Mobile IPv4 Regional Registration

Status of This Memo

This memo defines an Experimental Protocol for the Internet
community. It does not specify an Internet standard of any kind.
Discussion and suggestions for improvement are requested.
Distribution of this memo is unlimited.

Copyright Notice

Abstract

Using Mobile IP, a mobile node registers with its home agent each
time it changes care-of address. This document describes a new kind
of "regional registrations", i.e., registrations local to the visited
domain. The regional registrations are performed via a new network
entity called a Gateway Foreign Agent (GFA) and introduce a layer of
hierarchy in the visited domain. 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 document is an optional
extension to the Mobile IPv4 protocol.

Table of Contents

1. Introduction

   This document is an optional extension to the Mobile IPv4 protocol,
   and proposes a means for mobile nodes to register locally within a
   visited domain. By registering locally, the number of signaling
   messages to the home network are kept to a minimum, and the signaling
   delay is reduced.

   In Mobile IP, as specified in [RFC3344], 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
   minimize 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 will both
   decrease the load on the home network, and speed up the process of
   handover within the visited domain.

   Regional registrations introduce a new network node: the Gateway
   Foreign Agent (GFA). The address of the GFA is advertised by the
   foreign agents in a visited domain. When a mobile node first arrives
   at this visited domain, it performs a home registration -- that is, a
   registration with its home agent. At this registration, the mobile
   node registers the address of the GFA as its care-of address with its
   home agent. When moving between different foreign agents within the
   same visited domain, the mobile node only needs to make a regional
   registration to the GFA.

   In their simplest form, regional registrations are performed
   transparently to the home agent. Additionally, regional
   registrations may also allow dynamic assignment of GFA. The solution
   for dynamic GFA assignment requires support in the mobile node, the
   foreign agent, the GFA, and the home agent.

   The proposed regional registration protocol supports one level of
   foreign agent hierarchy beneath the GFA, but the protocol may be
   utilized to support several levels of hierarchy. Multiple levels of
   hierarchy are not discussed in this document.

   Although this document focuses on regional registrations in visited
   domains, regional registrations are also possible in the home domain.

   Foreign agents that support regional registrations are also required
   to support registrations according to Mobile IPv4 [RFC3344].

   The following section gives an overview of regional registrations.

2. Overview of Regional Registrations

In standard Mobile IP, there are three entities of interest. The
Mobile Node (MN), the Foreign Agent (FA), and the Home Agent (HA).
The MN communicates with the HA, either through an FA or directly (if
it has a co-located care-of address). With Regional Registrations, a
new entity is defined: the Gateway Foreign Agent (GFA). The GFA sits
between the MN/FA and HA, and to the HA, it appears as if the MN's
temporary care-of address is that of the GFA. When a MN moves within
a site, it only need interact with the GFA, so that the GFA knows at
what temporary address the MN is currently reachable.

Two types of registration messages are used. Regular [RFC3344]
Registration Requests/Replies are still used for when the MN
exchanges Registration Requests/Replies with the HA, but these
messages get forwarded through a GFA, and include new extensions.

In addition, a new pair of registration messages, Regional
Registration Requests/Replies, are used between MNs/FAs/GFAs for
intra-site signaling. A MN uses these messages to communicate its
new addresses to the GFA as it moves around within a site.

There are two models of how the MN uses Regional Registrations. The
FA can advertise a GFA to the MN. Alternatively, the FA can indicate
that dynamic assignment of GFA is to be used. With dynamic GFA
assignment, the MN does not choose the GFA, rather the FA (or GFA)
does so after receiving a Registration Request from the MN. However,
in this mode the HA must understand (and support) Regional
Registrations in order for them to be used. This last form is not
transparent because the MN doesn't know in advance what GFA will be
used, and cannot include it in a signed message to the HA.

When a MN moves to a new domain (determined by comparing its Network
Access Identifier (NAI) [RFC4282] with the FA-NAI included in
received Agent Advertisements), it can opt to use Regional
Registrations. A site indicates support for Regional Registrations
by setting the I-bit of the Mobile IP Agent Advertisement extension.
In addition, such advertisements include a list of one or more care-
of addresses. If there is only one care-of address, this is the
address of the FA itself. In addition, the advertisement may include
the address of the GFA. A GFA care-of address of all-ones indicates
that dynamic assignment of GFA is supported.

A MN requests initial Regional Registration by sending a normal
Registration Request to the FA, but setting the care-of address to
that of the GFA (i.e., if it has selected it wishes to use this GFA)
or all-zeros (which signals a dynamic GFA assignment request). The
FA adds a Hierarchical FA (HFA) extension and relays the request to

the appropriate GFA. The HFA extension contains a single field: the
IP address of the FA.

Note: the algorithm for MNs with co-located care-of addresses is
similar, except that there is no FA, so the MN behaves as the FA in
terms of the messages it sends.

A GFA receives Registration Requests relayed from an FA. If the
care-of address in the received Registration Request is zero, the GFA
assigns one. A GFA IP Address extension is then added to the
Registration Request, and the message is forwarded to the HA. The
GFA IP Address extension contains a single field: the IP address of
the GFA. (A separate field is needed for this because the
Registration Request message between the MN/HA is signed and cannot
be modified.)

HAs process received Registration Requests in the same way as before,
except in the case of dynamic GFA assignment. In this case, the HA
uses the GFA address from the GFA IP Address extension as the MN's
current care-of address. In addition, the Registration Reply message
must include the GFA IP Address extension.

The regular Registration Requests/Replies are protected as described
in [RFC3344], by use of the mobility security association between the
MN and the HA. For regional registrations, it is assumed that a
mobility security association is established between the MN and GFA
during registration with the HA. Regional Registration Requests/
Replies are protected by use of this security association between the
MN and the GFA, e.g., by use of a MN-GFA Authentication extension.

HFA extensions, added by an FA to a Registration Request or Regional
Registration Request, are protected by an FA-FA Authentication
extension. Security associations between FAs and GFAs within a
domain are assumed to exist prior to regional registrations.

Dynamic GFA assignment requires means for securely sending
Registration Requests from the GFA to the HA, in order to protect the
GFA IP Address extension.

3. 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 [RFC2119].

This document uses the following terms:

Critical type
   A type value for an extension in the range 0-127, which indicates
   that the extension MUST either be known to the recipient, or that
   the message containing the extension MUST be rejected. In other
   words, an extension with a critical type value is non-skippable.

Domain
   A collection of networks sharing a common network administration.

Foreign Agent (FA)
   As defined in [RFC3344].

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.

Home Agent (HA)
   As defined in [RFC3344].

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

Home network
   As defined in [RFC3344].

Home Registration
   A registration, processed by the home agent and the GFA, using the
   specification in [RFC3344] possibly with additional extensions
   defined in this document.

Local Care-of Address
   A care-of address that is assigned to either a mobile node or 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.

Mobile Node (MN)
   As defined in [RFC3344].

Mobility Agent (MA)
   As defined in [RFC3344].

Network Access Identifier(NAI)
   Some features of this protocol specification rely on use of the
   Network Access Identifier (NAI) [RFC2794].

   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
      signals and control messages specified by Mobile IP.

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

   Visited network
      As defined in [RFC3344].

4. Description of the Protocol

   This section provides an overview of the regional registration
   protocol.

4.1. General Assumptions

   Our general model of operation is illustrated in Figure 1, showing a
   visited domain with FA and GFA, and a home network with a HA:

```
   +----------------------------+              +-----------------+
   |       Visited Domain       |              |      Home       |
   |                            |  +---------+ |    Network      |
   |                            |  |         | |                 |
   |   +------+     +-------+    |  | Public  | |    +------+     |
   |   | FA   |-----| GFA   |-------------------------| HA   |     |
   |   +--+---+     +-------+    |  | Network | |    +------+     |
   |      |                     |  |         | |                 |
   +------|---------------------+  +---------+ +-----------------+
          |
       +--+---+
       | MN   |
       +------+
```
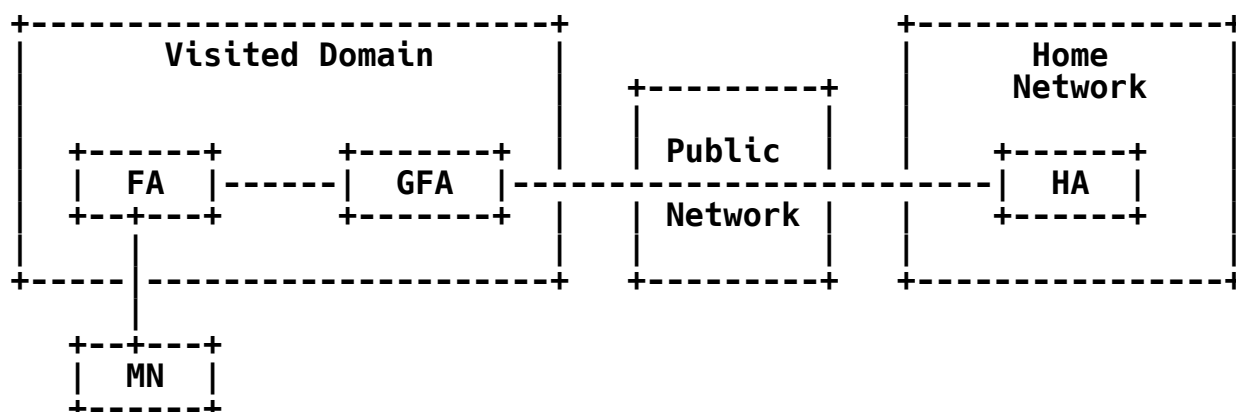
                    Figure 1: Model of Operation

   For MNs that cannot process a NAI, or with mobility agents that are
   not configured to advertise their NAI, regional registration is still
   useful, but processing the NAI makes it easier for the mobile node to
   reliably detect domain changes.

4.1.1. Visited Domain

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

   When a MN changes care-of address under the same GFA, it MAY perform
   a regional registration. If the MN changes GFA, within a visited
   domain or between visited domains, it MUST perform a home
   registration.

4.1.2. Authentication

   With regional registrations, a GFA address is registered at the HA as
   the care-of address of the MN. If a Mobile-Foreign (MN-FA)
   Authentication extension is present in a Registration Request message
   directed to the HA, the GFA will perform the authentication.
   Similarly, if a Foreign-Home (FA-HA) Authentication extension is
   present in a Registration Request message, the authentication is
   performed between the GFA and the HA. To summarize, the GFA takes
   the role of an FA with regard to security associations in the home
   registrations.

   Regional registration messages also need to be protected with
   authentication extensions in the same way as registrations with the
   HA. This means that the MN and the GFA MUST have received the keys
   needed to construct the authentication extensions before any regional
   registration is performed. As described above, since the GFA address
   is the registered care-of address of the MN at its home network, the
   GFA is the agent within the visited domain that has to have the
   appropriate security associations with the HA and the MN. The GFA's
   security association with the MN is then used to enable proper
   authentication for regional registrations (see Section 6). How the
   keys are distributed is outside the scope of this draft. One example
   is to distribute the keys as part of the home registration, for
   example according to [RFC4004] and [RFC3957]. Another example is
   pre-configured keys.

4.2. Protocol Overview

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

Since the care-of address registered at the HA is the GFA address, it
will not change when the MN changes FA under the same GFA. Thus, the
HA does not need to be informed of further MN movements within the
visited domain.

Figure 2 illustrates the signaling message flow for home
registration. During the home registration, the HA records the GFA
address as the care-of address of the MN.

```
   MN                         FA1                      GFA                   HA
    |                          |                        |                    |
    |  Registration Request    |                        |                    |
    |------------------------->|  Reg.  Request         |                    |
    |                          |----------------------->|  Reg.  Request     |
    |                          |                        |--------------->    |
    |                          |                        |  Reg.  Reply       |
    |                          |  Reg.  Reply           |<---------------    |
    |  Registration Reply      |<-----------------------|                    |
    |<-------------------------|                        |                    |
    |                          |                        |                    |
```
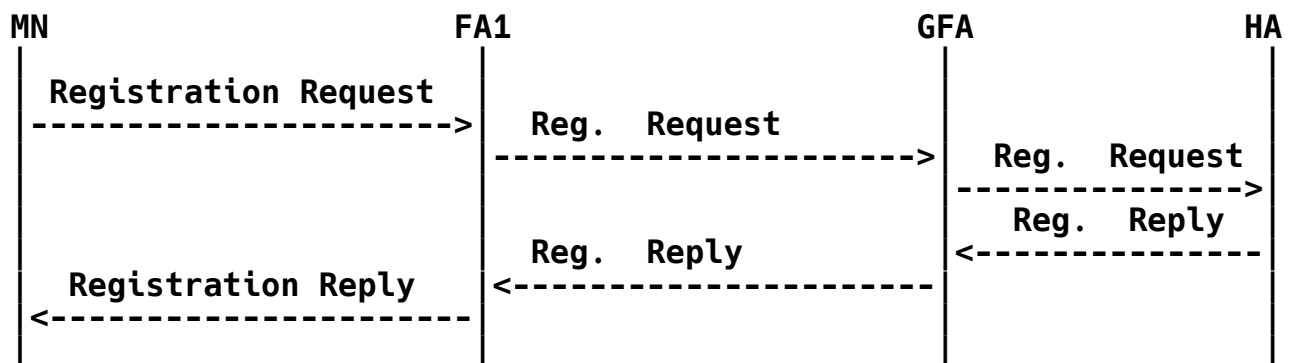
                       Figure 2: Home Registration

Figure 3 illustrates the signaling message flow for regional
registration. Even though the MN's local care-of address changes,
the HA continues to use the GFA address as the care-of address of the
MN. We introduce two new message types for regional registrations:
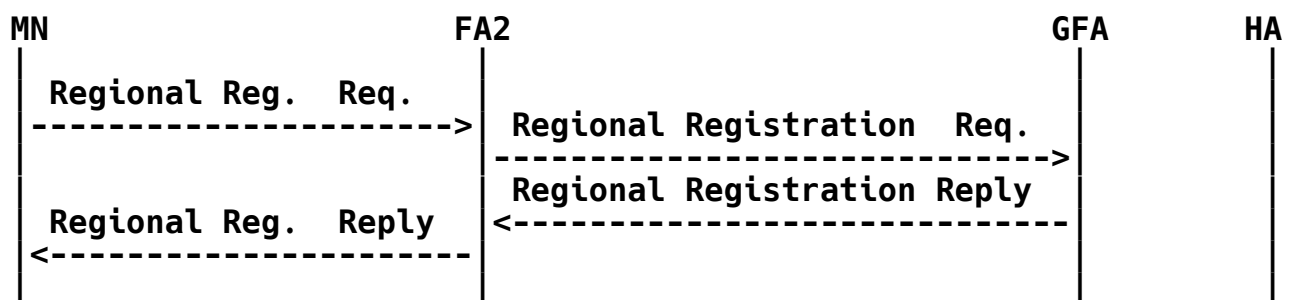Regional Registration Request and Regional Registration Reply.

```
   MN                        FA2                         GFA        HA
   |                          |                           |          |
   | Regional Reg.  Req.      |                           |          |
   |------------------------->| Regional Registration  Req.          |
   |                          |-------------------------->|          |
   |                          | Regional Registration Reply          |
   | Regional Reg.  Reply     |<--------------------------|          |
   |<-------------------------|                           |          |
   |                          |                           |          |
```

                  Figure 3: Regional Registration

4.3. Advertising Foreign Agent and GFA

   A FA typically announces its presence via an Agent Advertisement
   message [RFC3344]. If the domain to which an FA belongs supports
   regional registrations, the following changes apply to the Agent
   Advertisement.

   The 'I' flag (see Section 8.1) MUST be set to indicate that the
   domain supports regional registrations. If the 'I' flag is set,
   there MUST be at least one care-of address in the Agent
   Advertisement. If the 'I' flag is set and there is only one care-of
   address, it is the address of the FA. If the 'I' flag is set, and
   there is more than one care-of address, the first care-of address is
   the local FA, and the last care-of address is the GFA. (Any care-of
   addresses advertised in addition to these two are out of scope for
   this document).

   The FA-NAI (see Section 8.2) SHOULD also be present in the Agent
   Advertisement to enable the MN to decide whether or not it has moved
   to a new domain since its last registration. The decision is based
   on whether the realm part of the advertised FA-NAI matches the realm
   of the FA-NAI advertised by the MN's previous FA.

4.4. Backwards Compatibility with RFC 3344

   A domain that supports regional registrations should also be
   backwards compatible.

   An FA MUST support registrations according to Mobile IPv4 as defined
   in [RFC3344]. This allows MNs that don't support regional
   registrations to register via this FA using standard Mobile IPv4. If
   the FA advertises both its own care-of address and a GFA care-of
   address, a MN that supports regional registrations but has a HA that
   doesn't, will still be able to make use of regional registrations
   through that GFA care-of address.

The advertised GFA care-of address MAY be set to all-ones, to
indicate dynamic GFA assignment. If the MN supports regional
registrations, and an all-ones GFA care-of address is advertised, the
MN SHOULD use dynamic GFA assignment (see Section 7.1).

5. Home Registration

This section gives a detailed description of home registration, i.e.,
registration with the HA (on the home network). Home registration is
performed when a MN first arrives at a visited domain, when it
requests a new HA, or when it changes GFA. Home registration is also
performed to renew bindings which would otherwise expire.

5.1. Mobile Node Considerations

Upon receipt of an Agent Advertisement message with the 'I' flag set
and an FA-NAI extension, the MN compares the domain part of the FA
NAI with the one received in the previous Agent Advertisement, to
determine whether it has moved to a new domain since its last
registration. If the NAIs do not match, the MN MUST assume it has
moved to a new domain.

If the MN determines that it has moved to a new domain, it SHOULD
insert the advertised GFA address in the care-of address field in the
Registration Request message. For dynamic GFA assignment, see
Section 7.1.

A MN with a co-located care-of address might also want to use
regional registrations. It then finds out the address of a GFA,
either from Agent Advertisements sent by an FA, or by some means not
described in this document. The MN 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 an FA). In this case, the
MN MUST add a Hierarchical Foreign Agent (HFA) extension (see Section
9.2), including its co-located care-of address, to the Registration
Request before sending it. The HFA extension MUST be protected by an
authentication extension. If the MN has established a mobility
security association with the GFA, the HFA extension MUST be placed
before the MN-FA Authentication extension, and it SHOULD be placed
after the Mobile-Home (MN-HA) Authentication extension. Otherwise,
if the MN has no established mobility security association with the
GFA, the HFA extension MUST be placed before the MN-HA authentication
extension.

If the MN receives an Agent Advertisement with the 'R' bit set, even
if it has a co-located care-of address, it still formulates the same
Registration Request message with extensions, but it sends the
message to the advertising FA instead of to the GFA.

If the home registration is about to expire, the MN performs a new
home registration using the same GFA care-of address to refresh the
binding [RFC3344]. If the MN has just moved to a new FA and not yet
sent a Regional Registration Request when the home registration is
due to expire, the MN sends only a Registration Request, as this will
update both the GFA and the HA.

If the Registration Reply includes a Replay Protection Style
extension, the value in the Initial Identification field is the value
to be used for replay protection in the next Regional Registration
Request (see Section 6.1).

5.2. Foreign Agent Considerations

When the FA receives a Registration Request message from a MN, it
extracts the care-of address field to find the GFA to which the
message shall be relayed. All FAs that advertise the 'I' flag MUST
also be able to handle Registration Requests with an all-zeros care-
of address (used for dynamic GFA assignment).

If the FA receives a Registration Request where the care-of address
is set to all-ones (which could happen if a MN that doesn't support
Regional Registrations copied an all-ones care-of address from an
Agent Advertisement), it MUST reply with the Code field set to
"poorly formed request" [RFC3344].

If the Registration Request has the 'T' bit set, the MN is requesting
Reverse Tunneling [RFC3024]. In this case, the FA has to tunnel
packets from the MN to the GFA for further handling.

If the care-of address in the Registration Request is the address of
the FA, the FA relays the message directly to the HA, as described in
[RFC3344]. For each pending or current home registration, the FA
maintains a visitor list entry as described in [RFC3344]. If reverse
tunneling is being used, the visitor list MUST contain the address of
the GFA, in addition to the fields required in [RFC3344].

Otherwise, if the care-of address in the Registration Request is the
address of a GFA (or all-zeros), the FA adds a Hierarchical Foreign
Agent (HFA) extension, including its own address, to the Registration
Request, and relays it to the GFA. The HFA extension MUST be
appended at the end of all previous extensions that were included in
the Registration Request when the FA received it, and it MUST be
protected by a Foreign-Foreign (FA-FA) Authentication extension (see
Section 11).

5.3. GFA Considerations

For each pending or current home registration, the GFA maintains a
visitor list entry as described in [RFC3344]. This visitor list
entry is also updated for the regional registrations performed by the
MN. In addition to the fields required in [RFC3344], the list entry
MUST contain:

o the current care-of address of the MN (i.e., the FA or co-located
   address) received in the HFA extension
o the remaining Lifetime of the regional registration
o the style of replay protection in use for the regional
   registration
o the Identification value for the regional registration.

The default replay protection style for regional registrations is
timestamp-based replay protection, as defined in Mobile IPv4
[RFC3344]. If the timestamp sent by the MN in the Registration
Request is not close enough to the GFA's time-of-day clock, the GFA
adds a Replay Protection Style extension (see Section 9.3) to the
Registration Reply, with the GFA's time of day in the Identification
field to synchronize the MN with the GFA for the regional
registrations.

If nonce-based replay protection is used, the GFA adds a Replay
Protection Style extension to the Registration Reply, where the high-
order 32 bits in the Identification fields is the nonce that should
be used by the MN in the following regional registration.

If the Registration Request contains a Replay Protection Style
extension (see Section 9.3) 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 REPLAY_PROT_UNAVAIL (see Section 9.5).

If the Hierarchical Foreign Agent (HFA) extension comes after the
MN-FA Authentication extension, the GFA MUST remove it from the
Registration Request. The GFA then sends the Registration Request to
the HA. Upon receipt of the Registration Reply, the GFA consults its
pending registration record to find the care-of address within its
domain that is currently used by the MN, and sends the Registration
Reply to that care-of address.

If the Replay Protection Style extension (see Section 9.3) is present
in a Registration Request, and follows the MN-HA Authentication
extension, the GFA SHOULD remove the Replay Protection Style
extension after performing any necessary processing and before
sending the Registration Request to the HA.

If the GFA receives a Registration Request from a MN that it already
has a mobility binding for, this is an update of a binding that is
about to expire. If the address in the Hierarchical Foreign Agent
(HFA) extension is the same as the current care-of address in the
visitor list for the MN, the entries in the visitor list concerning
regional registrations are not changed, except to update the
lifetime. If the address in the HFA extension is a new address, the
values for the regional registration are updated.

If the Registration Request has the 'T' bit set, the GFA has to
decapsulate the packets from the FA and re-encapsulate them for
further delivery back to the HA. These actions are required because
the HA has to receive such packets from the expected care-of address
(i.e., that of the GFA) instead of the local care-of address (i.e.,
that of the FA).

When receiving a Registration Reply from the HA, the GFA MAY add a
Regional Registration Lifetime extension to the message before
relaying it to the FA. The extension defines the lifetime that the
GFA allows the MN before it has to renew its regional registration.
The GFA MUST set the lifetime of the regional registration to be no
greater than the remaining lifetime of the MN's registration with its
HA. If used, the Regional Registration Lifetime extension MUST be
added after any other extensions, and MUST be protected by an MN-FA
Authentication extension.

5.4. Home Agent Considerations

The Registration Request is processed by the HA as described in
[RFC3344].

6. Regional Registration

This section describes regional registrations. Once the HA has
registered the GFA address as the care-of address of the MN, the MN
may perform regional registrations. When performing regional
registrations, the MN may either register an FA care-of address or a
co-located address with the GFA. In the following, we assume that a
home registration has already occurred, as described in Section 5,
and that the GFA has a mobility security association with the MN.

Suppose the MN moves from one FA to another FA within the same
visited domain. It will then receive an Agent Advertisement from the
new FA. Suppose further that the Agent Advertisement indicates that
the visited domain supports regional registrations, and either that
the advertised GFA address is the same as the one the MN has
registered as its care-of address during its last home registration,
or that the realm part of the newly advertised FA-NAI matches the FA-

NAI advertised by the MN's previous FA. Then, the MN can perform a
regional registration with this FA and GFA. The MN issues a Regional
Registration Request to the GFA via the new FA. The request is
authenticated using the existing mobility security association
between the GFA and the MN and the message is authenticated by the
MN-GFA Authentication extension (see Section 11). The care-of
address should be set to the address of the local FA.

If the Regional Registration Request contains a care-of address field
of all-zeros, the FA adds a Hierarchical Foreign Agent (HFA)
extension to the message and relays it to the GFA. Based on the
information in the HFA extension, the GFA updates the MN's current
point of attachment in its visitor list. The GFA then issues a
Regional Registration Reply to the MN via the FA.

If the advertised GFA is not the same as the one the MN has
registered as its care-of address, and if the MN is still within the
same domain as it was when it registered that care-of address, the MN
MAY try to perform a regional registration with its registered GFA.
If the FA cannot support regional registration to a GFA, other than
advertised, the FA denies the Regional Registration Request with code
UNKNOWN_GFA (see Section 10.3). In this case, the MN has to do a new
home registration via the new GFA.

New message types are introduced for the Regional Registration
Request and Reply. The motivation for introducing new message types,
rather than using the Registration Request and Reply defined in
[RFC3344] is: (1) the MN must be able to distinguish regional
registrations from home registrations, since in the former case the
timestamps/nonces are synchronized with its GFA and in the latter
with its HA; and (2) a home registration MUST be directed to the home
network before the lifetime of the GFA care-of address expires.

6.1. Mobile Node Considerations

For each pending or current home registration, the MN maintains the
information described in [RFC3344]. The information is also updated
for the regional registrations performed by the MN. In addition to
the information described in [RFC3344], the MN MUST maintain the
following information, if present:

o the GFA address
o the remaining Lifetime of the regional registration
o the style of replay protection in use for the regional
   registration
o the Identification value for the regional registration.

The replay protection for home registrations and regional
registrations is performed as described in [RFC3344]. Since the MN
performs regional registrations at the GFA in parallel with home
registrations at the HA, the MN MUST be able to keep one replay
protection mechanism and sequence for the GFA, and a separate
mechanism and sequence for the HA.

For regional registrations, replay protection may also be provided at
the FA by the challenge-response mechanism, as described in
[RFC4721].

6.2. Foreign Agent Considerations

When the FA receives a Regional Registration Request from a MN,
addressed to a GFA, it generally processes the message according to
the rules of processing a Registration Request addressed to a HA (see
Section 5.2). The only difference is that the GFA IP address field
replaces the HA address field. If that address belongs to a known
GFA, the FA forwards the request to the indicated GFA. Otherwise,
the FA MUST generate a Regional Registration Reply with error code
UNKNOWN_GFA.

For each pending or current registration, the FA maintains a visitor
list entry as described in [RFC3344]. If reverse tunneling is being
used, the visitor list MUST contain the address of the GFA, in
addition to the fields required in [RFC3344]. This is required so
that the FA can tunnel datagrams, sent by the MN, to the GFA. The
GFA then decapsulates the datagrams, re-encapsulates them, and sends
them to the HA.

6.3. GFA Considerations

If the GFA accepts a Regional Registration Request, it MUST set the
lifetime of the regional registration to be no greater than the
remaining lifetime of the MN's registration with its HA, and put this
lifetime into the corresponding Regional Registration Reply. The GFA
MUST NOT accept a request for a regional registration if the lifetime
of the MN's registration with its HA has expired. In that case, the
GFA sends a Regional Registration Reply with the value in the Code
field set to NO_HOME_REG.

If the GFA receives a tunneled packet from an FA 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, it checks the visitor list to see
whether reverse tunneling has been requested; if it was requested,
the GFA re-encapsulates the packet with its own address as the source
IP address, and the address of the HA as the destination IP address.

7. Dynamic GFA Assignment

   Regional registrations may also allow dynamic assignment of a GFA to
   a MN. The visited network (i.e., the FA) indicates support for
   dynamic GFA assignment by advertising an all-ones care-of address in
   the Agent Advertisement. The MN then sets the care-of address in the
   Registration Request to all-zeros to request a dynamically assigned
   GFA. Upon receiving this Registration Request, the FA relays it to
   the appropriate GFA, and the GFA assigns its address to the MN by
   means of a GFA IP Address extension added to the Registration
   Request.

   In order for dynamic GFA assignment to work, the MN, GFA, and HA,
   respectively, MUST support the GFA IP Address extension. Also, the
   FA MUST be able to advertise an all-ones care-of address and handle a
   Registration Request with an all-zeros care-of address.

   Note also that protection of the GFA IP Address extension, added to
   the Registration Request, requires either the use of an FA-HA
   Authentication extension or other means to secure the Registration
   Request when forwarded from the GFA to the HA.

7.1. Mobile Node Considerations for Dynamic GFA Assignment

   If the 'I' flag in the Agent Advertisement sent out by the FA is set,
   and the care-of address indicating the GFA is set to all-ones, this
   indicates support for dynamic GFA assignment.

   If the MN supports dynamic GFA assignment, and if the advertised GFA
   address is all-ones, the MN SHOULD set the care-of address field in
   the Registration Request to all-zeros to request to be assigned a
   GFA.

   When requesting dynamic GFA assignment, the MN MUST check to make
   sure that it receives a GFA IP Address extension in the Registration
   Reply.

7.2. Foreign Agent Considerations for Dynamic GFA Assignment

   If an FA supports dynamic GFA assignment, and receives a Registration
   Request with the care-of address field set to all-zeros, the FA
   assigns a GFA to the MN. A FA can either have a default GFA that it
   assigns to all MNs or it can assign a GFA by some means not described
   in this specification.

   If an FA that does not support dynamic GFA assignment receives a
   Registration Request with the care-of address field set to all-zeros,
   the FA will deny the request as described in [RFC3344], i.e., by

sending a Registration Reply with the Code field set to "invalid
care-of address".

7.3. GFA Considerations for Dynamic GFA Assignment

If a GFA supports dynamic GFA assignment, and receives a Registration
Request with the care-of address field set to all-zeros, the GFA
assigns its own IP address as care-of address for this MN, and adds a
GFA IP Address extension with this address to the Registration
Request. The GFA MUST NOT insert the GFA IP address directly in the
care-of address field in the Registration Request, since that would
cause the MN-HA authentication to fail.

The GFA IP Address extension has to be protected so that it cannot be
changed by a malicious node when the Registration Request is
forwarded to the HA. If the HA and the GFA have a mobility security
association, the GFA IP Address extension MUST be protected by the
FA-HA authentication extension. Otherwise, the Registration Request
MUST be sent to the HA in a secure way, for example via a secure AAA
protocol (e.g., [RFC4004], [RFC3957]).

If the GFA does not support dynamic GFA assignment, it will deny the
request by sending a Registration Reply with the Code field set to
ZERO_COA_NOT_SUPP (see Section 9.5).

7.4. Home Agent Considerations for Dynamic GFA Assignment

If a HA receives a Registration Request with a GFA IP Address
extension, and the HA does not allow the use of this extension, the
HA MUST return a Registration Reply with the Code value set to
DYN_GFA_NOT_SUPP (see Section 9.5).

If a HA receives a Registration Request message with the care-of
address set to all-zeros, but no GFA IP Address extension, it MUST
deny the request by sending a Registration Reply message with the
Code field set to ZERO_CAREOF_ADDRESS (see Section 9.5).

If a HA that does not support dynamic GFA assignment receives a
Registration Request with a GFA IP Address extension, the request
will be denied by the HA, as described in [RFC3344].

If a HA that supports dynamic GFA assignment receives a Registration
Request with the care-of address set to all-zeros and a GFA IP
Address extension, it MUST register the IP address of the GFA as the
care-of address of the MN in its mobility binding list. If the
Registration Request is accepted, the HA MUST include the GFA IP
Address extension in the Registration Reply, before the MN-HA
Authentication extension.

7.5. Regional Registration

   If the MN receives an Agent Advertisement with the care-of address
   field indicating the GFA set to all-ones, and if the MN determines
   that it is within the same visited domain as when it did its last
   home registration, it MAY send a Regional Registration Request to its
   current GFA. Otherwise, it MUST send a Registration Request to its
   HA as described in Section 7.1.

8. Router Discovery Extensions

   This section specifies a new flag within the Mobile IP Agent
   Advertisement, and an optional extension to the ICMP Router Discovery
   Protocol [RFC1256].

8.1. Regional Registration Flag

   The only change to the Mobility Agent Advertisement Extension defined
   in [RFC3344] is a flag indicating that the domain, to which the FA
   generating the Agent Advertisement belongs, supports regional
   registrations. The flag is inserted after the flags defined in
   [RFC3344], [RFC3024], and [RFC3519].

   Regional Registration flag:

```
     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     |         Sequence Number       |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |         Lifetime              |R|B|H|F|M|G|r|T|U|I| reserved  |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                   zero or more Care-of Addresses              |
    |                              ...                              |
```
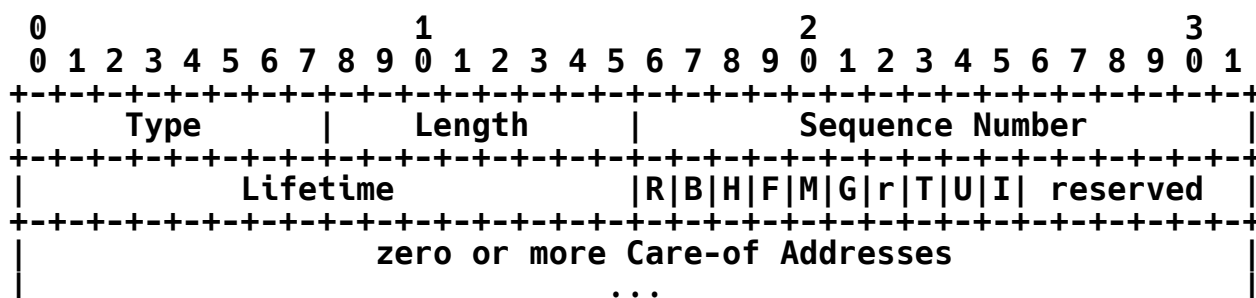
   The flag is defined as follows:

          Type   16 (Mobility Agent Advertisement)

          I   Regional Registration. This domain supports
                  regional registration as specified in this document.

8.2. Foreign Agent NAI Extension

   The FA-NAI extension is defined as subtype 3 of the NAI Carrying
   Extension [RFC3846].

The FA SHOULD include its NAI in the Agent Advertisement message. If
present, the Foreign Agent NAI (FA-NAI) extension MUST appear in the
Agent Advertisement message after any of the advertisement extensions
defined in [RFC3344].

By comparing the domain part of the FA-NAI with the domain part of
the FA-NAI it received in the previous Agent Advertisement, the MN
can determine whether it has moved to a new domain since it last
registered.

9. Regional Extensions to Mobile IPv4 Registration Messages

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

9.1. GFA IP Address Extension

The GFA IP Address extension is defined for the purpose of supporting
dynamic GFA assignment. If the MN requests a dynamically assigned
GFA, the GFA adds a GFA IP Address extension to the Registration
Request before relaying it to the HA. The MN indicates that it wants
a GFA to be assigned by sending a Registration Request with the
care-of address field set to all-zeros. The GFA IP Address extension
MUST appear in the Registration Request before the FA-HA
Authentication extension, if present.

If a HA receives a Registration Request message with the care-of
address set to all-zeros, and a GFA IP Address extension, it MUST
register the IP address of the GFA as the care-of address of the MN.
When generating a Registration Reply message, the HA 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 MN-HA Authentication
extension.

The GFA IP Address 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      |            reserved       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          GFA IP Address                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
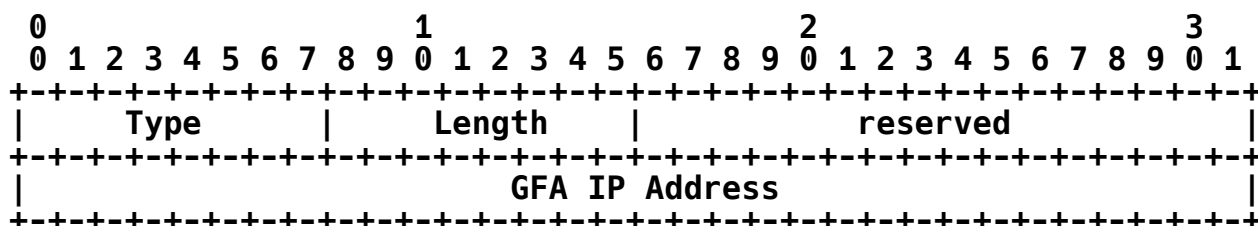
Type
   46 (GFA IP Address) (non-skippable)

Length
     6

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

9.2. Hierarchical Foreign Agent Extension

   The Hierarchical Foreign Agent (HFA) extension may be present in a
   Registration Request or Regional Registration Request. When an FA
   adds this extension to a Registration Request, the receiving mobility
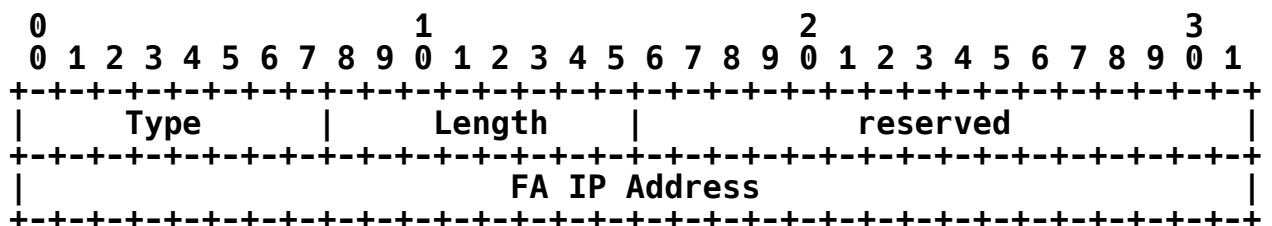   agent (GFA) sets up a pending registration record for the MN, using
   the IP address in the HFA extension as the care-of address for the
   MN. Furthermore, in this case, the extension MUST be appended at the
   end of all previous extensions that had been included in the
   registration message as received by the FA. The HFA extension MUST
   be protected by an FA-FA Authentication extension. When the
   receiving mobility agent (GFA) receives the registration message, it
   MUST remove the HFA extension added by the sending FA.

   If a MN with a co-located care-of address adds the HFA extension to a
   Registration Request, the receiving mobility agent (GFA) sets up a
   pending registration record for the MN, using the IP address in the
   HFA extension as the care-of address for the MN. The extension MUST
   be protected by an authentication extension. If the MN has
   established a mobility security association with the GFA, the HFA
   extension MUST be placed before the MN-FA Authentication extension,
   and it SHOULD be placed after the Mobile-Home (MN-HA) Authentication
   extension. Otherwise, if the MN has no established mobility security
   association with the GFA, the HFA extension MUST be placed before the
   MN-HA authentication extension. If the HFA extension is placed after
   all other extensions, the receiving mobility agent (GFA) MUST remove
   the HFA extension added by the MN. Otherwise, when the HA receives
   the registration message, it ignores the HFA extension.

   The Hierarchical Foreign Agent (HFA) 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    |            reserved           |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                         FA IP Address                         |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type
     140 (Hierarchical Foreign Agent) (skippable)

   Length
      6

   FA IP Address
      The IP Address of the FA relaying the Registration Request.
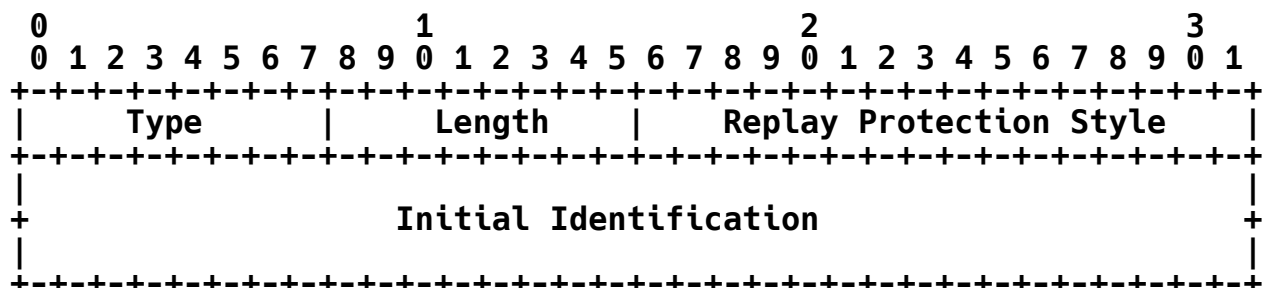
9.3. Replay Protection Style

   When a MN uses Mobile IPv4 to register a care-of address with its HA,
   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 MN and the HA receiving the request.
   No such pre-existing security association between the MN and the GFA
   is likely to be available. By default, the MN SHOULD treat replay
   protection for Regional Registration messages exactly as specified in
   Mobile IPv4 [RFC3344] for timestamp-based replay protection.

   If the MN requires nonce-based replay protection, also as specified
   in Mobile IPv4, it MAY append a Replay Protection Style extension to
   a Registration Request. Since Registration Requests are forwarded to
   the HA by way of the GFA, the GFA will be able to establish the
   selected replay protection (see Section 5.3).

   The GFA also uses this extension by adding a Replay Protection Style
   extension to a Registration Reply to synchronize the replay
   protection for Regional Registrations (see Section 5.3).

   The format of the Replay Protection Style extension is:

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

   Type
      141 (Replay Protection Style) (skippable)

   Length
      2

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

   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:

```
              +-------+---------------------------+
              | Value | Replay Protection Style   |
              +-------+---------------------------+
              | 0     | timestamp [RFC3344]       |
              | 1     | nonce [RFC3344]           |
              +-------+---------------------------+
```

   The Replay Protection Style extension MUST be protected by an
   authentication extension. If the MN has an established mobility
   security association with the GFA, the Replay Protection Style
   extension MUST be placed before the MN-FA Authentication extension in
   the Registration Request, and SHOULD be placed after the MN-HA
   Authentication extension. Otherwise, the Replay Protection Style
   extension MUST be placed before the MN-HA Authentication extension in
   the Registration Request.

   If the GFA adds a Replay Protection Style extension to a Registration
   Reply, it SHOULD be placed before the MN-FA Authentication extension.
   The MN-FA Authentication extension should be based on security
   associations between the MN and GFA established during home
   registration.

   Replay protection MAY also be provided through a challenge-response
   mechanism, at the FA issuing the Agent Advertisement, as described in
   [RFC4721].

9.4. Regional Registration Lifetime Extension

   The Regional Registration Lifetime extension allows the GFA to set a
   lifetime for the regional registration with an MN during its home
   registration. When receiving a Registration Reply from the HA, the
   GFA MAY add this extension to the Registration Reply before relaying
   it to the FA. The GFA MUST set the Regional Registration Lifetime to
   be no greater than the remaining lifetime of the MN's home
   registration.

The Regional Registration Lifetime 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    |            reserved           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Regional Registration Lifetime               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type
    142 (Regional Registration Lifetime) (skippable)

Length
    6

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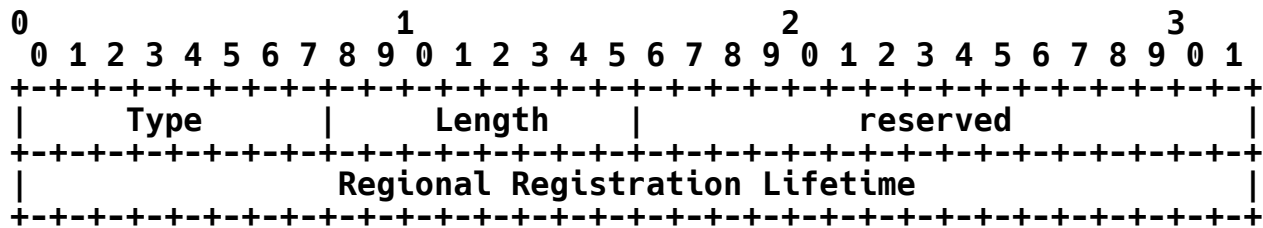   unspecified and MUST be ignored on reception.

    If the GFA adds a Regional Registration Lifetime extension to a
    Registration Reply, it MUST be placed before the MN-FA Authentication
    extension. The MN-FA Authentication extension should be based on
    security associations between the MN and GFA established during home
    registration.

9.5. New Code Values for Registration Reply

    The values to use within the Code field of the Registration Reply are
    defined in [RFC3344]. In addition, the following values are defined:

                    Registration denied by the GFA:

        +----------------------+-------+---------------------+
        | Error Name | Value | Section of Document |
        +----------------------+-------+---------------------+
        | REPLAY_PROT_UNAVAIL | 110 | Section 5.3 |
        | ZERO_COA_NOT_SUPP | 111 | Section 7.3 |
        +----------------------+-------+---------------------+

    Registration denied by the HA (for dynamic GFA assignment):

        +----------------------+-------+----------------------+
        | Error Name | Value | Section of Document |
        +----------------------+-------+----------------------+
        | ZERO_CAREOF_ADDRESS | 145 | Section 7.4 |
        | DYN_GFA_NOT_SUPP | 146 | Section 7.4 |
        +----------------------+-------+----------------------+

10. Regional Registration Message Formats

   This section specifies two new registration message types: Regional
   Registration Request and Regional Registration Reply. These messages
   are used by the MN instead of the existing Mobile IPv4 Registration
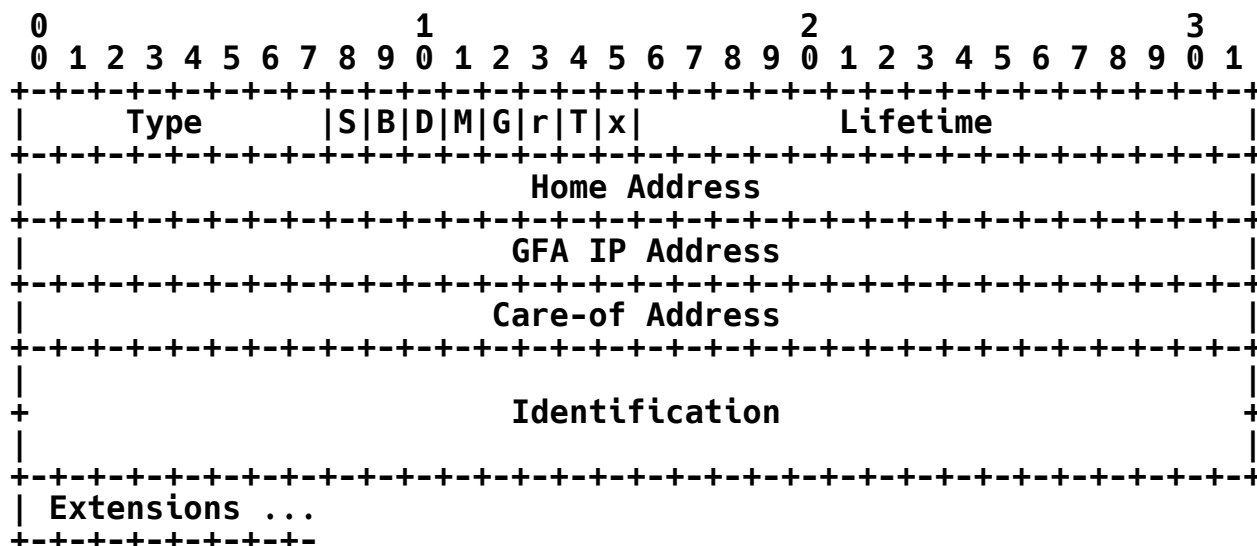   Request and Registration Reply, as described in Section 6.

   Regional registration messages are protected by required
   authentication extensions, in the same way as the existing Mobile
   IPv4 registration messages are protected. The following rules apply
   to authentication extensions:

   o The MN-GFA Authentication extension [RFC3344] MUST be included in
      all regional registration messages.
   o The MN-FA Authentication extension [RFC3344] MAY be included in
      regional registration messages.
   o The FA-HA Authentication extension [RFC3344] MUST NOT be included
      in any regional registration message.

10.1. Regional Registration Request

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

   Regional Registration Request:

```
     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|B|D|M|G|r|T|x|            Lifetime           |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                         Home Address                          |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                        GFA IP Address                         |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                        Care-of Address                        |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                                                               |
    +                        Identification                         +
    |                                                               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    | Extensions ...
    +-+-+-+-+-+-+-
```

   The Regional Registration Request is defined as the Registration
   Request in [RFC3344], but with the following changes:

   Type
      18 (Regional Registration Request)

   Lifetime
      The number of seconds remaining before the Regional Registration
      is considered expired. A value of zero indicates a request for
      deregistration with the GFA. A value of 0xffff indicates
      infinity.

   GFA IP Address
      The IP address of the Gateway Foreign Agent (GFA). (Replaces Home
      Agent field in Registration Request message in [RFC3344].)

   Care-of Address
      Care-of address of local FA; MAY be set to all-ones.

   Identification
      A 64-bit number, constructed by the MN, used for matching Regional
      Registration Requests with Regional Registration Replies, and for
      protecting against replay attacks of regional registration
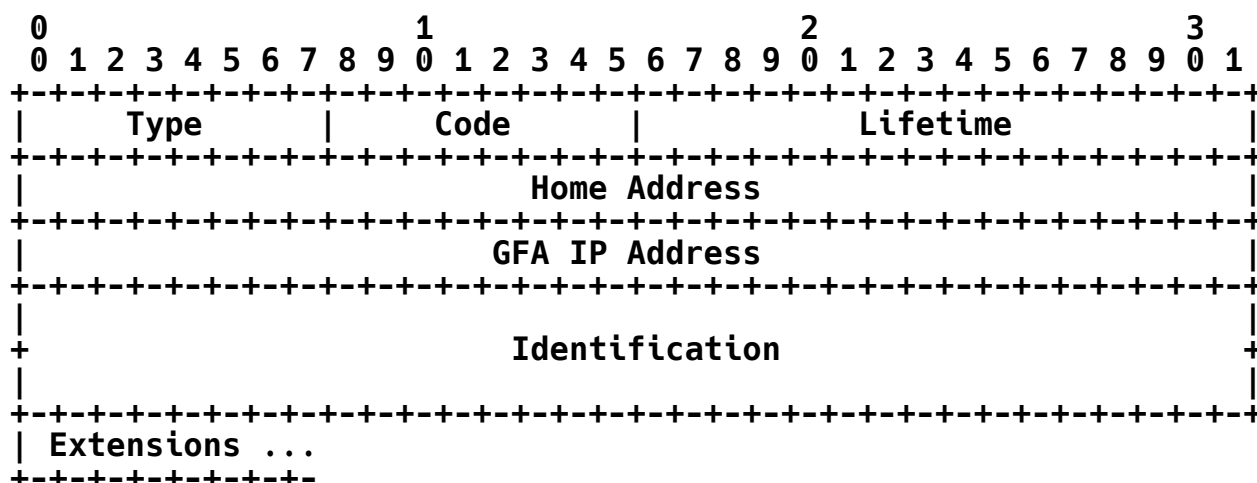   messages.

   Extensions
      For the Regional Registration Request, the Hierarchical Foreign
      Agent (HFA) Extension is an allowable extension (in addition to
      those which are allowable for the Registration Request).

10.2. Regional Registration Reply

   The Regional Registration Reply delivers the indication of regional
   registration acceptance or denial to a MN.

   In the Regional Registration Reply, the UDP header is followed by the
   Mobile IP fields shown below:

```
    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           |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                        Home Address                           |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                        GFA IP Address                         |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   +                        Identification                         +
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   | Extensions ...
   +-+-+-+-+-+-+-+-+-
```

   This message is defined as the Registration Reply message in
   [RFC3344], but with the following changes:

   Type
      19 (Regional Registration Reply)

   Code
      A value indicating the result of the Regional Registration
      Request. See [RFC3344] for a list of currently defined Code
      values.

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

GFA IP Address
    The IP address of the Gateway Foreign Agent (GFA) generating the
    Regional Registration Reply. (Replaces Home Agent field specified
    in Mobile IPv4 [RFC3344].)

Identification
    A 64-bit number used for matching Regional Registration Requests
    with Regional Registration Replies, and for protecting against
    replay attacks of regional registration messages. The value is
    based on the Identification field from the Regional Registration
    Request message from the MN, and on the style of replay protection
    used in the security context between the MN and its GFA (defined
    by the mobility security association between them).

10.3. New Regional Registration Reply Code Values

    For a Regional Registration Reply, the following additional Code
    values are defined in addition to those specified in Mobile IPv4
    [RFC3344].

                    Registration denied by the FA:

        +----------------------+-------+----------------------+
        | Error Name | Value | Section of Document |
        +----------------------+-------+----------------------+
        | UNKNOWN_GFA | 112 | Section 6.2 |
        | GFA_UNREACHABLE | 113 | |
        | GFA_HOST_UNREACHABLE | 114 | |
        | GFA_PORT_UNREACHABLE | 115 | |
        +----------------------+-------+----------------------+

                    Registration denied by the GFA:

            +-------------+-------+----------------------+
            | Error Name | Value | Section of Document |
            +-------------+-------+----------------------+
            | NO_HOME_REG | 193 | Section 6.3 |
            +-------------+-------+----------------------+

The four first Code values are returned to the MN in response to ICMP
errors that may be received by the FA.

11. Authentication Extensions

In this section, two new subtypes for the Generalized Authentication
Extension [RFC4721] are specified. First, the FA-FA Authentication
extension is used by FAs to secure the HFA extension to the
Registration Request and Regional Registration Request messages. A
new authentication extension is necessary because the HFA extension
is typically added after the MN-HA Authentication extension or, e.g.,
the MN-AAA Authentication extension [RFC4721].

The MN-GFA Authentication extension is used whenever the MN has a co-
located address. The MN-GFA Authentication extension is also used to
provide authentication for a Regional Registration Request.

The subtype values for these new subtypes are as follows:

```
+-------------------------+-------+
| Subtype Name            | Value |
+-------------------------+-------+
| FA-FA authentication    | 2     |
| MN-GFA authentication   | 3     |
+-------------------------+-------+
```

The default algorithm for computation of the authenticator is the
same as for the MN-AAA Authentication subtype defined in [RFC4721].

12. Security Considerations

This document proposes a method for a MN to register locally in a
visited domain. The authentication extensions to be used are those
defined in [RFC3344] and [RFC4721]. Key distribution, assumed to
take place during home registration, is to be performed, for
instance, according to [RFC4004] or [RFC3957]. Alternatively, the
keys can be pre-configured.

If the Hierarchical Foreign Agent (HFA) extension is appended to a
Registration Request, this extension is to be followed by an FA-FA
Authentication extension (see Section 11) to prevent any modification
to the data. Security associations between FAs and GFAs within a
domain are assumed to exist prior to regional registrations.

If the GFA IP Address extension is added to a registration message,
it is to be followed by a authentication extension. In case of the
GFA IP Address extension being added to a Registration Request, it
should be protected by an FA-HA Authentication extension. If no

security association exists between the GFA and the HA, the
Registration Request needs to be protected by other means not defined
in this document. When a GFA IP Address extension is added to a
Registration Reply, it is protected by the Mobile-Home Authentication
extension as defined in [RFC3344].

Replay protection for regional registrations is defined similarly to
[RFC3344], with the addition of a Replay Protection Style extension.
If this extension is added to a Registration Reply by a GFA, it needs
to be protected by a MN-FA Authentication extension.

A co-operating malicious MN-HA pair can trick the GFA into setting up
state for an incorrect MN home address. This would result in
redirection of data of the node that actually owns that IP address to
the malicious MN. Given that the forwarding happens based on the
home address at the GFA, such an attack is scoped to the prefix of
the HA, not that of the GFA. This type of attack, or its
consequences, is not considered in this document.

13. IANA Considerations

This document defines:

o A subtype for the NAI Carrying Extension [RFC3846] is specified in
   Section 8.2, which needs to have a value assigned from the space
   of NAI Carrying Extension subtypes.

o Four new extensions to Mobile IP Registration messages: GFA IP
   Address, Hierarchical Foreign Agent, Replay Protection Style, and
   Regional Registration Lifetime (see Sections 9.1, 9.2, 9.3, and
   9.4). The Type values for the GFA IP Address extension must be
   within the range 0 through 127, while the other three must be
   within the range 128 through 255.

o New Code values for Registration Reply messages (see Section 9.5).

o Two new subtypes for the Generalized Authentication Extension
   [RFC4721]; see Section 11.

o Two new message types for Mobile IP: Regional Registration Request
   and Regional Registration Reply (see Sections 10.1 and 10.2).

o Code values for Regional Registration Reply messages (see Section
   10.3).

14. Acknowledgements

This document is a logical successor to documents 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 for his commentary on a rough version of this document.

15. References

15.1. Normative References

   [RFC1256]   Deering, S., "ICMP Router Discovery Messages", RFC 1256,
               September 1991.

   [RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate
               Requirement Levels", BCP 14, RFC 2119, March 1997.

   [RFC4282]   Aboba, B., Beadles, M., Arkko, J., and P. Eronen, "The
               Network Access Identifier", RFC 4282, December 2005.

   [RFC2794]   Calhoun, P. and C. Perkins, "Mobile IP Network Access
               Identifier Extension for IPv4", RFC 2794, March 2000.

   [RFC3024]   Montenegro, G., "Reverse Tunneling for Mobile IP,
               revised", RFC 3024, January 2001.

   [RFC3344]   Perkins, C., "IP Mobility Support for IPv4", RFC 3344,
               August 2002.

   [RFC3519]   Levkowetz, H. and S. Vaarala, "Mobile IP Traversal of
               Network Address Translation (NAT) Devices", RFC 3519, May
               2003.

   [RFC3846]   Johansson, F. and T. Johansson, "Mobile IPv4 Extension for
               Carrying Network Access Identifiers", RFC 3846, June 2004.

   [RFC4721]   Perkins, C., Calhoun, P., and J. Bharatia, "Mobile IPv4
               Challenge/Response Extensions (Revised)", RFC 4721,
               January 2007.

15.2. Informative References

   [RFC3957]   Perkins, C. and P. Calhoun, "Authentication,
               Authorization, and Accounting (AAA) Registration Keys for
               Mobile IPv4", RFC 3957, March 2005.

   [RFC4004]   Calhoun, P., Johansson, T., Perkins, C., Hiller, T., and
               P. McCann, "Diameter Mobile IPv4 Application", RFC 4004,
               August 2005.

Appendix A. Authentication, Authorization, and Accounting (AAA)
             Interactions

   When the mobile node has to obtain authorization by way of
   Authentication, Authorization, and Accounting (AAA) infrastructure
   services, the control flow implicit in the main body of this
   specification is likely to be modified. Typically, the mobile node
   will supply credentials for authorization by AAA as part of its
   registration messages. The GFA will parse the credentials supplied
   by the mobile and forward the appropriate authorization request to a
   local AAA server (see [RFC3012] and [RFC4004]).

   Concretely, this means that:

   o The GFA MAY include the Mobile IP Registration Request data inside
      an authorization request, directed to a local AAA server.

   o The GFA MAY receive the Mobile IP Registration Reply data from a
      message granting authorization, received from the AAA
      infrastructure.

Appendix B. Anchoring at a GFA

   As described earlier in this draft, once a mobile node has registered
   the address of a GFA as its care-of address with its home agent, it
   MAY perform regional registrations when changing foreign agent under
   the same GFA. When detecting that is has changed foreign agent, and
   if the new foreign agent advertises the 'I' flag, the mobile node MAY
   address a Regional Registration Request message to its registered
   GFA, even if the address of that particular GFA is not advertised by
   the new foreign agent. The foreign agent MAY then relay the request
   to the GFA in question, or deny the request with error code
   UNKNOWN_GFA.

Authors' Addresses

    Eva Fogelstroem
    Ericsson
    Torshamnsgatan 23
    SE-164 80 Stockholm
    Sweden

    EMail: eva.fogelstrom@ericsson.com

    Annika Jonsson
    Ericsson
    Tellusborgsvagen 83-87
    S-126 37 Hagersten
    Sweden

    EMail: annika.jonsson@ericsson.com

    Charles E. Perkins
    Nokia Siemens Networks
    313 Fairchild Drive
    Mountain View, California 94043
    USA

    EMail: charles.perkins@nsn.com