Internet Engineering Task Force   C. Perkins
INTERNET DRAFT   IBM
                                                        22 February 1996

Mobile-IP Local Registration with Hierarchical Foreign Agents
<draft-perkins-mobileip-hierfa-00.txt>

Status of This Memo

This document is a submission to the Mobile IP Working Group of the Internet Engineering Task Force (IETF). Comments should be submitted to the mobile-ip@SmallWorks.COM mailing list.

Distribution of this memo is unlimited.

Abstract

The base mobile-IP specification allows mobile computers to move freely between various points of attachment to the Internet. However, each time the mobile computer moves, a Registration Request message has to be approved by the mobile node's Home Agent. In cases where the home agent is far away, it may become too expensive or (in the cases of network partition) even impossible to complete these frequent registrations. In this draft document, we specify a new variety of registration, using a Regional Registration Request and Regional Registration Reply, that is no longer always required to be transacted with the home agent.

Contents

1. Introduction

The base mobile-IP specification allows mobile computers to move freely between various points of attachment to the Internet. However, each time the mobile computer moves, a Registration Request message has to be approved by the mobile node's Home Agent. In cases where the home agent is far away, it may become too expensive or (in the cases of network partition) even impossible to complete these frequent registrations.

In this draft document, we specify a new variety of registration, using a Regional Registration Request and Regional Registration Reply, that is no longer always required to be transacted with the home agent. Using this new registration technique, the foreign agents in the local and/or regional area provide mobility services to the mobile node and allow some degree of independence from the home agent. The foreign agents are arranged hierarchically in the regional topology, and the mobile node is then allowed to move from one local area of the regional topology to another area of the same regional topology without requiring approval by or rebinding at the home agent.

In this document, when a mobile node changes its point of attachment to the Internet, we say it "moves". Thus, a change in point of attachment is a movement.

It is possible to make improvements by allowing a mobile node to inform only local mobility agents each time it moves. However, the local agents must then cooperate to allow the home agent to have incomplete knowledge of the mobile node's true point of attachment. For example, if the mobile node is currently located at one care-of address, but the home agent stores another care-of address in the mobile node's binding, then the two foreign agents offering those two care-of addresses in question must cooperate to make sure all datagrams tunneled to the latter care-of address are actually delivered to the mobile node.

One approach to this problem is to allow the mobile node to send Registration Requests to a regional foreign agent that tracks its regional movements but does not forward the mobile node's Request to its home agent. If the regional foreign agent is the tunnel endpoint for datagrams encapsulated by the home agent, then the regional foreign agent can make further arrangements for delivery of the datagram. In this document, we further enhance this regional handling by effectively allowing subregions of regions and so on, and structuring the foreign agents which manage each region in a hierarchy.

Since Agent Advertisements can contain multiple care-of addresses, a natural implementation of the hierarchy presents itself. Each foreign agent simply includes its ancestors in the tree of regional foreign agents in the list of care-of addresses in the Agent Advertisement. In order to maintain compatibility with mobile nodes that do not implement any processing for the foreign agent hierarchy, each foreign agent must advertise its own care-of address first in the list.

In this specification, the mobile node will re-register using a new Registration Request that includes all the fields of the existing Registration Request, but which includes more "care-of addresses and places a different meaning on the address found in the Home Agent field in the existing Registration Request. Put briefly, the Home Agent address is replaced by the address of the nearest "regional foreign agent" that has a previous registration with the mobile node.

1.1. Terminology

In addition to all the terminology in the base mobile-IP specification, this document frequently uses the following terms:

Targeted Mobility Agent

The mobility agent to which a Regional Registration Request is sent.

2. Operation

Conceptually, the mobile node attempts to minimize the amount of tracking required to maintain its traffic flow. This amounts to identifying the smallest region for which the mobile node has not travesed any regional boundary. That amounts to finding the closest ancestor to the foreign agent advertising the first care-of address in the list in the Advertisement, which was also an ancestor at the mobile node's last point of attachment. The mobile node may do this as outlined below.

2.1. Finding the Right Foreign Agent

Each time a mobile node determines that it has moved, it keeps track of the hierarchy of foreign agents serving its new point of attachment. At least the first care-of address will be different in the Agent Advertisements detected at the mobile node's new point of attachment.

When a mobile node moves to a new point of attachment, it checks the list of care-of addresses, starting with the last one. If the last care-of address is the same as the previous last care-of address, it looks at the next-last care-of address. If that one is also the same as the next-last care-of address at its previous point of attachment, the mobile node checks the next-next-last care-of address, and so on until a care-of address is found that is different than the corresponding care-of address in the list which was advertised at the mobile node's previous point of attachment.

Once the mobile node finds out the lowest level of the hierarchy, which has a different care-of address, it notifies the foreign agent at the next-higher level of the hierarchy about the different care-of address. This is done by the new Registration Request message, called the Regional Registration Request message. The foreign agent nearest the mobile node (the first care-of address) relays the Registration Request to next-higher level of the hierarchy and thus along towards the target of the Registration Request, just as if the target foreign agent (call it the targeted mobilitye agent) were the home agent.

If the targeted mobility agent approves the Regional Registration Request, it returns a Registration Reply of similar type and format as inthe base mobile-IP specification.

The processing of the Regional Registration Request and Registration Reply requires further refinement compared to the registration processing in the base mobile-IP specification. When the foreign agent receives the Request from the mobile node, it must pass the Request along to its next nearest ancestor in the hierarchy along the way to the agent listed as the Home Agent. In this way, each foreign agent in the hierarchy between the mobile node and the home agent will be able to maintain a binding for the mobile node. Similarly, Regional Registration Replies are passed down from one level of the hierarchy to the next along the way to the mobile node, so that each foreign agent can determine the status of the corresponding Registration Request and create the appropriate binding for the mobile node. Note that each foreign agent's binding will be for the care-of address at the next lower level of the hierarchy, not necessarily the care-of address of the foreign agent advertising the care-of address hierarchy to the mobile node.

2.2. Security

Note that home agent can be considered a "universal root" for all such hierarchies of foreign agents as described above. In fact, considered as an implicit care-of address, the home agent's address

is an ancestor of every other care-of address, and the mobile node is guaranteed of never straying from the boundaries of the region defined by the home agent's "care-of address".

Thought of in this way, there is the same clear threat posed by illicit Registration Requests, and thus the same need for authenticating that Registration Requests.

Unfortunately, the mobile node and the home agent currently share keys which are configured manually. Such manual configuration is unrealistic with the Regional Registration Request. Fortunately, the problem is analogous to the requirement in the Route Optimization [2] protocol specification, for a mobile node's current foreign agent to obtain a session key with the mobile node for as long as the mobile node is on the foreign agent's visitor list.

As outlined in this document, when a mobile node registers with its home agent, it "registers" with all the foreign agents in the hierarchy between the home agent and the mobile node. When it registers the top-level care-of address with its home agent, the mobile node acquires a session key, using one of the extensions specified for Route Optimization [2]. Suppose that each foreign agent in the hierarchy shares the same session key that the home agent sent to the foreign agent at the top level of the hierarchy.

Subsequent moves by the mobile node may require re-registration with some (or all) of the foreign agents in the hierarchy without causing any change to the home agent's binding for the mobile node. Since each foreign agent between the mobile node's previous care-of address and the home agent shares the same session key, when the mobile re-registers an intermediate care-of address with an unchanged care-of address immediately above it in the hierarchy, the mobile node already shares a session key with the care-of address which didn't change. To effect the move, then, the mobile node just has to send the session key along with its registration through the changed parts of the hierarchy, until the re-registration occurs at the lowest-level care-of address which has not changed and which is handled by a foreign agent which shares the same session key with the mobile node.

Since each Regional Registration Request is passed to every foreign agent between the mobile node and the "closest" foreign agent that didn't change, when the Regional Registration Reply comes back, the targeted mobility agent processing the Request can encode the session key for each new foreign agent which will handle the Reply.

2.3. Forwarding Datagrams to the Mobile Node

At each level of the hierarchy, the foreign agent advertising the care-of address at that level has a binding for the mobile node. The mobile node's binding shows that it is "regionally registered" at the care-of address at the next lower level of the hierarchy.

Thus, a datagram arriving at the top of the hierarchy from the home agent will (figuratively speaking) be decapsulated and re-encapsulated with a new tunnel endpoint, viz. the care-of address at the next lower level of 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.

3. Agent Advertisements

A foreign agent wishing to participate in a hierarchy of foreign agents advertises its services using the Mobility Extension to ICMP Router Advertisement which is defined in the base mobile-IP document. However, a strict ordering is imposed on the list of care-of addresses; the first care-of address is associated with the advertising agent, and each successive care-of address must be associated with the next-higher foreign agent in the hierarchy.

In addition, a new bit (the 'I' bit, for hIerarchical) is defined in the "flags" field of the Agent Advertisement, so that the mobile node can be assured that the advertising agent is indeed equipped to handle the Regional Registration Request 4. The format is as follows

(all other fields not defined here are unchanged from the definition given in the base mobile-IP document [1]).

```
    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        |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |    Registration Lifetime      |R|B|H|F|M|G|V|I|   reserved    |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                  zero or more Care-of Addresses               |
   |                              ...                              |
```

I   If set, the foreign agent is advertising a hierarchy of care-of addresses, and can properly process a Regional Registration Request.

4. Regional Registration Request

A mobile node registers with all of the hierarchical mobility agents between itself and its home agent using a Regional Registration Request message. When using a co-located care-of address as the lowest level care-of address of the foreign agent hierarchy, the mobile node may re-register with its previous care-of address if that care-of address wasn't a co-located care-of address.

Each mobility agent receiving the Request relays it to the next higher-level care-of address in the hierarchy. For each pending Regional Registration Request, in addition to the information stored for the processing of Registration Requests as required by the base specification, each foreign agent stores the care-of address of the next-lower foreign agent in the hierarchy. This address is available in the Request message, as shown below.

Note the similarity between the Regional Registration Request and the conventional Registration Request defined in the base mobile-IP specification [1]. Unless specifically superseded in this document, all processing of Regional Registration Requests by mobility agents is required to be the same as the processing by mobility agents in the base mobile-IP draft specification [1]. The UDP fields also are the same as in the base draft specification.

IP fields:

Source Address   Typically the interface address from which
                      the message is sent.

Destination Address   Typically that of the mobility agent at
                      the next higher level of the hierarchy of
                      mobility agents.

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      |S|B|D|M|G|V|rsv|          Lifetime             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Care-of Address Count     |          Reserved             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Home Address                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Mobility Agent                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Care-of Addresses ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                         Identification                        +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Extensions ...
+-+-+-+-+-+-+-+-
```

All fields not listed here are definied just as in the base mobile-IP document.

Type   8 (Regional Registration Request)

Mobility Agent   The IP address of the targeted mobility agent, which is the lowest-level foreign agent which is present in Agent Advertisements received both at the mobile node's previous and current points of attachment.

Care-of Addresses   The care-of addresses of the mobile node sending the Regional Registration Request.

Extensions   The fixed portion of the Regional Registration Request is followed by one or more Extensions which are applicable to Registration Requests.

The Registration Request MUST include an authentication extension appropriate to the targeted mobility agent (either a Mobile-Home Authentication Extension, or a Mobile-Foreign Authentication Extension). In the case of the Mobile-Foreign Authentication Extension the mobile node MAY use the Mobility Security Association set up when it obtained a session key (e.g., using extension numbers 104 and 105 [2]). from a previous Regional Registration Extension it

transacted with its home agent and all intervening foreign agents at that time.

The same rules apply to the Regional Registration Request as apply to the Registration Request, regarding the relative order in which different extensions, when present, MUST be placed in a the registration message.

Each foreign agent which receives a Regional Registration Request compares its offered care-of address to the target mobility agent listed in the Request. If they are the same, the foreign agent determines whether or not to accept the request, and returns a Regional Registration Reply with the appropriate status code, as specified in 5. Otherwise, the foreign agent delivers the Registration Request to the next-higher care-of address in the hierarchy. The session-key extension selected by the mobile node is processed appropriately at each level of the hierarchy, if necessary. All foreign agents in the hierarchy between the mobile node and the home agents can share the same session key.

Each foreign agent MUST check to make sure that its address is included in the list of care-of addresses within the Request. If not, it rejects the request with status code 70.

Otherwise, the foreign agent makes note of the next lower-level care-of address, for future association with the mobile node's home address.

5. Regional Registration Reply

A mobility agent returns a Regional Registration Reply message to a mobile node which has sent a Regional Registration Request (Section 4) message, and to the foreign agent at each intermediate level of the hierarchy between itself and the mobile node. Each foreign agent above the mobile node in the hierarchy will receive the Regional Reply from the mobility agent at the next higher level of the hierarchy. The Regional Reply message contains the necessary codes to inform the mobile node about the status of its Request, along with the lifetime granted by the targeted agent, which MUST NOT be great enough to last longer than time at which the binding at the home agent would expire, as determined by the original lifetime granted by the mobile node's home agent in the last Registration Request (or Regional Registration Request) approved by the home agent.

When the foreign agent receives a successful Regional Registration Reply, it updates its binding for the mobile node, using the

next-lower care-of address in the hierarchy as the care-of address of the mobile node.

The foreign agent MUST NOT increase the Lifetime selected by the mobile node in the Regional Registration Request, since the Lifetime is covered by an Authentication Extension. The targeted mobility agent MUST NOT increase the Lifetime selected by the mobile node in the Regional Registration Request, since doing so could increase it beyond the maximum Registration Lifetime allowed by the foreign agent. If the Lifetime received in the Regional Registration Reply is greater than that in the Regional Registration Request, the Lifetime in the Request MUST be used. When the Lifetime received in the Regional Registration Reply is less than that in the Regional Registration Request, the Lifetime in the Reply MUST be used.

Note the similarity between the Regional Registration Reply and the conventional Registration Reply defined in the base mobile-IP specification [1]. Unless specifically superseded in this document, all processing of Regional Registration Replies by mobility agents is specified to be the same as the processing by mobility agents in the base mobile-IP draft specification [1]. This includes determining the validity of the Registration Request, and selecting the appropriate status code for the reply. The IP fields and UDP fields are chosen just as with the Registration Reply message in the base mobile-IP specification.

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                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Mobility Agent                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                         Identification                        +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Extensions ...
+-+-+-+-+-+-+-+-
```

```
   Type                  9 (Regional Registration Reply)
```

Code

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

Home Agent

The IP address of the mobile node's home agent.

Identification

A 64-bit number used for matching Registration Requests with Registration Replies, and for protecting against replay attacks of registration messages. The value is based on the Identification field from the Registration Request message from the mobile node, and on the style of replay protection used in the security context between the mobile node and its home agent (defined by the mobility security association between them, and SPI value in the Mobile-Home Authentication Extension). See Section 6.

Extensions

The fixed portion of the Regional Registration Reply is followed by one or more of Extensions. An authentication extension MUST be included in all Registration Replies returned by the mobility agent.

The following values are available for use within the Code field. Registration successful:

0	registration accepted
1	registration accepted, but simultaneous mobility bindings unsupported

Registration rejected:

64	reason unspecified
65	administratively prohibited
66	insufficient resources
67	mobile node failed authentication
68	mobility agent failed authentication
69	requested Lifetime too long
70	poorly formed Request
71	poorly formed Reply
72	requested encapsulation unavailable
73	requested Van Jacobson compression unavailable
80	home network unreachable (ICMP error received)
81	mobility agent host unreachable (ICMP error received)
82	mobility agent port unreachable (ICMP error received)
88	mobility agent unreachable (other ICMP error received)
133	registration Identification mismatch
135	too many simultaneous mobility bindings
136	unknown mobility agent address
144	Broadcast Preference Extension unsupported
145	Multicast Preference Extension unsupported

Up-to-date values of the Code field are specified in the most recent "Assigned Numbers" [3].

Note that processing of the Identification field, as discussed in Section 6, is significantly different than in the base mobile-IP specification when nonces are to be used. Each foreign agent receiving a successful Regional Registration Reply from the foreign agent immediately above it in the foreign agent hierarchy MUST replace any Identification stored and associated with the mobile node, with the fresh Identification in the received Reply message.

Note also that, when the targeted mobility agent is unknown, the Regional Registration Request works as well as the base mobile-IP Registration Request in helping the mobile node to discover its home agent's address. However, in that case the mobile node would probably prefer to use the base Registration Request, since the Request cannot be accepted anyway until the home agent's address is known.

6. Replay Protection

The Identification field is used to let the targeted mobility agent verify that a registration message has been freshly generated by the mobile node, not replayed by an attacker from some previous registration. Two methods are described in the base mobile-IP specification: timestamps (mandatory) and "nonces" (optional). All mobile nodes and mobility agents using Regional Registration messages MUST implement timestamp-based replay protection. These nodes MAY also implement nonce-based replay protection.

The style of replay protection in effect between a mobile node and its mobility agents is part of the mobile security association. A mobile node and its mobility agent MUST agree on which method of replay protection will be used. The interpretation of the Identification field depends on the method of replay protection as described in the subsequent subsections.

All requirements of the base mobile-IP specification regarding replay protection must be followed by mobile nodes using the regional registration procedures specified in this document. There is no change to the replay procedures when timestamps are used. However, for nonce-based replay protection additional refinements must be instituted by the mobile node. Other mobility agents process nonces as in the base protocol specification.

The Identification in a new Registration Request MUST NOT be the same as in an immediately preceding Request, and SHOULD NOT repeat while the same security context is being used between the mobile node and the home agent. Retransmission as in the base mobile-IP specification [1] is allowed.

6.1. Replay Protection using Nonces

The basic principle of nonce replay protection does not change from that described in the base mobile-IP specification. However, since there can now be multiple mobility agents all registering the same mobile node, the mobile node must maintain a vector of nonces, one for each mobility agent in its current hierarchy.

Whenever a targeted mobility agent receives a Regional Registration Request, it selects a new nonce using the same methods described for home agents selecting a new nonce in the base mobile-IP specification. The mobility agent then inserts the resulting Identification in the appropriate field of the Regional Registration Reply. Each mobility agent at lower levels of the hierarchy copy, when it receives the Reply, copies the new Identification for

possible use in receiving future Regional Registration Requests from the mobile node. In other words, new nonces from above in the hierarchy supersede existing nonces stored by intermediate foreign agents in the hierarchy.

When a mobile node receives a Regional Registration Reply, it in turn associates the nonce from the Identification field with every intermediate foreign agent between itself and the targeted mobility agent to which it had sent the Regional Registration Request.

If a registration message is rejected because of an invalid nonce, the Reply always provides the mobile node, and each other intermediate foreign agent at lower levels than the targeted mobility agent, with a new nonce to be used in the next registration. Thus the nonce protocol is self-synchronizing.

References

[1] IPv4 Mobility Support. ietf-draft-mobileip-protocol-15.txt - work in progress, February 1996.

[2] David B. Johnson and Charles E. Perkins. Route Optimization in Mobile-IP. draft-ietf-mobileip-optim-03.txt -- work in progress, November 1995.

[3] Joyce K. Reynolds and Jon Postel. Assigned Numbers. RFC 1700, October 1994.

Chair's Addresses

The working group can be contacted via the current chairs:

Jim Solomon
Motorola, Inc.
1301 E. Algonquin Rd.
Schaumburg, IL 60196

Work: +1-847-576-2753
E-mail: solomon@comm.mot.com

Tony Li
cisco systems
170 W. Tasman Dr.
San Jose, CA 95134

Work: +1-408-526-8186
E-mail: tli@cisco.com

Author's Address

Questions about this memo can be directed to:

Charles Perkins
Room J1-A25
T. J. Watson Research Center
IBM Corporation
30 Saw Mill River Rd.
Hawthorne, NY 10532

Work: +1-914-784-7350
Fax: +1-914-784-6205
E-mail: perk@watson.ibm.com