimization in Mobile-IP. draft-ietf-mobileip-optim-08.txt, February 1999. (work in progress).

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

A. Hierarchical Foreign Agents

The main body of this draft assumes two hierarchy levels of foreign agents in the visited domain. At the top level, there is one or several GFAs, and on the lower level, there is a number of foreign agents. The structure can be extended to include multiple hierarchy levels of foreign agents beneath the GFA level (Figure 8). Such multiple hierarchy levels are discussed in this appendix.

```
                          ________
                         |        |
                         |  GFA   |
                         |________|
                          /   |  \
                        ...  ...  ...
                          ____|___
                         |        |
                         |   FA3  |
                         |________|
                    ______/_     _\______
                   |        |   |        |
                   |   FA2  |   |   FA1  |
                   |________|   |________|
                        |        ____|___
                                |        |
                                |   MN   |
                                |________|
```

Figure 8: Domain with a GFA and multiple hierarchies of FAs.

We assume that there exist established security associations among a GFA and all the foreign agents beneath it in the hierarchy. As before, we assume that when a mobile node performs registration at its home network, registration keys are generated and distributed to the mobile node and to the GFA. The GFA may then in turn distribute the registration keys to the foreign agents beneath it in the hierarchy, using methods not specified in this document.

A.1. Registration with Home Agent

As described in this draft, a foreign agent announces itself and a GFA in the Agent Advertisement; in the first and last address in the care-of address field in the Mobility Agent Advertisement extension [9]. If there is a hierarchy of foreign agents between the GFA and the announcing foreign agent, the foreign agent MAY include the corresponding addresses in order between its own address (first) and the GFA address (last):

- Address of announcing foreign agent
- Address of the next higher-level foreign agent
- ...
- Address of GFA

If a foreign agent advertises the entire hierarchy between itself and the GFA, the Registration Request and Regional Registration Request messages MUST be delivered to each care-of address in turn within that hierarchy.

When newly arriving at a visited domain, the mobile node sends a Registration Request, with the care-of address set to the GFA address announced in the Agent Advertisement. The mobile node may also request a GFA to be assigned to it, as described earlier in this draft.

When the foreign agent closest to the mobile node receives the Registration Request, it processes it as described in Section 3.4.2. It adds a Hierarchical Foreign Agent extension to the Registration Request, including its own address, and relays the Registration Request to the next foreign agent in the hierarchy toward the GFA.

The next foreign agent receives the Registration Request. For each pending or current registration, a foreign agent maintains a visitor list entry as described in [9]. In addition to the list entry contents required in [9], the list entry for regional registrations MUST contain:

- the address of the next lower-level foreign agent in the hierarchy
- the remaining Lifetime of the regional registration.

The foreign agent removes the Hierarchical Foreign Agent extension that the last foreign agent added, and adds a new Hierarchical Foreign Agent extension with its own address. This procedure is repeated in each foreign agent in the hierarchy toward the GFA.

When the GFA receives the Registration Request, it removes the Hierarchical Foreign Agent extension and caches information about the next lower-level foreign agent in the hierarchy. It then relays the Registration Request to the home agent, possibly via AAA servers.

For each pending or current registration, the GFA maintains a visitor list entry as described in [9]. In addition to the list entry contents required in [9], the list entry MUST contain:

- the address of the next lower-level foreign agent in the hierarchy
- the remaining Lifetime of the regional registration.

If there is only one level of hierarchy beneath the GFA, the address of the next lower-level foreign agent is the current care-of address of the mobile node, as stated in Section 3.4.3.

The home agent, as described before, processes the Registration Request, stores the GFA address as the current care-of address of the mobile node, generates a Registration Reply, and sends it to the GFA. The home agent also distributes a registration key to the mobile node and to the GFA, for instance by using a Home-Mobile Key Reply extension and a Foreign Agent Key Reply extension [7], added to the Registration Reply message, or via other AAA functions [6].

When the GFA receives the Registration Reply, it checks with its cached information to see which next lower-level foreign agent to send the Registration Reply message to. If, for instance, the Foreign Agent Key Reply extension [8] is present, the GFA decrypts the key. It SHOULD then add, for instance, a new Foreign Agent Key Reply extension to the Registration Reply message, before relaying it to the next foreign agent. The new Foreign Agent Key Reply extension contains the registration key, encrypted with a secret shared between the GFA and the next lower-level foreign agent in the hierarchy. Similar procedures are be used with [6].

The next lower-level foreign agent receives the Registration Request and checks its cached information to see which lower-level foreign agent should next receive the Registration Reply. It reads, decrypts and caches the registration key, and relays the Registration Reply to the next foreign agent. This procedure is repeated in every foreign agent in the hierarchy, until the message reaches the foreign agent closest to the mobile node.

When the lowest-level foreign agent receives the Registration Reply, it checks its cached information, as described in [9], and relays the Registration Reply to the mobile node.

A.2. Regional Registration

A Regional Registration Request is addressed to the GFA by way of one or more intermediate foreign agents. When the Regional Registration Request message arrives at the first foreign agent, the foreign agent checks its visitor list to see if this mobile node is already registered with it. If it is not, the foreign agent checks which next higher-level foreign agent to relay the Regional Registration Request to. It adds a Hierarchical Foreign Agent extension to the

Regional Registration Request, including its address, and relays the message to the next foreign agent in the hierarchy toward the GFA.

The next foreign agent checks its visitor list to see if the mobile node is already registered with it. If it is not, the foreign agent removes the Hierarchical Foreign Agent extension and adds a new one, with its own address, and relays the message to the next higher-level foreign agent in the hierarchy toward the GFA.

This process is repeated in each foreign agent in the hierarchy, until a foreign agent recognizes the mobile node as already registered. This foreign agent may be the GFA, or any foreign agent beneath it in the hierarchy. If the mobile node is already registered with this foreign agent, the foreign agent generates a Regional Registration Reply and sends it to the next lower-level foreign agent in the hierarchy. The lifetime field in the Regional Registration Reply is set to the remaining lifetime that was earlier agreed upon between the mobile node and the GFA. If the remaining lifetime of the GFA registration is shorter than a certain limit, the Regional Registration Request is relayed all the way to the GFA.

If the hierarchy between the advertising foreign agent and the GFA is announced in the Agent Advertisement, the mobile node may generate a Regional Registration Request not destined to the GFA, but to the closest foreign agent with which it can register.

DISCUSSION:

Need to specify how nonces can be used with multiple levels of hierarchy. Use idea of "nonce vector" from old hierarchical foreign agent draft. If structure of foreign agents with private addresses is to be hidden from the mobile node, define new FA-FA extensions to transmit current nonce values.

If a mobile node includes a Hierarchical Foreign Agent extension in its registration request message, it MAY insert the extension before the MN-HA or MN-FA authentication extension. In this case, the Hierarchical Foreign Agent extension MUST NOT be removed by the GFA or any other foreign agent prior to the generation of the registration reply message.

If more than one Hierarchical Foreign Agent extension is inserted by the mobile node into the registration message, the order of the extensions MUST be maintained through the hierarchy. When sending a Regional Registration Reply, the GFA MUST ensure that the order of the Hierarchical Foreign Agent extensions is reversed from the order found in the Regional Registration Request.

As before, if Hierarchical Foreign Agent extensions are present in a Request, each foreign agent receiving it makes note of the address of the next lower-level foreign agent along with the rest of the information in the pending registration request for the mobile node, for future association with the mobile node's home address.

A.2.1. Deregistration

If the GFA receives a Regional Registration Request message from a mobile node, and the mobile node uses a foreign agent care-of address for its regional registration, then there are the following possibilities:

1. The mobile node is registering at the same foreign agent as during its previous registration.

2. The mobile node is registering at a different foreign agent and using smooth handoff extensions [8].

3. The mobile node is registering at a different foreign agent but not using any smooth handoff extensions.

In case (1), there is no need for a deregistration, while in case (3) and (2), there is. Since any foreign agent in the hierarchy, that recognizes the mobile node as already registered, may generate a Regional Registration Reply, not all Regional Registration Requests will reach the GFA. Therefore, if old locations are not deregistered, it is possible that tunnels are not correctly redirected when a mobile node moves back to a previous foreign agent.

In case (2), when the mobile node uses smooth handoff extensions, the previous foreign agent is notified that the mobile node has moved. The previous foreign agent then forwards traffic to the new foreign agent.

In case (3), the mobile node sends a Regional Registration Request to its new foreign agent. If the mobile node does not request smooth handoff, the previous foreign agent is not notified. The Regional Registration Request is relayed upwards in the hierarchy until it reaches a foreign agent that recognizes the mobile node as already registered. This foreign agent generates a Regional Registration Reply and sends it downwards in the hierarchy toward the new location of the mobile node, updating its own visitor list. At the same time, it also sends a Binding Update with a zero lifetime to the previous care-of address it had registrered for the mobile node. Each foreign agent receiving the (authenticated!) Binding Update removes the mobile node from its visitor lists. The Binding Update is relayed down to the care-of address of the mobile node known to that foreign agent, and each foreign agent in the hierarchy receiving this notification removes the mobile node from its visitor list.

If the mobile node uses a co-located care-of address for its regional registration, there is no need to deregister its previous location when it moves, since regional registrations with a co-located care-of address are performed directly with the GFA.

A.3. Traffic

When a correspondent node sends traffic to the mobile node, the traffic arrives at the home agent, and the home agent tunnels the traffic to the GFA. The GFA or foreign agent at each level of the hierarchy has a visitor list for the mobile node, showing the address of the next lower-level foreign agent in the hierarchy.

Thus, a datagram arriving at the top level of the hierarchy, that is, the GFA, will be decapsulated and re-encapsulated with the new tunnel endpoint at the next lower-level foreign agent in the hierarchy. This decapsulation and re-encapsulation occurs at each level of the hierarchy, until the datagram reaches the last tunnel endpoint which is either the mobile node itself (in case of a co-located care-of address) or a foreign agent that can deliver the decapsulated datagram to the mobile node with no further special Mobile IP handling.

Note that the actual decapsulation need not occur at each step of the hierarchy. Instead, the foreign agent at that level can merely change the source and destination IP addresses of the encapsulating IP header.

Traffic from the mobile node is sent as described in [9] or [5].

Addresses

The working group can be contacted via the current chairs:

Basavaraj Patil
Nortel Networks Inc.
2201 Lakeside Blvd.
Richardson, TX. 75082-4399
USA

+1 972-684-1489

bpatil@nortelnetworks.com

Phil Roberts
Motorola
1501 West Shure Drive
Arlington Heights, IL 60004
USA

+1 847-632-3148

QA3445@email.mot.com

Questions about this memo can be directed to:

Eva Gustafsson
Ericsson Radio Systems AB
Network and Systems Research
SE-164 80 Stockholm
SWEDEN
+46 8 7641342
Eva.Gustafsson@ericsson.com

Annika Jonsson
Ericsson Radio Systems AB
Network and Systems Research
SE-164 80 Stockholm
SWEDEN
+46 8 4047242
Annika.Jonsson@ericsson.com

Charles E. Perkins
Sun Microsystems Laboratories
15 Network Circle
Menlo Park, California 94025
USA

Phone: +1-650 786-6464
EMail: cperkins@eng.sun.com
Fax: +1 650 786-6445