                    Route Optimization in Mobile IP

                    draft-ietf-mobileip-optim-08.txt

Status of This Memo

   This document is a submission by 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.

   This document is an Internet-Draft and is in full conformance with
   all provisions of Section 10 of RFC2026. Internet-Drafts are working
   documents of the Internet Engineering Task Force (IETF), its areas,
   and its working groups. Note that other groups may also distribute
   working documents as Internet-Drafts.

   Internet-Drafts are draft documents valid for a maximum of six months
   and may be updated, replaced, or obsoleted by other documents at
   any time. It is inappropriate to use Internet-Drafts as reference
   material or to cite them other than as "work in progress."

   The list of current Internet-Drafts can be accessed at:

      http://www.ietf.org/ietf/1id-abstracts.txt

   The list of Internet-Draft Shadow Directories can be accessed at:

      http://www.ietf.org/shadow.html.

Abstract

   This document defines extensions to the base Mobile IP protocol to
   allow for optimization of datagram routing from a correspondent
   node to a mobile node. Without Route Optimization, all datagrams
   destined to a mobile node are routed through that mobile node's home
   agent, which then tunnels each datagram to the mobile node's current
   location. The protocol extensions described here provide a means
   for correspondent nodes to cache the binding of a mobile node and to

then tunnel their own datagrams for the mobile node directly to that
location, bypassing the route for each datagram through the mobile
node's home agent. Extensions are also provided to allow datagrams
in flight when a mobile node moves, and datagrams sent based on an
out-of-date cached binding, to be forwarded directly to the mobile
node's new binding.

Contents

[1]. Introduction

The base Mobile IP protocol [12], allows any mobile node to move
about, changing its point of attachment to the Internet, while
continuing to be identified by its home IP address. Correspondent
nodes sending IP datagrams to a mobile node at its home address
in the same way as with any other destination. This scheme
allows transparent interoperation between mobile nodes and their
correspondent nodes, but forces all datagrams for a mobile node to
be routed through its home agent. Thus, datagrams to the mobile
node are often routed along paths that are significantly longer than
optimal. For example, if a mobile node is visiting some subnet,
even datagrams from a correspondent node on the same subnet must be
routed through the Internet to the mobile node's home agent (on its
home network), only then to be tunneled back to the original subnet
for final delivery. This indirect routing delays the delivery of the
datagrams to mobile nodes, and places an unnecessary burden on the
networks and routers along their paths through the Internet.

In this document, we will define extensions to the operation of
the base Mobile IP protocol to allow for better routing, so that
datagrams can be routed from a correspondent node to a mobile node
without going to the home agent first. We refer collectively to
these extensions as Route Optimization.

Route Optimization extensions provide a means for nodes to cache
the binding of a mobile node and to then tunnel their own datagrams
directly to the care-of address indicated in that binding, bypassing
the mobile node's home agent. Extensions are also provided to allow
datagrams in flight when a mobile node moves, and datagrams sent
based on an out-of-date cached binding, to be forwarded directly to
the mobile node's new care-of address.

All operation of Route Optimization that changes the routing of IP
datagrams to the mobile node is authenticated using the same type of
mechanisms used in the base Mobile IP protocol. This authentication
generally relies on a mobility security association established
in advance between the sender and receiver of such messages. The
association can be created using ISAKMP [7], SKIP [1], or any of the
registration key establishment methods specified in [10].

After Section 2 gives some extra terminology, Section 3 provides
an overview of the basic protocol operations associated with
Route Optimization. Section 4 defines the message types used
to update binding caches. Subsequent sections show the formats
for the messages, explaining the function of fields within each
message. Home agent considerations in Section 7, and foreign agent
considerations in Section 8.

2. Terminology

This document introduces the following terminology, in addition to
that used to describe the base Mobile IP protocol:

   Binding cache

      A cache of mobility bindings of mobile nodes, maintained by a
      node for use in tunneling datagrams to those mobile nodes.

   Binding update

      A message indicating a mobile node's current mobility binding,
      and in particular its care-of address.

   Registration Lifetime

      The registration lifetime is the time duration for which a
      binding is valid. The term remaining registration lifetime
      means the amount of time remaining for which a registration
      lifetime is still valid, at some time after the registration
      was approved by the home agent.

   Security Parameters Index (SPI)

      An index identifying a security context between a pair of
      nodes among the contexts available in the Mobility Security
      Association. SPI values 0 through 255 are reserved and MUST
      NOT be used in any Mobility Security Association.

   Triangle Routing

      A situation in which a Correspondent Host's packets to a Mobile
      Host follow a path which is longer than the optimal path
      because the packets must be forwarded to the Mobile Host via a
      Home Agent.

This protocol specification uses conventional meanings [2] for
capitalized words such as MUST, SHOULD, etc., to indicate requirement
levels for various protocol features.

3. Route Optimization Overview

This section provides an overview of the protocols and operations of
Route Optimization. These can be divided into two main parts:

 1. Updating binding caches

   2. Managing smooth handoffs between foreign agents

The first part of the document goes into detail about binding cache
maintenance, and then smooth handoff is considered.

3.1. Binding Caches

Route Optimization provides a means for any node to maintain a
binding cache containing the care-of address of one or more mobile
nodes. When sending an IP datagram to a mobile node, if the sender
has a binding cache entry for the destination mobile node, it may
tunnel the datagram directly to the care-of address indicated in the
cached mobility binding.

In the absence of any binding cache entry, datagrams destined for a
mobile node will be routed to the mobile node's home network in the
same way as any other IP datagram, and then tunneled to the mobile
node's current care-of address by the mobile node's home agent.
This is the only routing mechanism supported by the base Mobile IP
protocol. With Route Optimization, as a side effect of this indirect
routing of a datagram to a mobile node, the original sender of the
datagram may be informed of the mobile node's current mobility
binding, giving the sender an opportunity to cache the binding.

Any node may maintain a binding cache to optimize its own
communication with mobile nodes. A node may create or update a
binding cache entry for a mobile node only when it has received
and authenticated the mobile node's mobility binding. As before,
each binding in the binding cache also has an associated lifetime,
specified in the Binding Update message in which the node obtained
the binding. After the expiration of this time period, the binding
is deleted from the cache. In addition, a node cache may use any
reasonable strategy for managing the space within the binding cache.
When a new entry needs to be added to the binding cache, the node may
choose to drop any entry already in the cache, if needed, to make
space for the new entry. For example, a least-recently used (LRU)
strategy for cache entry replacement is likely to work well.

When a mobile node's home agent intercepts a datagram from the home
network and tunnels it to the mobile node, the home agent may deduce
that the original source of the datagram has no binding cache entry
for the destination mobile node. The home agent should then send
a Binding Update message to the original source node, informing it
of the mobile node's current mobility binding. No acknowledgment
for such a Binding Update message is needed, since additional future
datagrams from this source node intercepted by the home agent for the
mobile node will cause transmission of another Binding Update. For

a Binding Update to be authenticated by the original source node,

the source node and the home agent must have established a mobility
security association.

Similarly, when any node (e.g., a foreign agent) receives a tunneled
datagram, if it has a binding cache entry for the destination mobile
node (and thus has no visitor list entry for this mobile node), the
node receiving this tunneled datagram may deduce that the tunneling
node has an out-of-date binding cache entry for this mobile node.
In this case, the receiving node should send a Binding Warning
message to the mobile node's home agent, advising it to send a
Binding Update message to the node that tunneled this datagram. The
mobile node's home agent can be determined from the binding cache
entry, because the home agent address is learned from the Binding
Update that established this cache entry. The address of the node
that tunneled this datagram can be determined from the datagram's
header, since the address of the node tunneling this datagram is
the outer source address of the encapsulated datagram. As in the
case of a Binding Update sent by the mobile node's home agent, no
acknowledgment of this Binding Warning is needed, since additional
future datagrams for the mobile node tunneled by the same node will
cause the transmission of another Binding Warning. However, unlike
the Binding Update message, no authentication of the Binding Warning
message is necessary, since it does not directly affect the routing
of IP datagrams to the mobile node.

When sending an IP datagram, if the sending node has a binding cache
entry for the destination node, it should tunnel the datagram to the
mobile node's care-of address using the encapsulation techniques used
by home agents, and described in [8, 9, 3, 4].

3.2. Foreign Agent Smooth Handoff

When a mobile node moves and registers with a new foreign agent, the
base Mobile IP protocol does not notify the mobile node's previous
foreign agent. IP datagrams intercepted by the home agent after
the new registration are tunneled to the mobile node's new care-of
address, but datagrams in flight that had already been intercepted
by the home agent and tunneled to the old care-of address when
the mobile node moved are likely to be lost and are assumed to be
retransmitted by higher-level protocols if needed. The old foreign
agent eventually deletes its visitor list entry for the mobile node
after the expiration of the registration lifetime.

Route Optimization provides a means for the mobile node's previous
foreign agent to be reliably notified of the mobile node's new
mobility binding, allowing datagrams in flight to the mobile
node's previous foreign agent to be forwarded to its new care-of

address. This notification also allows any datagrams tunneled to

the mobile node's previous foreign agent, from correspondent nodes
with out-of-date binding cache entries for the mobile node, to be
forwarded to its new care-of address. Finally, this notification
allows any resources consumed by the mobile node at the previous
foreign agent (such as radio channel reservations) to be released
immediately, rather than waiting for its registration lifetime to
expire.

As part of the registration procedure, the mobile node may
request that its new foreign agent attempt to notify its previous
foreign agent on its behalf, by including a Previous Foreign Agent
Notification extension in its Registration Request message sent to
the new foreign agent. The new foreign agent then builds a Binding
Update message and transmits it to the mobile node's previous foreign
agent as part of registration, requesting an acknowledgment from the
previous foreign agent. The extension includes only those values
needed to construct the Binding Update message that are not already
contained in the Registration Request message. The authenticator for
the Binding Update message is computed by the mobile node using the
security association shared with its previous foreign agent. This
notification will typically include the mobile node's new care-of
address, allowing the previous foreign agent to create a binding
cache entry for the mobile node to serve as a forwarding pointer [5]
to its new location. Any tunneled datagrams for the mobile node that
arrive at its previous foreign agent after the forwarding pointer has
been created can then be re-tunneled to the mobile node's new care-of
address.

For this smooth handoff to be secure, during registration with a
new foreign agent, the mobile node and the foreign agent have to
have a security association. The security association is used to
authenticate the notification sent to the previous foreign agent.

The Mobility Agent Advertisement extension of the agent advertisement
message is revised under Route Optimization to include a bit
indicating that the foreign agent sending the advertisement supports
smooth handoffs.

The mobile node is responsible for occasionally retransmitting a
Binding Update message to its previous foreign agent until the
matching Binding Acknowledge message is received, or until the
mobile node can be sure that foreign agent has expired its binding.
The mobile node is likely to select a small timeout value for the
lifetime available to such bindings sent to previous foreign agents.

4. Route Optimization Message Formats

Route Optimization defines four message types used for management
of binding cache entries. These message types fit in the numbering
space defined in the base Mobile IP specification for messages sent
to UDP port 434. Each of these messages begins with a one-octet
field indicating the type of the message. The binding cache
management messages in this section are carried by way of UDP, sent
to port 434.

The following type codes are defined in this document:

```
     16      Binding Warning message
     17      Binding Request message
     18      Binding Update message
     19      Binding Acknowledge message
```

Route Optimization also requires one minor change to existing
Mobile IP messages: a new flag bit must be added to the Registration
Request message, replacing a previously unused, reserved bit in the
message.

This section describes each of the new Route Optimization messages
and the change to Registration Request message.

4.1. Binding Warning Message

A Binding Warning message is used to transmit advice that one or
more correspondent nodes or foreign agents are likely to have either
no binding cache entry or an out-of-date binding cache entry for
some mobile node. When any node detunnels a datagram destined for
the mobile node, if it is not the current foreign agent for the
destination mobile node, it SHOULD send a Binding Warning message to
the mobile node's home agent.

```
 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      |                 Reserved                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Mobile Node Home Address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Target Node Addresses ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
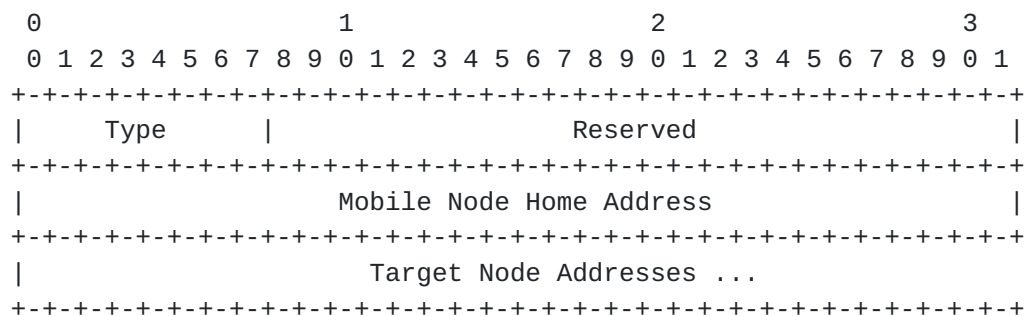
The format of the Binding Warning message is illustrated above, and
contains the following fields:

        Type   16

        Reserved Sent as 0; ignored on reception.

        Mobile Node Home Address
                The home address of the mobile node to which the Binding
                Warning message refers.

        Target Node Addresses
                One or more addresses of nodes that need to receive
                Binding Update messages. Each node should be the target
                of a Binding Update message sent by the home agent.

   A home agent will receive a Binding Warning message if a node
   maintaining a binding cache entry for one of the home agent's mobile
   nodes uses an out-of-date entry. When a home agent receives a
   Binding Warning message, it should send a Binding Update message to
   each target node address identified in the Binding Warning, giving it
   the current binding for the mobile node identified in the mobile node
   home address field of the Binding Warning.

   When a mobile node receives a new Care-of Address, it MAY send a
   Binding Warning message to its Home Agent, requesting that the home
   agent send Binding Update messages to one or more correspondent
   nodes. This feature MAY be used by the mobile node when it returns
   to its home network, so that the Home Agent will send out Binding
   Updates with zero lifetimes to all the mobile node's correspondent
   nodes. It is important for the correspondent nodes to delete their
   binding cache entries for the mobile node when the mobile node no
   longer has a Care-of Address.

4.2. Binding Request Message

   A Binding Request message is used by a node to request a mobile
   node's current mobility binding from the mobile node's home agent.

```
 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      |                   Reserved                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                   Mobile Node Home Address                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                        Identification                        +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The format of the Binding Request message is illustrated above, and
contains the following fields:

   Type   17

   Reserved Sent as 0; ignored on reception.

   Mobile Node Home Address
             The home address of the mobile node to which the Binding
             Request refers.

   Identification
             A 64-bit sequence number, assigned by the node sending
             the Binding Request message, used to assist in matching
             requests with replies, and in protecting against replay
             attacks.

When the home agent receives a Binding Request message, it consults
its home list and determines the correct binding information to be
sent to the requesting node. Before satisfying the request, the home
agent is required to check whether or not the mobile node has allowed
the information to be disseminated. If the mobile node specified
the private (P) bit in its Registration Request message, then the
home agent must make no further attempt to satisfy Binding Requests
on behalf of that mobile node. In this case, the home agent should
return a Binding Update in which both the care-of address is set
equal to the mobile node's home address and the lifetime is set to
zero. Such a Binding Update message indicates that the binding cache
entry for the specified mobile node should be deleted.

4.3. Binding Update Message

The Binding Update message is used for notification of a mobile
node's current mobility binding. It should be sent by the mobile
node's home agent in response to a Binding Request message, a Binding
Warning message, or the reception of a Binding Warning extension to
a Registration Request. It should also be sent by a mobile node, or
by the foreign agent with which the mobile node is registering, when
notifying the mobile node's previous foreign agent that the mobile
node has moved.

```
 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      |A|I|M|G|  Rsvd |            Lifetime           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Mobile Node Home Address                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Care-of Address                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                        Identification                         +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Extensions ...
+-+-+-+-+-+-+-+-
```

The format of the Binding Update message is illustrated above, and
contains the following fields:

    Type   18

      A   The 'A' (acknowledge) bit is set by the node sending the
               Binding Update message to request a Binding Acknowledge
               message be returned.

      I   The 'I' (identification present) bit is set by the node
               sending the Binding Update message if the identification
               field is present in the message.

      M   If the 'M' (minimal encapsulation) bit is set, datagrams
               may be tunneled to the mobile node using the minimal
               encapsulation protocol [9].

      G   If the 'G' (Generic Record Encapsulation, or GRE) bit is
               set, datagrams may be tunneled to the mobile node using
               GRE [3].

    Rsvd   Reserved. Sent as 0; ignored on reception.

    Lifetime The number of seconds remaining before the binding cache
              entry must be considered expired. A value of all ones
              indicates infinity. A value of zero indicates that no
              binding cache entry for the mobile node should be created
              and that any existing binding cache entry (and visitor
              list entry, in the case of a mobile node's previous
              foreign agent) for the mobile node should be deleted.
              The lifetime is typically equal to the remaining lifetime
              of the mobile node's registration.

     Mobile Node Home Address
             The home address of the mobile node to which the Binding
             Update message refers.

     Care-of Address
             The current care-of address of the mobile node. When set
             equal to the home address of the mobile node, the Binding
             Update message instead indicates that no binding cache
             entry for the mobile node should be created, and any
             existing binding cache entry (and visitor list entry, in
             the case of a mobile node's previous foreign agent) for
             the mobile node should be deleted.

     Identification
             If present, a 64-bit number, assigned by the node sending
             the Binding Request message, used to assist in matching
             requests with replies, and in protecting against replay
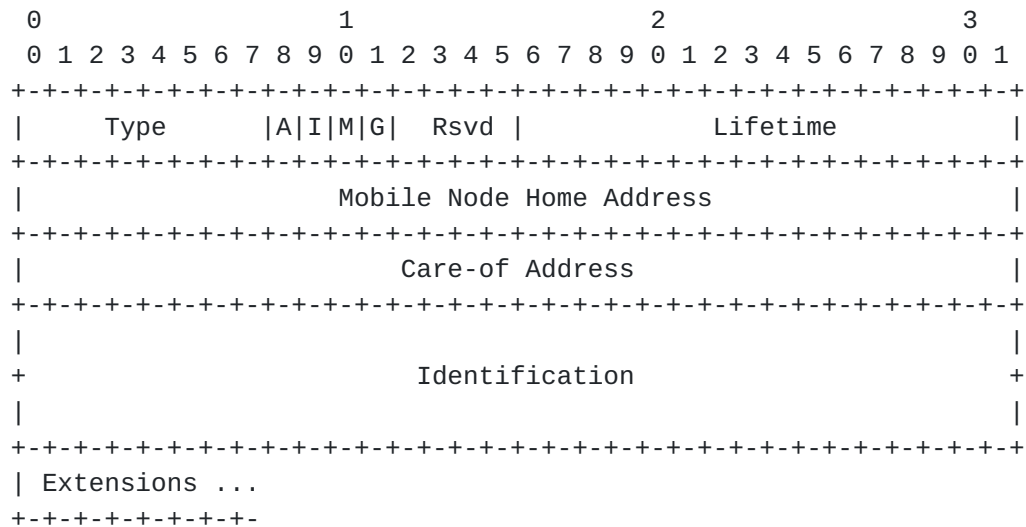   attacks.

Each Binding Update message indicates the binding's maximum lifetime.
When sending the Binding Update message, the home agent should set
this lifetime to the remaining registration lifetime. A node wanting
to provide continued service with a particular binding cache entry
may attempt to reconfirm that mobility binding before the expiration
of the registration lifetime. Such reconfirmation of a binding cache
entry may be appropriate when the node has indications (such as an
open transport-level connection to the mobile node) that the binding
cache entry is still needed. This reconfirmation is performed by
the node sending a Binding Request message to the mobile node's
home agent, requesting it to reply with the mobile node's current
mobility binding in a new Binding Update message. Note that the node
maintaining the binding should also keep track of the home agent's
address, to be able to fill in the destination IP address of future
Binding Requests.

When a node receives a Binding Update message, it is required to
verify the authentication in the message, using the mobility security
association it shares with the mobile node's home agent. The
authentication data is found in the Route Optimization Authentication
extension (Section 4.5), which is required. If the authentication
succeeds, then a binding cache entry should be updated for use in
future transmissions of data to the mobile node. Otherwise, an
authentication exception should be raised.

Under all circumstances, the sending of Binding Update messages is
subject to the rate limiting restriction described in Section 7.1.

When using nonces for replay protection, the identification field in

the Binding Update message is used differently in this case, to still

allow replay protection even though the Binding Update is not being
sent in reply to a request directly from the target node. In this
case, the home agent is required to set the high-order 32 bits of the
identification field to the value of the nonce that will be used by
the home agent in the next Binding Update message sent to this node.
The low-order 32 bits of the identification field are required to be
set to the value of the nonce being used for this message.

Thus, on each Binding Update message, the home agent communicates to
the target node, the value of the nonce that will be used next time,
and if no Binding Updates are lost in the network, the home agent and
the target node can remain synchronized with respect to the nonces
being used. If, however, the target node receives a Binding Update
with what it believes to be an incorrect nonce, it may resynchronize
with the home agent by using a Binding Request message.

4.4. Binding Acknowledge Message

A Binding Acknowledge message is used to acknowledge receipt of a
Binding Update message. It should be sent by a node receiving a
Binding Update message if the acknowledge (A) bit is set in the
Binding Update message.

```
 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      |            Reserved           |    Status     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Mobile Node Home Address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                              |
+                      Identification                          +
|                                                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The format of the Binding Acknowledge message is illustrated above,
and contains the following fields:

   Type   19

   Status   If the Status is nonzero, this acknowledgment is
            negative. For instance, if the Binding Update was
            not accepted, but the incoming datagram has the
            Acknowledge flag set, then the status code should be set
            appropriately in the Binding Acknowledge message.

   Reserved Sent as 0; ignored on reception.

      Mobile Node Home Address
              Copied from the Binding Update message being
              acknowledged.

      Identification
              Copied from the Binding Update message being
              acknowledged, if present there.

   Allowable values for the Status include:

      128 reason unspecified
      129 administratively prohibited
      130 insufficient resources
      131 sending node failed authentication
      133 identification mismatch
      134 poorly formed Binding Update

   Up-to-date values of the Code field are specified in the most recent
   "Assigned Numbers" [13].

4.5. Route Optimization Authentication Extension

   The Route Optimization Authentication extension is used to
   authenticate certain Route Optimization management messages. It has
   the same format and default algorithm support requirements as the
   three authentication extensions defined for base Mobile IP [12], but
   is distinguished by its type, which is 35. The authenticator value
   is computed, as before, from the stream of bytes including the shared
   secret, the UDP payload (that is, the Route Optimization management
   message), all prior extensions in their entirety, and the type and
   length of this extension, but not including the authenticator field
   itself nor the UDP header. This extension is required to be used in
   any Binding Update message.

4.6. Modified Registration Request Message

   One bit is added to the flag bits in the Registration Request message
   to indicate that the mobile node would like its home agent to keep
   its mobility binding private. Normally, the home agent sends Binding
   Update messages to correspondent nodes as needed to allow them to
   cache the mobile node's binding. If the mobile node sets the private
   ('P') bit in the Registration Request message, the home agent MUST
   NOT send the mobile node's binding in any Binding Update message.
   Instead, each Binding Update message should give the mobile node's
   care-of address equal to its home address, and should give a lifetime
   value of 0.

Thus, the Registration Request message under Route Optimization
begins as 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|P|r|            Lifetime           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     (Unchanged ...)
+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

   P   The private ('P') bit is set by the node sending the
            Binding Update message to indicate that the home agent
            should keep its mobility binding private. In any Binding
            Update message sent by the mobile node's home agent, the
            care-of address should be set equal to the mobile node's
            home address, and the lifetime should be set equal to 0.

   r   reserved

5. Format of Smooth Handoff Extensions

This section specifies the format for messages which are used
to enable smooth handoff from a mobile node's previous foreign
agent to its new foreign agent when a mobile node initiates a new
registration.

5.1. Previous Foreign Agent Notification Extension

The Previous Foreign Agent Notification extension may be included in
a Registration Request message sent to a foreign agent. It requests
the new foreign agent to send a Binding Update message to the mobile
node's previous foreign agent on behalf of the mobile node, to notify
it that the mobile node has moved. The previous foreign agent may
then delete the mobile node's visitor list entry and, if a new
care-of address is included in the Binding Update message, create a
binding cache entry for the mobile node with its new care-of address.
The Previous Foreign Agent Notification extension contains only those
values not otherwise already contained in the Registration Request
message that are needed for the new foreign agent to construct the
Binding Update message.

```
 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     |         Cache Lifetime        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 Previous Foreign Agent Address                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  New Care-of Address Address                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                              SPI                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Authenticator ...                     
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

   Type   96

   Length   14 plus the length of the authenticator

   Cache Lifetime
            The number of seconds remaining before the binding
            cache entry created by the previous foreign agent must
            be considered expired. A value of all ones indicates
            infinity. A value of zero indicates that the previous
            foreign agent should not create a binding cache entry for
            the mobile node once it has deleted the mobile node's
            visitor list entry. The cache lifetime value is copied
            into the lifetime field of the Binding Update message.

   Previous Foreign Agent Address
            The IP address of the mobile node's previous foreign
            agent to which the new foreign agent should send a
            Binding Update message on behalf of the mobile node.

   New Care-of Address
            The new care-of address for the new foreign agent to send
            in the Binding Update message to the previous foreign
            agent. This should be either the care-of address being
            registered in this new registration (i.e., to cause IP
            datagrams from the previous foreign agent to be tunneled
            to the new foreign agent) or the mobile node's home
            address (i.e., to cause the previous foreign agent to
            delete its visitor list entry only for the mobile node,
            but not forward datagrams for it).

   SPI   Security Parameters Index (4 bytes). An opaque
            identifier. The SPI is copied over into the Route
            Optimization Authentication extension by the new foreign

agent.

   Authenticator
               The authenticator value to be used in the Route
               Optimization Authentication extension in the Binding
               Update message sent by the new foreign agent to the
               mobile node's previous foreign agent. This authenticator
               is calculated only over the Binding Update message body.

   The binding cache entry created at the mobile node's previous
   foreign agent is treated in the same way as any other binding cache
   entry [12].

5.2. Modified Mobility Agent Advertisement Extension

   Performing smooth handoffs requires one minor change to the existing
   Mobile IP Mobility Agent Advertisement extension [12]. A new flag
   bit, the 'S' bit, replaces a previously unused reserved bit in
   the extension, to indicate that the foreign agent supports smooth
   handoffs. By default, every foreign agent that supports smooth
   handoffs SHOULD support at least the establishment of a registration
   key [10] by using Diffie-Hellman key exchange.

```
 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|V|T|S|  reserved    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     ...      zero or more Care-of Addresses
+-+-+-
```

   Thus, the proposed modification to the Mobility Agent Advertisement
   extension, illustrated above, keeps the advertisement almost the same
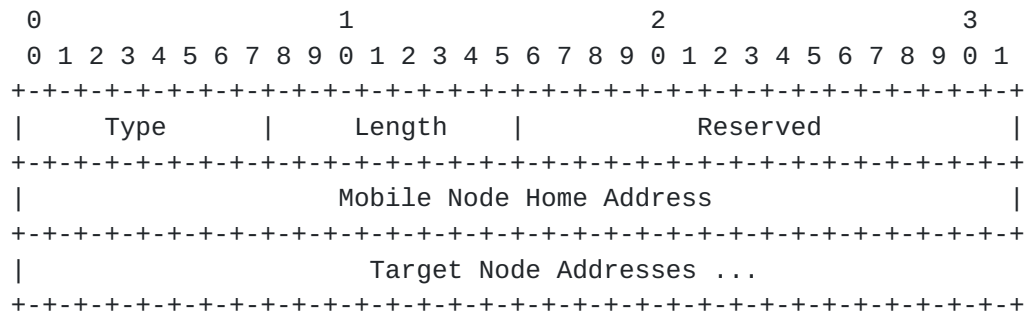   as in the base Mobile IP specification, except for adding following
   bit:

     S   The 'S' smooth handoff bit is set by the foreign agent
              sending the agent advertisement message to indicate
              that it supports the smooth handoffs, and thus the
              Registration Key Request and Diffie-Hellman Registration
              Key Reply extensions [10].

   More detailed information about the handling of this extension by
   foreign agents is deferred until Section 8.1.

6. **Binding Warning Extension**

   A mobile node may append a Binding Warning Extension to a
   Registration request. The Binding Warning extension is used to
   advise a mobile node's home agent that one or more correspondent
   nodes are likely to have either no binding cache entry or an
   out-of-date binding cache entry for the mobile node sending the
   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      |     Length    |             Reserved          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                   Mobile Node Home Address                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Target Node Addresses ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

   The format of the Binding Warning extension is illustrated above, and
   contains the following fields:

   Type   TBD

   Reserved Sent as 0; ignored on reception.

   Mobile Node Home Address
           The home address of the mobile node to which the Binding
           Warning message refers.

   Target Node Addresses
           One or more addresses of the correspondent nodes that
           need to receive Binding Update messages. Each node
           should be the target of a Binding Update message sent by
           the home agent.

   When a home agent receives a Binding Warning extension as part of a
   valid Registration Request, it should send a Binding Update message
   to each target node address identified in the Binding Warning, giving
   it the current binding for the mobile node identified in the mobile
   node home address field of the Binding Warning.

   When a mobile node returns to its home network, it MAY append a
   Binding Warning extension to the Registration Request message sent
   to its Home Agent, requesting that the home agent send Binding
   Update messages (naturally, with zero lifetimes) to one or more
   correspondent nodes. It is important for the correspondent nodes
   to delete their binding cache entries for the mobile node when the
   mobile node no longer has a Care-of Address.

7. Miscellaneous Home Agent Operations

7.1. Home Agent Rate Limiting

   A home agent is required to provide some mechanism to limit the
   rate at which it sends Binding Update messages to to the same node
   about any given mobility binding. This rate limiting is especially
   important because it is expected that, within the short term, most
   Internet nodes will not support maintenance of a binding cache. In
   this case, continual transmissions of Binding Update messages will
   only waste processing resources at the home agent and correspondent
   node, and along the Internet path between these nodes.

7.2. Mobility Security Association Management

   One of the most difficult aspects of Route Optimization for Mobile IP
   in the Internet today is that of providing authentication for all
   messages that affect the routing of datagrams to a mobile node.
   In the base Mobile IP protocol, only the home agent is aware of
   the mobile node's mobility binding and only the home agent tunnels
   datagrams to the mobile node. Thus, all routing of datagrams to the
   mobile node while away from its home network is controlled by the
   home agent. Authentication is currently achieved based on a manually
   established mobility security association between the home agent and
   the mobile node. Since the home agent and the mobile node are both
   owned by the same organization (both are assigned IP addresses within
   the same IP subnet), this manual configuration is manageable, and
   (for example) can be performed while the mobile node is at home.

   However, with Route Optimization, authentication is more difficult
   to manage, since a Binding Update may in general need to be sent to
   almost any node in the Internet. Since no authentication or key
   distribution protocol is generally available in the Internet today,
   the Route Optimization procedures defined in this document MAY make
   use of the same type of manual key distribution discussed in the base
   Mobile IP protocol. For use with Route Optimization, a mobility
   security association held by a correspondent node or a foreign agent
   must include the same parameters as required by base Mobile IP [12].

   For a correspondent node to be able to create a binding cache entry
   for a mobile node, the correspondent node and the mobile node's
   home agent are required to have established a mobility security
   association. This mobility security association, though, could
   conceivably be used in creating and updating binding cache entries
   at this correspondent node for all mobile nodes served by this home
   agent. Doing so places the correspondent node in a fairly natural
   relationship with respect to the mobile nodes served by this home

agent. For example, the mobile nodes may represent different people

affiliated with the same organization owning the home agent, with
which the user of the correspondent node often collaborates. The
effort of establishing such a mobility security association with
the relevant home agent may be more easily justified (appendix A)
than the effort of doing so with each mobile node. It is similarly
possible for a home agent to have a manually established mobility
security association with the foreign agents often used by its mobile
nodes, or for a particular mobile node to have a manually established
mobility security association with the foreign agents serving the
foreign networks that it often visits.

In general, if the movement and communication patterns of a mobile
node or the group of mobile nodes served by the same home agent are
sufficient to justify establishing a mobility security association
with the mobile node's home agent, users or network administrators
are likely to do so. Without establishing a mobility security
association, nodes will not currently be able to authenticate the
values transmitted in Route Optimization extensions.

7.3. Managing Binding Updates for Correspondent Nodes

The home agent MAY keep a list of correspondent nodes from which it
has received Binding Acknowledgements for Binding Updates for active
registrations (i.e., registrations which have not yet timed out). In
this case, when the home agent receives a valid Registration Request,
it MAY transmit new Binding Updates to each correspondent node that
is on its list for the particular mobile node. In order to know
which correspondent nodes correctly received the Binding Updates, the
home agent MUST set the `A' bit in the Binding Update, requesting an
acknowledgement.

Rate-limiting MUST be employed by a Home Agent offering this service,
as specified in section 7.1.

8. Miscellaneous Foreign Agent Operations

This section details various operational considerations important
for foreign agents wishing to support smooth handoff. This includes
processing Previous Foreign Agent Notification messages, and the
maintenance of up-to-date binding cache entries.

8.1. Previous Foreign Agent Notification

When a foreign agent receives a Previous Foreign Agent Notification
message, it creates a Binding Update for the previous foreign agent,
using the specified SPI and precomputed authenticator sent to it by

the mobile node. The Binding Update message is also required to set
the 'A' bit, so that the previous foreign agent will know to send a
Binding Acknowledge message back to the mobile node.

When the previous foreign agent receives the Binding Update, it will
authenticate the message using the mobility security association and
SPI specified in the Binding Update. If the message authentication
is correct, the visitor list entry for this mobile node at the
previous foreign agent will be deleted and a Binding Acknowledge
message returned to the sender. In addition, if a new care-of
address was included in the Binding Update message, the previous
foreign agent will create a binding cache entry for the mobile node;
the previous foreign agent can then tunnel datagrams to the mobile
node's new care-of address using that binding cache, just as any node
maintaining a binding cache. The previous foreign agent is also
expected to return a Binding Acknowledge message to the mobile node.

Note that this Binding Acknowledge is addressed to the mobile node,
and SHOULD be tunneled using the new binding cache entry. The
tunneled acknowledgment then SHOULD be delivered directly to the
new foreign agent, without having to go to the home network. This
creates an interesting problem for the new foreign agent when it
receives the acknowledgment before the Registration Reply from the
home agent. It is suggested that the new foreign agent deliver the
acknowledgment to the mobile node anyway, even though the mobile
node is technically unregistered. If there is concern that this
provides a loophole for unauthorized traffic to the mobile node, the
new foreign agent could limit the number of datagrams delivered to
the unregistered mobile node to this single instance. Alternatively,
a new extension to the Registration Reply message can be defined to
carry along the acknowledgment from the previous foreign agent. This
latter approach would have the benefit that fewer datagrams would
be transmitted over bandwidth-constrained wireless media during
registration.

When the Binding Acknowledge message from the previous foreign agent
is received by the new foreign agent, it detunnels it and sends
it to the mobile node. In this way, the mobile node can discover
that its previous foreign agent has received the Binding Update
message. The mobile node has to be certain that its previous foreign
agent has been notified about its new care-of address, because
otherwise the previous foreign agent could become a "black hole"
for datagrams destined for the mobile node based on out-of-date
binding cache entries at other nodes. The new foreign agent has no
further responsibility for helping to update the binding cache at the
previous foreign agent, and does not retransmit the message even if
no acknowledgment is received.

If the acknowledgment has not been received after sufficient time,
the mobile node is responsible for retransmitting another Binding
Update message to its previous foreign agent. Although the previous
foreign agent may have already received and processed the Binding
Update message (the Binding Acknowledge message may have been lost in
transit to the new foreign agent), the mobile node should continue
to retransmit its Binding Update message until the previous foreign
agent responds with a Binding Acknowledge.

8.2. Maintaining Binding Caches

It is possible that the binding cache entry taken by the previous
foreign agent from the information in the Previous Foreign Agent
Notification extension 5.1 will be deleted from its cache at any
time. In this case, the previous foreign agent will be unable to
re-tunnel subsequently arriving tunneled datagrams for the mobile
node, and would resort to using a special tunnel [11]. Mobile nodes
SHOULD assign small lifetimes to such bindings so that they will not
take up space in the foreign agent's binding cache for very long.

8.3. Rate Limiting

A foreign agent MUST provide some mechanism to limit the rate at
which it sends Binding Warning messages to the same node about any
given mobility binding. This rate limiting is especially important
because it is expected that, within the short term, many Internet
nodes will not support maintenance of a binding cache. In this case,
continual transmissions of Binding Warning messages will only waste
processing resources at the foreign agent and correspondent node, and
along the Internet path between these nodes.

9. Security Considerations

The calculation of the authentication data supplied with the Route
Optimization Authentication extension in section 4.5 is specified
to be the same as in the base Mobile IP document for ease of
implementation. There is a better method available (HMAC), specified
in RFC 2104 [6]. If the base Mobile IP specification is updated to
use HMAC, then this route optimization specification should also be
updated similarly.

10. Summary

In this document, we have presented the current protocol definition
for Route Optimization, by which is meant the elimination of triangle

routing whenever the correspondent node is able to perform the
necessary protocol operations. The Route Optimization protocol
definition is largely concerned with supplying a Binding Update to
any correspondent node that needs one (and has some realistic chance
to process it correctly). The Binding Update message is also used in
conjunction with the Previous Foreign Agent Notification message to
allow for smooth handoffs between foreign agents.

11. Acknowledgement

Expanding the Binding Warning to allow a mobile node to send a list
of correspondent nodes to the Home Agent was suggested by Mohamad
Khalil, Emad Qaddoura, Haseeb Akhtar, and Liem Le of Nortel Networks.

A. Using a Master Key at the Home Agent

Rather than storing each mobility security association that it has
established with many different correspondent nodes and foreign
agents, a home agent may manage its mobility security associations so
that each of them can be generated from a single master key. With
the master key, the home agent could build a key for any given other
node, for example by computing the node-specific key as
                MD5(node-address | master-key | node-address)
where node-address is the IP address of the particular node for which
the home agent is building a key, and master-key is the single master
key held by the home agent for all mobility security associations it
has established with correspondent nodes. The node-specific key is
built by computing an MD5 hash over a string consisting of the master
key with the node-address concatenated as a prefix and as a suffix.

Using this scheme, when establishing each mobility security
association, the network administrator managing the home agent
computes the node-specific key and communicates this key to the
network administrator of the other node through some secure channel,
such as over the telephone. The mobility security association
is configured at this other node in the same way as any mobility
security association. At the home agent, though, no record need be
kept that this key has been given out. The home agent need only be
configured to know that this scheme is in use for all of its mobility
security associations (perhaps only for specific set of its mobile
nodes).

When the home agent needs a mobility security association as part
of Route Optimization, it builds the node-specific key based on the
master key and the IP address of the other node with which it is
attempting to authenticate. If the other node knows the correct

     node-specific key, the authentication will succeed; otherwise, it
     will fail as it should.

References

  [1] A. Aziz, T. Markson, and H. Prafullchandra. Simple
      Key-Management For Internet Protocols (SKIP).
      draft-ietf-ipsec-skip-07.txt, August 1996. (work in progress).

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

  [3] Stan Hanks, Tony Li, Dino Farinacci, and Paul Traina. Generic
      Routing Encapsulation (GRE). RFC 1701, October 1994.

  [4] Stan Hanks, Tony Li, Dino Farinacci, and Paul Traina. Generic
      Routing Encapsulation over IPv4 networks. RFC 1702, October
      1994.

  [5] David B. Johnson. Scalable and Robust Internetwork Routing
      for Mobile Hosts. In Proceedings of the 14th International
      Conference on Distributed Computing Systems, pages 2--11, June
      1994.

  [6] H. Krawczyk, M. Bellare, and R. Cannetti. HMAC: Keyed-Hashing
      for Message Authentication. RFC 2104, February 1997.

  [7] D. Maughan, M. Schertler, M. Schneider, and J. Turner. Internet
      Security Association and Key Management Protocol (ISAKMP).
      draft-ietf-ipsec-isakmp-08.txt, July 1997. (work in progress).

  [8] Charles Perkins. IP Encapsulation within IP. RFC 2003, May
      1996.

  [9] Charles Perkins. Minimal Encapsulation within IP. RFC 2004,
      May 1996.

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

 [11] Charles E. Perkins and David B. Johnson. Special Tunnels for
      Mobile IP. draft-ietf-mobileip-spectun-00.txt, November 1997.
      (work in progress).

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

 [13] Joyce K. Reynolds and Jon Postel. Assigned Numbers. STD 2,
      October 1994.

Chairs' Addresses

   The working group can be contacted via the current chairs:

      Jim Solomon   Erik Nordmark
      Redback Networks, Inc.   Sun Microsystems, Inc.
      1301 E. Algonquin Road   17 Network Circle
      Schaumburg, IL 60196   Menlo Park, California 94025
      USA   USA

      Phone: +1-847-576-2753   Phone: +1 650 786-5166
      Fax: Fax: +1 650 786-5896
      E-mail: solomon@redbacknetworks.com   E-mail: nordmark@sun.com

   Questions about this document can also be directed to the authors:

      Charles E. Perkins   David B. Johnson
      Sun Microsystems Laboratories   Computer Science Department
      Mail Stop MPK15-214
      Room 2682
      Sun Microsystems, Inc.   Carnegie Mellon University
      15 Network Circly   5000 Forbes Avenue
      Menlo Park, California 94025   Pittsburgh, PA 15213-3891
      USA   USA
      Phone: +1-650-786-6464   Phone: +1-412-268-7399
      Fax: +1-650-786-6445   Fax: +1-412-268-5576
      E-mail: charles.perkins@Sun.COM   E-mail: dbj@cs.cmu.edu